Bournemouth University

# CYBERSECURITY FOR THE UNBANKED: USABLE SECURITY HEURISTICS FOR MOBILE FINANCIAL SERVICES

Stephen Mathew Ambore

A thesis submitted in partial fulfilment of the requirements of Bournemouth University for the degree of Doctor of Philosophy

Supervisors:

Prof Huseyin Dogan

Dr Edward Apeh

14 November 2024

## COPYRIGHT

# ACKNOWLEDGEMENT

I give all glory to God for his help, favour, and guidance through this journey.

I dedicate this work to the loving memory of my father, Maj LM Ambore, RTD, who unfortunately did not live to see me conclude this PhD journey.

I want to thank my supervisors Prof Huseyin Dogan and Dr Edward Apeh for their guidance, support and valuable feedback during this research. I would also like to acknowledge my former supervisor Dr Christopher Richardson for the opportunity given to me to enrol in this programme and for all the support and guidance he provided while he was still on the supervisory team.

Special thanks and love to my wife, Mallin, and the kids Ethan, Zara, and Bethel for their support and patience throughout this time-consuming journey.

My appreciation also goes to my mum, parents-in-law, siblings, Rev Williams, and other elders in my church for the prayers, support, and goodwill shown me throughout this study. Thank you, Dr Bala Tyeoden, Dr Robert Ifeonu, Erezi Esiekpe, and the rest of my colleagues for your support.

Finally, I thank my employer for their support, without which this would not have been possible.

Stephen Ambore

14 November 2024

# DECLARATION

I attest that all the work contained in this thesis was undertaken by me as part of this PhD research. All the content presented in this thesis is the output of the work I carried out since I commenced this study. Some of the findings of this research have been, fully or partially, presented at six conferences and published in one journal as indicated in section 1.7 of this thesis.

## ABSTRACT

Financial service providers leverage the growing adoption of mobile phones to develop and deploy new business models to provide financial services to new and existing customer bases. This has enabled the deployment of innovative financial products via mobile devices to capture new market segments while reducing operational costs. However, the downside of this development is the increased risk of cybersecurity threats to customers. These threats have affected existing users of mobile financial services and have the potential to impact 1.4 billion of the global adult population who are unbanked. Existing technical countermeasures, such as strong encryption algorithms, multi-factor authentication, and higher passcode complexity, have not fully addressed the cybersecurity problem in Mobile Financial Services (MFS). Literature has identified usable security as a problem area that leads to cybersecurity issues that affect users and developers of MFS solutions. While various aspects of this problem have been studied, the nature of usable security in the MFS sociotechnical system and how to address it, from the perspective of stakeholders in the ecosystem, has not been thoroughly examined.

This PhD thesis provides both theoretical and practical contributions by providing an understanding of socio-technical factors in mobile financial services and their impact on usable security from the perspective of stakeholders in the ecosystem. Also, it provides empirical evidence of the impact of user behaviours and DevOps practices on usable security for mobile financial services through a survey of 698 end-users and semi-structured interviews with 37 DevOps participants. Finally, the thesis presents a set of 12 usable security heuristics that were applied in a real-world scenario in the development and usable security evaluation of MFS.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# CHAPTER ONE: INTRODUCTION

The adoption of mobile phones as a means of accessing financial services is growing. Financial service providers are increasingly utilising this technology to engage both new and existing customer segments. However, this shift has concurrently resulted in a rise in cybersecurity incidents associated with using mobile financial services. While some technical countermeasures like strong encryption of wireless access points and two-factor authentication exist, these cybersecurity incidents have not abated. The chapter outlines the rationale for this PhD study and describes the problem under investigation. It presents the research questions posed, along with the overarching aim and specific objectives of the study, elucidating how these were addressed throughout the thesis. Furthermore, the chapter highlights the original contributions made by this PhD to the existing body of knowledge and provides an overview of the structure of the remaining chapters.

## 1.1 PROBLEM STATEMENT

Mobile Financial Services (MFS) present an opportunity for over 1.4 billion people globally to have access to finance (Demirgüç-Kunt et al. 2022). However, cybersecurity threats to MFS are affecting both existing and potential users of the solution. Various research studies that revealed the cybersecurity weaknesses in MFS have been conducted. For instance, in a study that exposed vulnerabilities in some mobile device-based solutions including MFS for banking and cryptocurrency, a man-in-the-middle (MITM) attack was possible in some MFS due to vulnerabilities with Transport Layer Security (TLS), despite the implementation of trusted certificate authority and certificate pinning. It also highlighted that security APIs can be misused by developers. Over 10 million mobile app users of banks were affected by a TLS vulnerability that exposed them to MITM attacks (Stone et al. 2017). Similarly, 2157 vulnerabilities in 693 MFS in 83 countries were identified in a recent study. Some of the identified weaknesses were classified as input harvest, lack of timely patching, use of applications from 3$^{rd}$ party sources, and communication infrastructure (Stone et al.2017, Chen et al. 2020). While some of these vulnerabilities are technical, some are based on the activity of human actors. For instance, user behaviour and developers' appreciation of security control are some key vulnerabilities that have been exploited in MFS (Chen et al. 2020, Wazid et al. 2019). These vulnerabilities have been exploited and have led to actual financial losses to MFS users (Khandelwal

2017a; Odues 2022). These incidents raise important questions about the security of MFS and the MFS ecosystem.

Strong technical countermeasures exist to mitigate cybercrime and provide a sense of security in the use of MFS. For instance, multi-factor authentication (MFA), biometric authentication, and secure encryption technology exist for mobile phones (Kunda and Chishimba 2018; Ibrahim et al. 2019). Furthermore, research has also been conducted on strengthening MFS security countermeasures. These studies have focused on strengthening technical countermeasures. For instance, Stone et al. 2017, proposed the automation of the certificate process to improve cybersecurity in MFS (Stone et al. 2017). Strengthening mobile app security through the strengthening of the hardware execution environment has also been explored (Li et al. 2019).

The literature highlighted suggests that there has been a predominant emphasis on the development and implementation of technical solutions to address cybersecurity in MFS. However, the effectiveness of these cybersecurity measures has been called into question, as these solutions neglect behavioural and environmental factors that influence user behaviours. This is evident in the fact that 80% of cybersecurity incidents and 82% of data breaches have been attributed to human factors (Gobler et al. 2021, Furnell 2024). This highlights the importance of addressing vulnerabilities related to the human element in ensuring cybersecurity works for MFS users.

Despite the significant impact of human-related vulnerabilities, it has been argued that the human element is not the "weakest link" in cybersecurity. Rather, the challenge lies in the disconnection between users and security systems, as well as the lack of emphasis on the principles of usable security (Gobler et al. 2021).

Various research studies have been conducted on improving cybersecurity through improving usable security. A historical perspective examined usable security evolution since 1975 and noted that it is a hard research problem as users are not inherently motivated to focus on adhering to security controls to the detriment of their tasks (Theofanos 2020). Similarly, it was noted that the lack of an approach to measure usable security might make it difficult to ascertain its efficacy in a system. The responsibility for ensuring usable security in the development process does not lie with the developer alone, but also with the user who should be part of the process of determining usable security requirements (Feth and Polts 2017). Furthermore, it has been argued that developers also need support to better improve the integration

of usable security principles in solution development (Chowdhury et al. 2021). These studies have highlighted the crucial need to address usable security in MFS to improve cybersecurity for both users and developers. Some studies while acknowledging this still focused on addressing the problem from a technical standpoint (Focardi et al. 2019). In other studies, the factors of usable security were simply derived by fusing elements of usability and security, which will further lead to addressing these two important perspectives in silos (Kumar et al.2020, Angrawal et al. 2022).

This PhD thesis project investigated the nature of usable security problems in MFS and how it affects the end-users and developers of the system. Furthermore, the study examined approaches for incorporating usable security into the development process of MFS to address the human element of cybersecurity for both end-users and supply-side actors like developers of MFS.

The proposed solution has been validated using real-world case studies. The findings from this research have been disseminated and have informed national central banking policy.

## 1.2 RESEARCH AIM

This PhD study examined usable security as a human factor problem that leads to cybersecurity threats in MFS. The study aims to explore how usable security can be improved for users and developers of MFS in order to enhance the human factor of cybersecurity in MFS.

## 1.3 RESEARCH QUESTIONS

The main question (RQM) this PhD thesis seeks to address is: *What design principles should inform the integration of usable security features in mobile financial services (MFS) to enhance cybersecurity?*

To address the challenge raised by the main question, the following supporting questions were also examined:

RQ1: In what ways does the current landscape of usable security influence cybersecurity effectiveness in the context of MFS, and what emerging trends or gaps exist?

RQ2: What is the experience of different stakeholders within the MFS ecosystem in usable security, and what insights can be drawn from their interactions with the system?

RQ3: What are the key usable security requirements for MFS that can mitigate human-centred vulnerabilities, and how can they be prioritised and integrated into development processes?

RQ4: What are the key considerations for designing a solution that addresses the identified usable security challenges in MFS?

RQ5: What approach can be used to test and validate the proposed solution in a real-world scenario?

## 1.4 RESEARCH OBJECTIVES

The objectives of this research are:

- **Objective 1: To investigate the state of play in usable security and how it affects cybersecurity in mobile financial services**

  This objective explored the impact of the human factor in cybersecurity as it affects MFS. Furthermore, it examined usable security problems in cybersecurity and how they are addressed in various domains, with the aim of understanding how addressing them can strengthen the human element and improve cybersecurity in MFS.

- **Objective 2: To contextualise the problem space from the perspective of MFS stakeholders**

  In addition to the insight obtained from the literature, this thesis examined the problem of MFS security from the perspective of key stakeholders in the ecosystem. Together with objective 1, this provided a more circumspect understanding of the problem space both in theory and practice, providing a foundation for a human-centred design solution.

  To address this objective, the following supporting objectives were also considered:

  2a. To identify cybersecurity imperatives in mobile financial services sociotechnical systems from the perspective of ecosystem actors

  2b. To examine how user behaviours affect the secure use of MFS

  2c. To examine practices of supply-side actors like developers and how they affect usable security in MFS

- **Objective 3: To develop an approach to address usable security in MFS, together with an implementation process**

  Based on the outcome obtained in objectives 1 and 2, a solution for addressing identified usable security concerns in MFS was developed. The solution was aimed at addressing the problem through the development of

solutions that can be applied during the mobile financial services solution development and testing phase of the developed solution. The proposed solution comprises various components leading to an overarching solution.

To address this objective, the following supporting objectives were also considered:

3a. To draw up detailed requirement documentation for addressing usable security problems in mobile financial services

3b. To design and develop an approach to address usable security solutions for mobile financial services based on the requirement developed, together with an implementation approach

- **Objective 4: To validate the proposed approach for addressing usable security problems in MFS**

  The developed solution was validated and improved. The findings of the studies were also published and presented at an academic conference to facilitate further input from experts. The proposed solution was then published as a peer-reviewed paper. The approach was refined to reflect critical suggested improvements.

- **Objective 5: To exploit and disseminate the validated solution including recommendations**

  The refined outcome of objective 4 was exploited by applying it to real-world MFS case studies. The first case study was for the incorporation of the solution in the development of MFS and fintech solutions via a hackathon where 44 teams participated in developing minimum viable products for various mobile financial services solutions. The second real-world problem used the developed solution to evaluate existing mobile financial services solutions.

## 1.5 CONTRIBUTIONS

This PhD provides both theoretical and practical contributions that have improved the understanding of usable security in MFS and also advanced an approach that can be applied in addressing gaps in current usable security practices within the MFS domain as follows:

**C1: Provide an Understanding of Sociotechnical Factors in Mobile Financial Services and Their Impact on Usable Security**: This PhD thesis provided a comprehensive understanding of usable security in mobile financial services sociotechnical systems by obtaining diverse stakeholders' perspectives through exploratory studies and focus groups. Through this effort, the study has enhanced the understanding of usable security issues in mobile financial services (MFS) from

multiple perspectives, identifying social and technical elements that influence usable security. This has contributed to a deeper comprehension of how various ecosystem players perceive and manage usable security in MFS, providing relevant sociotechnical insights into developing usable security for MFS. This contribution is valuable for researchers and solution developers who seek to improve cybersecurity for MFS.

**C2: Provide Empirical Evidence of the Impact of User Behaviour and DevOps Practices on Usable Security in MFS**: Through a survey of 698 participants and semi-structured interviews of 37 supply-side actors, this PhD thesis examined user behaviours and DevOps practices and their impact on usable security in MFS. This empirical evidence provided quantitative and qualitative insights that were used to improve MFS design and policies. This contribution is valuable for MFS providers and regulators looking to take cognisance of the human element in addressing cybersecurity vulnerabilities in MFS.

**C3: Develop and Validate Usable Security Heuristics for MFS**: Building on findings from the study of MFS sociotechnical systems, user behaviour analysis, and feedback from DevOps players, a set of 12 usable security heuristics specifically tailored for MFS was developed. These heuristics were rigorously validated by experts. The heuristics provide a practical guide to a better understanding of usable security for MFS developers, addressing the concerns about a lack of a set of heuristics suitable for MFS.

**C4: Demonstrate Real-World Application of Heuristics through Hackathon and Black-Box Testing**: In addition to theoretical contributions, this PhD thesis demonstrated how usable security heuristics can be integrated into the development of MFS through a hackathon and how it can be applied to evaluate usable security in MFS through black-box testing. Applying the developed heuristics in real-world scenarios provides a guide to MFS developers and testers on how to adopt a user-centric approach to develop a more secure MFS.

## 1.6 MAPPING OF RESEARCH AIM, QUESTIONS, AND CONTRIBUTIONS

This section shows the mapping of the research aims to the questions, objectives, and key contributions to facilitate traceability.

- Mapping Research Question to Research Aim

RQM, RQ1, RQ2, RQ3, RQ4 -> {this PhD research aims to develop a usable security approach to enhance usable security for mobile financial services}

RQ1, RQ2 RQ3, RQ5-> {the aim will be achieved by developing artefacts and validating them against real-world problems of MFS security}

- Mapping of Research Questions to Objectives and Contributions

Table 1.1 shows the relationship between the research question, objective, and contribution, including the chapters they relate to.

| Objective | Research Questions | Contribution | Chapter |
|---|---|---|---|
| **Objective 1: To investigate the state of play in usable security and how it affects cybersecurity in mobile financial services** | RQ1: In what ways does the current landscape of usable security influence cybersecurity effectiveness in the context of MFS, and what emerging trends or gaps exist?<br><br>RQ2: How do different stakeholders within the MFS ecosystem perceive and experience challenges related to usable security, and what insights can be drawn from their interactions with the system? | C1: Provided an understanding of user behaviours and supply-side practices that impact usable security in MFS. | 2,3,4 and 5 |
| **Objective 2: To contextualise the problem space from the perspective of MFS stakeholders** | RQ1: In what ways does the current landscape of usable security influence cybersecurity effectiveness in the context of MFS, and | C1: Provided an understanding of user behaviours and supply-side practices that impact usable security in MFS. | 4 and 5 |

| Objective | Research Questions | Contribution | Chapter |
|---|---|---|---|
| | what emerging trends or gaps exist?<br><br>RQ2: How do different stakeholders within the MFS ecosystem perceive and experience challenges related to usable security, and what insights can be drawn from their interactions with the system? | | |
| **Objective 3: To develop an approach to address usable security in MFS, together with an implementation process** | RQ3: What are the key usable security requirements for MFS that can mitigate human-centred vulnerabilities, and how can they be prioritised and integrated into development processes?<br><br>RQ4: What are the key considerations for designing a solution that addresses the identified usable security challenges in MFS? | C2: Developed and validated usable security heuristics that addressed the requirement for developing a usable secure MFS<br><br>C3: Developed an approach for integrating the developed usable security heuristics in the development and evaluation of MFS<br><br>C4: Provided a tool that addresses usable security challenges for users, developers, and evaluators of usable security in MFS | 6, 7 and 8 |

| Objective | Research Questions | Contribution | Chapter |
|---|---|---|---|
| **Objective 4: To validate the proposed approach for addressing the usable security problem in MFS** | RQM: What design principles should inform the integration of usable security features in mobile financial services (MFS) to enhance cybersecurity?<br><br>RQ3: What are the key usable security requirements for MFS that can mitigate human-centred vulnerabilities and how can they be prioritised and integrated into processes? | C2: Developed and validated usable security heuristics that addressed the requirement for developing a usable secure MFS. | 4,5,6,7 and 8 |
| **Objective 5: To Exploit and disseminate the validated solution including recommendations** | RQM: What design principles should inform the integration of usable security features in mobile financial services (MFS) to enhance cybersecurity?<br><br>RQ5: How can proposed solutions for usable security in MFS be tested and validated in real-world scenarios? | C3: Developed an approach for integrating the developed usable security heuristics in the development and evaluation of MFS<br><br>C4: Provided a tool that addresses usable security challenges for users, developers, and evaluators of usable security in MFS | 6, 7, 8 |

Table 1.1: Research Objective Mapping

## 1.7 LIST OF PUBLICATIONS

The research undertaken so far has led to the following publications:

**Journals**

I. Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2017. A Resilient Cybersecurity Framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, pp.1-23

**Conference Papers**

I. Ambore, S., Dogan, H. and Apeh, E., 2021, July. Development of Usable Security Heuristics for Fintech. In *34th British HCI Conference 34* (pp. 121-132)

II. Ambore, S., Breban, A., Apeh, E. and Dogan, H., 2021, July. Evaluating Security and Accessibility Trade-off for Visually Impaired Mobile Financial Services Users. In *34th British HCI Workshop and Doctoral Consortium 34* (pp. 1-5)

III. Ambore, S., Richardson, C., Dogan, H., and Apeh, E. 2018, Have Usability and Security Trade-offs in Mobile Financial Services (MFS) become Untrustworthy? British Computer Society Human-Computer Interaction Conference (BHCI) 2018

*IV.* Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2016. Development of Human Factors and Cybersecurity Objectives for Mobile Financial Services (MFS). *In Proceedings of Ergonomics and Human Factors (EHF) 2017 Conference*

V. Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D.M., 2016. A “Soft” Approach to Analysing Mobile Financial Services Sociotechnical Systems. In *Proceedings of British HCI 2016 – Fusion, Bournemouth, UK*

VI. Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2016. Cybersecurity for the Unbanked. In *Proceedings of PGCS conference 2016 - Edinburg, UK*

**Workshops**

Work on usable security for the physically impaired inspired the inception of the 1st Workshop on Diversity, Accessibility, and Inclusivity in Cyber Security. In 34th British HCI Workshop and Doctoral Consortium (pp. 1-4). BCS Learning & Development

Served as Advisory Committee Member for the 1st and 2nd Workshop on Diversity, Accessibility, and Inclusivity in Cyber Security. In 34th British HCI Workshop and Doctoral Consortium (pp. 1-4). BCS Learning & Development

**Citations**

As of the time of writing this report, the aforementioned publications have been cited **23 times**, as follows:

| # | Publication | Citations |
|---|---|---|
| 1 | Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2017. A Resilient Cybersecurity Framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, pp.1-23. | 32 |
| 2 | Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D.M., 2016. A "Soft" Approach to Analysing Mobile Financial Services Sociotechnical Systems. In *Proceedings of British HCI 2016 – Fusion, Bournemouth, UK* | 6 |
| 3 | Ambore, S., Dogan, H. and Apeh, E., 2021, July. Development of Usable Security Heuristics for Fintech. In *34th British HCI Conference 34* (pp. 121-132). | 4 |
| 4. | Ambore, S., Breban, A., Apeh, E. and Dogan, H., 2021, July. Evaluating Security and Accessibility Trade-off for Visually Impaired Mobile Financial Services Users. In *34th British HCI Workshop and Doctoral Consortium 34 (pp. 1-5)* | 1 |

Table 1.2: Citation

## 1.8 ASSUMPTIONS

This thesis represents the synopsis of the research conducted to date within the constraints of the word count limit as prescribed by the postgraduate research guideline. Relevant details of the studies conducted and research published have been added to the appendix.

As highlighted in section 1.2 of this thesis, various technical countermeasures for securing mobile financial services exist but have not led to a significant reduction in MFS cybersecurity concerns. This research addressed this by adopting a human-centric ecosystem approach, focusing on understanding the problem space from the perspective of key stakeholders in the MFS ecosystem. The research philosophy is underpinned in the concept that once the "*weak link*", is properly addressed then holistic countermeasures can be developed, hence the focus on human aspects above other cybersecurity concerns.

## 1.9 THESIS STRUCTURE

Eight studies were conducted as part of this PhD research. The findings from the studies and literature review were incorporated into the thesis chapters and appendices as follows:

*Chapter One: Introduction*

This chapter provides a background to this study and also defines key methodologies. It explains the problem statement for the research and provides research questions addressed by the PhD study. Furthermore, it provides the objectives of the study and defines how the objectives relate to the research questions, the key contribution of the study, and how they all relate to the chapters of this thesis.

*Chapter Two: Literature Review*

This chapter outlines an in-depth literature review as it relates to this PhD study. The chapter provides an overview of mobile financial services and also conducts a threat landscape analysis of the solution. The chapter examined the nature of usable security in MFS. Furthermore, it examined how usable security challenges are addressed in other domains to adopt or adapt any suitable approach for MFS. The chapter addresses the research question through a critical analysis of extant literature.

*Chapter Three: Research Methodology*

This chapter outlines the design methodology adopted for this research, including strategy and design choices. Additionally, the chapter describes a pragmatic research philosophical stance adopted for this research. The research leverages both inductive and deductive approaches to address the objective of the thesis. The chapter also provides reasons behind the research method choices by offering insight into qualitative techniques adopted for this research such as rich picture, interactive management, and thematic analysis, among others. Similarly, it provides insight into quantitative techniques used for the research such as principal component analysis and structural equation model. The research objective was a key determinant in the methodology approach and choices made in this study.

*Chapter Four: Problem Space Contextualisation Study on Usable Security in Mobile Financial Services Sociotechnical System*

While Chapter Two reveals gaps in the literature as regards usable security for mobile financial services, the need to further examine the human element in the ecosystem was identified. To further understand the human element in the ecosystem and how

it impacts cybersecurity for MFS, an exploratory study was conducted from the viewpoint of key players using human factor approaches. Using interactive management techniques, interpretive structural models, and nominal group techniques, six workshops were conducted for 30 stakeholders and 269 issues were generated together with priority objectives for mitigating usable security in MFS. The chapter also presented the nature of the mobile financial services sociotechnical system.

*Chapter Five: Exploratory Study on User Behaviours and DevOps Practices that Impact Usable Security in Mobile Financial Services*

The previous chapter reveals usable security as the key issue impacting cybersecurity in mobile financial services. However, there was a need to understand the nature of usable security through the eyes of the users of the system and the developers of the solution. This chapter presents the results of a survey of 689 users of mobile financial services, and a semi-structured interview of 37 stakeholders comprising bank CIOs and fintech solution providers. Principal component analysis was leveraged to reveal observable and latent variables on usable security which formed the basis for developing an approach for addressing usable security in MFS.

*Chapter Six: Requirements for Developing Usable Security Heuristics for Mobile Financial Services*

This chapter draws from the literature review and the findings from the exploratory studies in Chapters Four and Five of this thesis to develop a detailed requirement for usable security heuristics in MFS. Drawing from the International Institute of Business Analysis (IIBA) framework and the MoSCoW methodology, this chapter provided the detailed requirement for the development of usable security heuristics to address gaps identified in Chapters Two, Four and Five of this thesis.

*Chapter Seven: Solution Design and Validation: Development of Usable Security Heuristics for MFS*

Based on the literature review and two exploratory studies conducted in the previous chapter, and the requirements developed in Chapter Six of this PhD thesis, 12 heuristics for usable security were developed and presented in this chapter. The heuristics were validated through semi-structured interviews and focus groups by experts.

*Chapter Eight: Case Studies*

This chapter presents the result of the implementation of the developed heuristics in addressing real-world problems. The first case study was the application of the heuristic in solution development through a hackathon where participants leveraged the heuristics to develop a minimum viable product. The second case study was the application of heuristics in testing the existing system through a black-box user acceptance test approach. The last case study was applied to address issues related to visually impaired MFS users.

*Chapter Nine: Discussion*

This chapter discussed the findings of the PhD thesis, its validity, and its relation to other existing literature.

*Chapter Ten: Conclusion and Future Work*

This chapter describes the conclusion and direction of future work including how the research area has evolved from the commencement of this PhD study to date.

*Appendices I – VII*

All other supplementary materials of this thesis are added to this section.

## 1.10 CHAPTER SUMMARY

Mobile financial services has the potential to provide banking services to over 1.4 billion people globally. However, cybersecurity challenges have hindered the uptake of the solution. Several technical countermeasures exist, yet, the issue persists. This chapter defined the problem space, study objective, research questions, study aims, and contribution to knowledge. It also highlighted publications carried out as part of this research and provided a map of the entire work of the thesis.

The next chapter presents insight from the review of related literature as it affects this PhD study.

# CHAPTER TWO: LITERATURE REVIEW

This chapter presents the state of play for usable security in mobile financial services.

## 2.1 MOBILE FINANCIAL SERVICES OVERVIEW

Two-thirds of the world's population has a mobile phone. It has also been forecasted that by 2020, 75% of the world's population will own a mobile phone (GSMA 2018; Salam 2020; Subashini et al. 2022). In a world where about 1.4 billion people have no access to formal financial services (Demirguc-Kunt et al. 2022) the mobile phone due to its high penetration rate has become a variable tool for providing financial services in a way hitherto not possible by traditional banking means. Also, the mobile phone is now considered an alternative banking channel. Banks now provide banking services to end-users on mobile phones, capitalising on the high penetration of mobile phones and the need to reduce operational costs. For instance, a group of banks in the UK offer banking services via mobile phone using the Paym product (Barclays 2018; Lai 2020). mCash is a merchant-side mobile phone-based solution that facilitates low-value retail payments in Nigeria (NIBSS 2018). Banks are also rolling back branches. According to the Financial Stability Board (2018) and Lai (2020), since 1989, over 53% of UK bank branches have closed.

The mobile phone is now a convenient means of payment, hence the number of bank customers that use mobile phones as their preferred means of banking has risen by over 73% since 2014 (Owusu et al. 2021; Zhu et al. 2022).

The trend of customers using mobile payment applications to make payments via mobile phone gained prominence with Starbucks over two decades ago. This trend has further been heightened with significant technology service providers focusing on mobile phone-based payment products for their customers, with Apple and Google launching mobile payment products, which has in many ways led to the advent of mobile financial services (Beck 2020; Kumar and Mittal 2020; Zhang and Williamson 2021).

Mobile financial services is a term that has been described in various forms. Section 2.1.1 and 2.1.2 examined various forms of mobile financial services described in the literature.

### 2.1.1 Defining Mobile Financial Services – Mobile Banking, Mobile Payment and Mobile Money

Mobile financial services have become an important subject of research that has been examined from various perspectives. It has been described as a solution that provides value-added tech-based services e.g. funds transfer, balance inquiry, bill payments, savings, etc. Mobile financial services were also described as mobile banking, a service that is only available to bank customers. It allows bank customers to carry out financial transactions far from the service provider's location using their mobile phones. The characteristics of mobile banking include ubiquity and immediacy. Better quality of services, availability, and usability differentiate it from other banking services. Another paper extended the scope of the definition of mobile financial services, to include consideration for financial inclusion and inclusivity in financial services provisioning addressing the needs of the unbanked and underserved. Specific characteristics of mobile financial services that meet the needs of this group include cheap, secure, reliable, and accessible. The authors also mentioned how mobile financial services via agent banking through leveraging mobile phones can help address the financial service access gap for this group (Ouma et al. 2017). Furthermore, another form of mobile financial services is a mobile wallet described as an m-wallet by Karjaluoto et al. (2019). It is described as a digital form of the ordinary wallet installed as an app on the mobile phone to save mobile money. It mitigates cash handling risks and fraud and seeks to improve the financial habits of the user (Tun 2020). While also describing mobile financial services in the context of mobile banking, the authors did not limit it to only bank customers like the previous authors but highlighted the opportunity it presents to access financial services via phone through ownership of virtual bank accounts (Abdinoor and Mbamba 2017). Mobile financial services is a broad term used to describe mobile banking, mobile money transfer, and mobile payment. Mobile banking is using mobile phones through SMS, banking applications, mobile browsers, or Unified Supplementary Service Code (USSD) to conduct a banking transaction (Sharma and Al-Muharrami 2018; Obaid et al. 2019). While mobile banking provides an additional banking channel to new customers, mobile money makes financial services access possible for the underserved. Mobile payment enables person-to-business transactions at a point of sale or remotely. Mobile financial services have a benefit for the underserved and the service provider (Gupta and Dhingra 2022). Another paper simply describes mobile financial services as innovative products made possible by fintech, which helped build resilience during the COVID-19 pandemic. It is banking services mediated by the

mobile network and can be accessed through channels like contactless (Yan et al. 2021).

Mobile banking has also been used as a term to describe an alternative channel to electronic banking otherwise called e-banking, which when delivered via mobile phone networks and performed on a mobile phone is referred to as mobile financial services (Al-Dmour et al. 2020; Ahmad et al. 2020; Ho et al. 2020). In countries like Kenya, Mozambique, and Nigeria, mobile financial services were manifested in the form of mobile money services, where the initial focus was to use the mobile phone as a means of providing money services like cash transfers and remittances (Agur et al. 2020; Fernandes et al. 2021; Mpofu and Mhlanga 2022). Furthermore, payments for goods, services, and bills authorised, initiated, or realised with a mobile phone are described as mobile payment services, which has been used to describe mobile financial services with a focus on payments (Choi et al. 2020; Gong et al. 2020; Lian and Li 2021).

Based on the preceding, mobile financial services can be described as the use of a mobile phone to provide banking, money, or payment services to various customer segments based on their needs. The definition describes three broad components of mobile financial services: mobile payment services, mobile banking services, and mobile money services (David-West et al. 2020; Humbani and Wiese 2018; Kang 2018).

The analysis of the literature reviewed shows that mobile financial services broadly described three main financial services offered by the use of the mobile phone, either directly at the point of sale, remotely, or through proximity channels like contactless. The three variants of mobile financial services include mobile banking, mobile payments, and mobile money. Mobile financial services is deployed via apps on the mobile phone. The characteristics of mobile financial services that made it a preferred choice are speed, lower cost, reduced risks of cash handling, and perceived security when compared to the traditional means of banking.

### 2.1.2 Defining Mobile Financial Services – Fintech, Neobanks, and Challenger Banks

Technological innovation has led to the emergence of new models for financial services delivery that have disrupted conventional banking as it is known. These new models leverage the mobile phone to enable financial services access to customers. The global financial crisis of 2008 changed the general perception that the bigger a

bank, the safer it was. Moreover, entrepreneurs, leveraging the ubiquitousness of the mobile phone and the internet, entered the financial services space, developing new models that would enable financial services to reach customers in a more cost-effective and user-friendly manner. This new model was called fintech. The term fintech has various definitions. However, the definition by the Financial Stability Board (FSB) has been widely adopted. FSB defines fintech as "technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions, and the provision of financial services." (Agarwal and Zhang 2020; Thakor 2020). While definitions differ, authors agree that fintech focuses on existing and new customer segments. They leverage the mobile phone and value-addition in financial services. They enable non-traditional players to provide financial services and they present opportunities and risks for customers and the financial services industry (Guild 2017; Kang 2018; Takeda and Ito 2021; Murinde et al. 2022). Describing the link between fintech and mobile financial services, mobile financial services were described as a tool for fintech and can be in the form of mobile money, mobile banking, mobile payment, and e-wallet, and was also described as mobile fintech payment (Guild 2017; Kang 2018; Takeda and Ito 2021). The mobile payment infrastructure is central to the fintech ecosystem (Kang 2018).

Fintech has led to the emergence of models like neobanks and challenger banks which are bank-like non-traditional financial services providers that provide financial services via mobile apps, leveraging innovation to reach new customer segments (Bradford 2020). While challenger banks are chartered, neobanks are not chartered. However, both leverage fintech to provide financial services and are platform-centric financial services entities as against product-centric traditional financial service providers like the bank (Bradford 2020; Temelkov 2020). Neobanks and challenger banks are built exclusively for smartphones, which means they can only be accessed via a mobile device and provide a promise of security via biometric and other technical cybersecurity countermeasures available for the mobile phone environment (Lu 2017). Neobanks have also been simply described as fintech (Koibichuk 2021). This study examined the relationship between mobile financial services, fintech and its variants.

Mobile financial services is the primary tool used to access fintech-based financial services. Neobanks, challenger banks, and traditional banks all leverage fintech to reach their customers. To that effect, addressing cybersecurity in mobile financial services would benefit banks, fintech, neobanks, and challenger banks.

The review of literature in this section shows that the end-users leverage the mobile phone as the primary platform to access financial services through mobile financial services. Various MFS products and services are available to meet the needs of the different segments of the market, from those who do not have access to formal banking services to those requiring an alternative banking channel and those looking for a convenient and secure means of paying for goods and services. The next section of this study examines the adoption study of mobile financial services, in light of the benefits it presents.

## 2.2 MOBILE FINANCIAL SERVICES ADOPTION

Mobile financial services present an opportunity for users to access suitable financial services through innovative models. However, adoption has not been impressive (Lema 2017). This section examined mobile financial services adoption literature to understand factors affecting the adoption of mobile financial services, despite the benefits it portends.

A study conducted among 250 underserved participants, leveraging the six variables of the Technology Adoption Model (TAM), revealed that user perception of cost, social influence, and usefulness significantly influence the adoption of mobile financial services amongst the underserved (Lema 2017). Furthermore, the study reveals a significant correlation between trust and adoption (Lema 2017). The study further highlights the negative correlation between the perception of trust and the perception of risks. It also shows the positive correlation between the perception of trust and the perception of social influence. The author then opined that the perception of risks impedes users' trust in mobile financial services (Lema 2017). While the study provides some insight into factors that facilitate the adoption of mobile financial services, the authors reported that the perception of risks has no significant influence on adoption, based on data from their study, and they also highlighted that the finding was not consistent with other findings where the perception of risks was identified as significant. Similarly, citing limited studies on user attitudes and behaviours and their impact on MFS adoption, a study of 196 respondents adopted a mixed-method approach and integrated the TAM and the Innovation Resistance Theory (IRT) models. The study opined that perceived usefulness, ease of use, and trust influence the adoption of MFS. The study noted fear of fraud, complexity and cost as other barriers inhibiting the adoption of MFS. Also, the study recommended further examination of the difference between usage intention and actual behaviour as it affects MFS adoption (Himel et al. 2021). In the same vein, a systematic literature review of 118 MFS adoption studies was conducted. The authors noted that TAM and the Unified Theory of Acceptance and Use of Technology (UTAUT) are the most

predominant technology adoption models used in the study of MFS adoption. The study identified six adoption factors for MFS. They include cognitive-based factors, emotional-related factors, trust-related factors, risk-related factors, influence-related factors, and consumer-based factors (Gupta and Dhingra 2022).

To have a consolidated view of factors affecting mobile financial services adoption, a systematic literature review of 24 empirical studies on the TAM model for mobile financial services adoption was conducted (Gbongli 2022). The author highlighted models that were applied in research to examine factors that drive mobile financial services adoption, including theory of reasoned action (TRA), technology acceptance model (TAM), unified theory of acceptance and use of technology (UTAUT), and theory of planned behaviour (TPB) (Gbongli 2022). The author asserted that TAM was the most widely used model for examining technology adoption due to its adaptability amongst other characteristics. The author identified perceived security as the highest factor that affects mobile financial services adoption as it has a frequency of seven based on the data from the systematic review. Trust (5) and Risk (4) are among the top variables that affect mobile financial services adoption (Gbongli 2022). The impact of security on mobile financial services adoption was highlighted in a study by (Johnson et al. 2018). Consumers are willing to use MFS but need more unified standards. Security and privacy concerns are critical barriers to MFS adoption. Furthermore, literature has identified a lack of trust in MFS as a result of cybersecurity concerns, a significant factor hindering the adoption of MFS (Mohamed 2019; Dzidzah et al. 2020; Yan et al. 2021).

This section examined mobile financial services adoption literacy and identified key factors that drive adoption. Some of these factors include perception of security, perception of risks, and perception of trust. The next section examined the nature of trust in mobile financial services.

### 2.2.1 Trust in Mobile Financial Services

The literature reviewed in section 2.2 highlighted how the perception of security concerns leads to a lack of trust in mobile financial services, which has slowed down the adoption of the solution. This section examined the nature of trust in mobile financial services. Evidence from studies reveals that MFS witnessed slow global adoption due to a high level of security concerns (Asatryan 2017; Marous 2018). This lack of trust is not unfounded, considering that several vulnerabilities and fraudulent attempts on MFS have succeeded, as presented in the section (Alderman 2021; Lokanan and Liu 2021; Lokanan and Sharma 2022). The primary reasons for this lack

of trust stemmed from increased reported vulnerabilities in mobile applications, and mobile phone-based reported fraud.

A study on trust by Gaehtgens et al. (2017) found that though trust is pivotal to human interaction, traditional trust models could not be the best fit for digital businesses. The research distinguished conventional trust models from digital trust models. Furthermore, the study found that conventional trust differs from digital trust in three ways as follows:

i. Traditional trust depends on persons or institutions to act as agents in certain circumstances, while things and algorithms act as brokers in digital trust.
ii. While conventional trust often focuses on a trust relationship between 2 specific parties, digital trust depends on an exponentially growing trust relationship in a chain of trust: and
iii. Traditional trust depends on establishing an initial trust relationship between trusted entities, while digital trust is rapid and dynamic (Gaehtgens et al. 2017).

Furthermore, Morgan and Moyer (2017) maintained that the current trust model, which is based on acceptance, is unsustainable. They believed transparent verification is a more sustainable paradigm of trust as it would help to quickly identify problems and opportunities in complex systems like digital businesses (Morgan and Moyer 2017).

To address the identified trust gap, various models have been proposed. White and Oestreich (2017) proposed a risk-based model for trust management, which categorises trust into six levels based on how the trust was observed in data. These categories of trust help in determining the level of reliability of data. A theoretical model for examining consumer trust in e-commerce with a focus on consumer-generated media has also been proposed. The model examined the consequence of trust on CGM through a survey of 401 participants, analysed through the Structural Equational Model (SEM).

To address observed gaps in trust research, a study by Joo and Han (2021) proposed a decentralised trust model where each “rational agent” is responsible for its trust mechanism. Furthermore, in a study of 318 participants, to examine the nature of distributed trust in a blockchain-based product, the author identified transparency, traceability, and security as key determinants of distributed trust (Joo and Han 2021).

Trust is a complex construct that has an element of risk and expectation. Lack of trust can occur when these risks are not well managed or when the expectations are not met; conversely, addressing risk promptly and meeting consistent expectations can enhance trust (i2i 2017). The paper posited that trust has two sources and three building blocks: predictability, acting in consumers' interests, and recourse mechanisms to help build or erode trust (i2i 2017). Another study examined trust mechanisms that can address cybersecurity problems in sensor-cloud systems (SCS). The study proposed a trust model that can facilitate subsystem trust (Wang et al.2020).

Other literature focused on trust measurement. For instance, in a study on how to measure trust in an autonomous system, to improve human and system interaction, thirty measures of trust that can be applied were highlighted. The measures were grouped into self-reporting measures where respondents self-report their behaviours, beliefs, attitudes, or intentions; behavioural, where participants and their tendencies were observed; and physiological, where biological responses are captured. Furthermore, the study opined that to improve trust measurement, constructs that have face validity should be used. It also recommended that experiments to measure trust should be contextualised within trust models. Similarly, they recommended the need to understand what the measurement seeks to capture (Kohn et al. 2021). In another conceptual study that examined the attribute of trust assessment in automation, the author noted that certain attributes in human trust are transferable to trust assessment in autonomation and can be useful in improving trust by providing attributes that can improve trust between humans and autonomation (Sheridan 2019). Trust measurement studies were also conducted in other domains. For instance, trust in social networks was also examined (Ruan et al. 2017). In the healthcare domain, trust measurement in vaccination was examined (Larson et al. 2018). These studies provide various perspectives on trust in systems and the interaction of humans and systems. Based on the MFS adoption studies examined, it was important to examine the nature of trust and how it affects MFS adoption. The literature review has provided insight into the nature of trust from other domains and how they apply to MFS. Another important conversation in literature is zero trust model and its implication on MFS adoption. The zero-trust model is based on the concept of continuous verification, irrespective of if the trust entity is internal or external to the trust domain. The proponents of zero trust advocate the model to address trust issues related to the rapidly evolving technology landscape (He et al. 2022). While the adoption of zero trust would improve security in a system, it is likely to have a negative impact on MFS adoption. The need to continuously verify might add to MFS complexity, cost,

cognitive workload and other technology adoption factors driving MFS adoption (Gupta and Dhingra 2022). There is therefore a need to balance zero trust in MFS with technology adoption factors.

The first two sections of the literature review examined mobile financial services and various adoption theories that enable their uptake with a more in-depth review of trust due to its pivotal impact on cybersecurity and the adoption factor. The next section will examine the architecture of the mobile phone as a prelude to exploring the threat landscape for mobile financial services.

## 2.3 MOBILE FINANCIAL SERVICES BASE ARCHITECTURE OVERVIEW

The implementation of usable security heuristics for a mobile financial service application is fundamentally dependent on the base architecture of the physical hardware components provisioned on the host mobile device. Consequently, this section presents the high-level architecture and hardware provisions of a typical smartphone device. The section expresses the minimum hardware components that a mobile smartphone must be equipped with to deliver the expressed functional, non-functional, and technical requirements as contained in the business requirements document.

### 2.3.1 Base Architecture of a Smartphone

At a high level, the base architecture of a typical smartphone device is under consideration for the implementation of cybersecurity solutions for mobile financial services.

Table 2.1 provides overview descriptions of the hardware and logical software components of a candidate smartphone device required for the implementation of the envisaged MFS application.

| S/N | Component Type | Component | Description |
|---|---|---|---|
| **1.** | Base Hardware | System-on-a-Chip (SoC) | This is the most important hardware part of a smartphone, and it comprises an integrated component module, herein referred to as "*SoC components*" that provides the core functionalities of a smartphone. |
| **2.** | SoC Component | Central Processing Unit (CPU) | This is the most important component of the SoC and indeed of a mobile phone device. It is responsible for all the processing and computations that facilitate the overall operations of a smartphone device. |

| S/N | Component Type | Component | Description |
|---|---|---|---|
| **3.** | SoC Component | Graphics Processing Unit (GPU) | This component is responsible for the drawing and rendering of the graphical user interface on a smartphone device. It processes the impulses from the physical interactions between the end-user and the smartphone device. |
| **4.** | SoC Component | Image Processing Unit (IMU) | This component is responsible for the conversion of visual data extracted from the camera component of a smartphone device into video and image files. |
| **5.** | SoC Component | Digital Signal Processor (DSP) | This is a specialised component of a smartphone device that is responsible for the handling of digital impulses that enable image processing, telecommunications, speech recognition, and audio signals among others. |
| **6.** | SoC Component | Neural Processing Unit (NPU) | This specialised component enables the capability of a smartphone device to support advanced computation and analysis that fosters machine learning and artificial intelligence operations such as voice recognition, facial recognition, and camera object segmentation. It is otherwise referred to as the “Intelligent Processing Unit (IPU)”. |
| **7.** | SoC Connectivity Component | Modem | This component enables the ability of a smartphone device to connect to wireless signals such as Wi-Fi, Bluetooth, and Near-Field Communication (NFC). |
| **8.** | Sensory Hardware | Gyroscope & other sensors | This set of sensory components enables the capability of a smartphone device to detect and measure motion attributes of the device. These components, in conjunction with the NPU, can enable behavioural biometric capabilities on a smartphone device, which enables it to detect the identity of an end-user based on the general handling of and interaction with the smartphone device. |
| **9.** | Biometric Hardware | Fingerprint scanner | Unlike behavioural biometrics, this component enables the capturing and verification of the physical biometrics of an end-user of a smartphone device. |

| S/N | Component Type | Component | Description |
|---|---|---|---|
| **10.** | Storage & Extension Hardware | Memory and SIM card modules | This set of components enables a smartphone device to increase its capacity for data storage and enhance its capability for connectivity with cellular network protocols. |

Table 2.1: Hardware and Logical Software Components of a Smartphone (STA 2018; Sommerhalder 2023; BIS 2023)

### 2.3.2 Base Architecture of a Tamper-Resistant Smartphone

To deliver an MFS application that is secure, the host environment, that is the mobile smartphone, must provide components that foster physical and cyber protection of the device and its constituent data stores. There are two approaches for achieving a tamper-resistant architecture of a mobile device, each offering varying degrees of protection and security. These approaches are:

i. Hardware-based tamper-resistant architecture, and
ii. Software-based tamper-resistant architecture.

While hardware-based tamper-resistant architecture offers a greater security assurance, software-based tamper-resistant architecture is desired for its "*flex-responsiveness*" — the flexible and responsive abilities to meet and address the ever-changing cybersecurity demands and concerns. However, to achieve the best of both options, several architecture implementations combine these approaches to deliver mobile solutions with assured protection of hardware security and the agility of cryptography-based software security (STA 2018; Sommerhalder 2023; BIS 2023).

Based on the foregoing, the following are the three options that are available for the delivery of a usable security heuristic for MFS applications:

i. Hardware-based secure elements (HSE)
ii. Trusted execution environment (TEE)
iii. Cryptography-based Secure Software (CSS)

i. Hardware-based Secure Elements (HSE)

Hardware-based secure elements are hardware chips that are designed to protect against unauthorised access to sensitive information on a mobile device. They have the advantage that they are pre-installed with applications, through which authorisation is granted to only trusted external applications to manipulate and process their constituent data/information. HSEs offer the highest level of security and protection for data/information stored on a mobile device. They deal very well with sophisticated cyber threats such as side-channel attacks and could be

provisioned on a mobile smartphone as an embedded chip or extension hardware such as a SIM card (STA 2018; Sommerhalder 2023; BIS 2023).

ii. Trusted Execution Environments (TEEs)

Like HSEs, a TEE is also a hardware-based implementation of secure processing and data stores on a mobile smartphone device. They are typically implemented as part of the microprocessor and derive operational support from the operating system (OS). A TEE allows software applications that are installed on the smartphone to execute code, process, and store data safely and securely in an isolated area on the hardware while preventing other system processes and applications from viewing, accessing, manipulating, or reporting stored data/information.

TEE-based mobile applications typically rely on other services, processes, and applications in the physical host environment to offer tamper-resistant capability. A TEE-based application can assess the integrity of the host environment for vulnerabilities such as rooting or jailbreaking. TEEs offer better functionalities than HSEs. However, they suffer from a lower security assurance than HSEs (STA 2018; Sommerhalder 2023; BIS 2023).

iii. Cryptography-based Secure Software (CSS)

This is the only software-based architecture approach and typically relies on the deployment of cryptographic keys to guarantee optimal protection of the application and its constituent data/information. Unlike, HSE and TSS-based architectures, cryptography-based secure software (CSS) does not require specialised hardware components to operate. For this reason, they are considered to offer the least grade of tamper resistance to both physical and remote security attacks. However, they offer the most flexibility in their ability to respond to the ever-changing dynamics of cyber security concerns (STA 2018; Sommerhalder 2023; BIS 2023).

The next section examines the threat landscape that seeks to exploit the MFS architecture.

## 2.4 MOBILE FINANCIAL SERVICES THREAT LANDSCAPE

Mobile financial transactions are a secondary risk of growing electronic fraud and cybersecurity concerns (Ambore et al. 2017; Rizzo 2018). Examining the threat landscape would provide a better understanding of the vulnerability that could be exploited in the system. Furthermore, an analysis of the threat landscape would provide a basis for developing a fit-for-purpose approach to addressing cybersecurity challenges in mobile financial services. Threat modelling is central to proactive cybersecurity defence and countermeasure implementation. It presents a systematic approach to defensively analysing vulnerabilities. Threat modelling methodologies

are used to conceptualise profiles of potential attacks, including their goals and threats, in such a way that the threat can be catalogued (Shevchenko et al. 2018; Balamurugan et al. 2023). They include **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial of Service, and **E**levation of Privilege (STRIDE); **P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis (PASTA); The **O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation (OCTAVE); **L**inkability, **I**dentifiability, **N**on-Repudiation, **D**etectability, **D**isclosure of Information, **U**nawareness, **N**on-Compliance (LINDDUN); and Attack Trees (Shevchenko et al. 2018; Balamurugan et al. 2023).

These models provide a theoretical framework for threat analysis for mobile financial services in this thesis. The insight from this study was helpful in analysis of mobile financial services literature to gain an understanding of its threat landscape.

### 2.4.2 Mobile Financial Services Threat Landscape - Technology

This section and the next present threat landscape analysis for the mobile financial services landscape. While this section focuses on technology threats, the next section focuses on threats related to the human element.

The technology threat landscape analysis conducted addressed four main technology-related areas as follows:

i. Secure MFS App Development Process and Practice

The two major mobile phone operating systems, Apple iOS and Android, have provided resources to facilitate a secure development process amongst their developer communities. Lack of adherence to laid down practices can lead to vulnerable mobile financial services solutions. For instance, iOS provides Xcode, an integrated development environment, code signing capability, and developer sign-in and gateway. Furthermore, API for the development of cryptographic interfaces exists. Any vulnerability in the API can lead to a concern in the system. Patch management and secure development practices are also vectors that affect cybersecurity in the development of mobile financial services (Android 2023a; Apple 2023).

ii. Authentication

Secure access to mobile phones has metamorphosed over the years, from a 4-digit passcode to a 6-digit passcode, making brute force attacks harder. In addition to the touch authentication option, various biometric authentication capabilities have also been developed, such as facial recognition. Others in this category are secure

authorisation, access control processes, and multi-factor authentication (Apple 2023; Android 2023a; Ferrag et al. 2020).

iii. Mobile OS and Device Security

In addition to the operating system (OS) components of the mobile devices, other key components of the mobile device can be vulnerable to cyber-attacks. Some of these components have been highlighted in section 2.3 of this thesis. They include the secure element which hosts sensitive applications and data, and the trusted execution environment which protects sensitive data and authorised software. Some of the areas affect malware detection and prevention, mobile device integrity, and tamper resistance (Android 2023b,; Li et al. 2019; Pinto et al. 2017).

iv. Data Protection

Mechanisms for protecting against man-in-the-middle attacks and eavesdropping are essential for data security. In addition to strong encryption algorithms, secure communication protocols are also necessary for the secure transmission of data. (Wang et al. 2019).

v. Transaction and Session Security

Risk assessment and real-time monitoring capabilities are necessary for ensuring session and transaction security. This coupled with fraud detection and prevention techniques, and secure verification and integrity mechanisms, are meant to strengthen transaction security (Kumari et al. 2017). Some attacks on transactions have exploited the limitations of the network protocols; Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS) (Kadena and Gupi 2021).

Analysis of literature along these five dimensions of the mobile financial services technology threat landscape revealed that counterfeiting of mobile phones and components presents a vulnerability to MFS. International Mobile Equipment Identity (IMEI) number provides information about the phone's country of origin, manufacturer, etc. This number can be reset by counterfeiters who might resell the phone. Over 180 million counterfeit phones are traded globally every year (Yaacoub 2019). The change in IMEI makes it impossible for mobile network operators (MNO) to apply correct settings remotely to a phone, as such a phone may not work effectively on the network, affecting MFS services (Perlman 2017). At the MNO end, infrastructure vulnerability like Unstructured Supplementary Service Data (USSD) makes MFS vulnerable to cyber-attacks (Lamoyero and Fajana 2023).

Furthermore, Stone et al. (2017) published research that claimed an implementation flaw in MFS solutions in HSBC, NatWest, Co-op, Santander, and Allied Irish Bank leaves the banking credentials of millions of users vulnerable to cybercriminals. Another study of mobile financial services also revealed 2,157 vulnerabilities in 693 solutions across 83 countries. Some of the identified vulnerabilities are related to outdated apps and third-party libraries (Chen et al. 2020).

The vulnerability could allow an attacker to hack into a network, intercept a Secure Sockets Layer (SSL) connection, retrieve banking credentials, and log details of unsuspecting customers. Incidents of customer financial loss due to cyberattacks on MFS have also been reported. For instance, a cybercrime gang had stolen over $900,000 before being arrested after infecting over 1 million mobile phones with banking trojans (Khandelwal 2017b). These concerns affect MFS users and the entire MFS ecosystem. More recent studies from various continents have also highlighted cybersecurity concerns in mobile financial services (Nambiro et al. 2020; Wodo et al. 2021; Ghelani et al. 2022)

Users of mobile financial services have security concerns in the use of the solution (Kishnani et al. 2022). Most service providers along the value chain want a piece of user data to enable them to analyse current use and improve future products. Also, mobile financial services still depend on sensitive information collected from users (Kishnani et al. 2022). The rush to release mobile applications also results in MFS applications not being adequately tested, thus increasing vulnerability to cyber-attacks (Ambore et al. 2017). The presence of rogue mobile apps and the ability of phone users to sideload—install a mobile application from unauthorised sources—have presented additional security challenges for mobile financial services users (Ambore et al. 2017).

Moreover, connections for MFS transactions and some technologies used are susceptible to cyber-attacks. Connection via public WI-FI can provide a window for cyber-attack (Rossi 2023). Mobile money still uses vulnerable technologies like USSD and SMS as the primary technologies to perform transactions, which can be exploited for cybercrime (Perlman 2017).

While existing technical countermeasures have helped in mitigating some security challenges, some weaknesses have been observed and more technical countermeasures proposed. For instance, citing a gap in existing technical countermeasures, a technical solution that can help detect malware-initiated transactions and legitimate ones has been proposed (Leguesse et al. 2021).

Suffice it to note that while technical countermeasures provide some reprieve, their effectiveness may vary depending on various factors, such as implementation, configuration, and human-related factors. For instance, the angle of consumer privacy concerns in mobile financial transactions and its impact on transaction security was brought to the fore (Chatterjee et al 2023). Furthermore, Seo and Park (2018) in their work highlighted the role of key stakeholders in the ecosystem in ensuring the security of financial transactions, specifically highlighting the manufacturers, banks, service providers, and users.

### 2.4.3 Mobile Financial Services Threat Landscape – Human Factors

The security of a system ultimately rests on the human factor in the cybersecurity ecosystem more than it does on technical controls and countermeasures (Benson et al. 2019). Human factors have been defined by the International Ergonomics Association as the scientific discipline focused on the understanding of the interaction among humans and elements of a system (Desolda et al. 2021). This section analyses the literature on the human factor of the mobile financial services threat landscape and its impact on cybersecurity.

There has been an emphasis on the development and implementation of technical solutions for cybersecurity. However, the overall effectiveness of these cybersecurity measures has been increasingly called into question. One notable critique is that cybersecurity designers often focus heavily on technical countermeasures while neglecting the diverse perceptions, knowledge, experiences, and risk awareness of users, which significantly influence behaviour. This oversight is underscored by the fact that human vulnerabilities account for 80% of exploited vulnerabilities and are implicated in 82% of data breach incidents (Gobler et al. 2021; Furnell 2024). Despite the significant impact of these human vulnerabilities, it is critical to recognise that users are not necessarily the "weakest link" in cybersecurity. Rather, the challenge lies in the disconnection between users and security systems, as well as the lack of emphasis on the principles of usable security. Indeed, addressing the human factor can significantly enhance the effectiveness of cybersecurity measures (Gobler et al. 2021). The actions and behaviours of the human element can lead to exploitable vulnerabilities. Buttressing the importance of the human factors in cybersecurity, Benson et al., (2019) opined that there was a consensus among cybersecurity professionals that security depends on people more than on technical controls and countermeasures (Benson et al. 2019; Kadena and Gupi 2021). Further analysing the reason for breaches, Verizon (2018) reported that 73% of breaches were perpetrated by human elements external to the system, while 28% involved insiders. Unpatched

systems have also led to cybersecurity vulnerabilities. For instance, it was reported that 330000 FortiGate firewalls were vulnerable to a critical security flaw affecting Fortinet devices due to a lack of updated patches. This vulnerability could allow an attacker to remotely execute code or commands to exploit the vulnerability (Lakshmanan 2023a). Similarly, it was reported that about 200,000 WordPress websites are at risk of attacks due to a lack of up-to-date patching (Lakshmanan 2023b).

Furthermore, attack vectors exploited in the human factor include the human target's fear, errors of end-users, administrators or developers, lack of awareness, and information asymmetry. Cybercriminals use this pathway to gain unauthorised access, obtain credentials, and infect the system with malware. The malware is then propagated through downloads or phishing attacks (Kadena and Gupi 2021). A secure system depends on the human user, administrator, or developer doing the right thing (Desolda et al. 2021). Drawing from the aviation domain, some issues that could lead to human factor vulnerabilities include lack of communication, complacency, lack of knowledge, distraction, fatigue, pressure, lack of awareness, and norm. (Desolda et al. 2021). Other highlighted human factor vulnerabilities include online fraud, distributed denial of service (DDoS), drive-by downloads, and social engineering attacks (Pollini et al. 2022). Others include privacy perception, trust perception, behaviour, and capability (Rohan et al. 2021a). It was noted that the human factor is complex and often overlooked. To address the human factor gap in cybersecurity research, the authors asserted that human factor methodologies should be integrated into the system development process. They also proposed that user behaviours that lead to security risks should be investigated, and mobile financial solutions should focus more on addressing these behaviours than technical problems (Desolda et al. 2021).

In a systematic literature review of 27 studies that was carried out to understand the attention given by the computer science research community to the human factor in cybersecurity, it was found that human factor literature highlights two types of user; experts and non-experts. While qualitative, quantitative, and mixed methods were used in the examined studies, qualitative methods were the most used in the literature (Rohan et al. 2021b). The authors identified cultural bias as a challenge in the sample collected as most studies are focused on the US and Europe. It was also noted that the measurement of the perception of cybersecurity of users poses a unique challenge. Furthermore, the authors noted that future research should consider human factors as a solution rather than the problem. While identifying user, system, and usability as the three pillars of cybersecurity, the paper recommended that more

studies on the usability aspect need to be conducted with care given to the balance with security (Rohan et al. 2021b).

## 2.5 ADDRESSING THE HUMAN FACTOR CHALLENGE IN MOBILE FINANCIAL SERVICES

The literature reviewed in the previous section identified the following research gaps with the human factor in cybersecurity:

- Human factor is a complex problem.
- User behaviours that lead to cyber-attacks need to be examined to address them.
- Cultural bias exists in human factor data that needs to be addressed.
- The measurement of the perception of cybersecurity for end-users is crucial in addressing it.
- The human factor is most often identified as the problem but should be viewed as the solution.
- More study on usability with a focus on balancing with security is required to address the human factor challenge.

Human factor approaches have been applied to address technical cybersecurity problems. For instance, usability evaluation was applied to address key management challenges in Bitcoin (Eskandari et al. 2018). Similarly, a usability analysis of Java Secure Socket Extension (JSSE) API was conducted to identify usability issues (Wijayarathna and Arachchilage 2019). Human factor techniques have also been applied to address authentication problems (Liu et al. 2017).

Most of the studies conducted on addressing human factor challenges in cybersecurity focus on evaluation through user or expert reviews. Heuristics evaluation has also been deployed to evaluate usability problem (Naqvi and Seffah 2018; Kumar et al. 2020; Reuter et al. 2022; Gutfleisch et al. 2022).

A significant number of human factor literature focuses on addressing usability and security. The next section focuses on analysing usable security studies and how they can be leveraged to address cybersecurity problems in mobile financial services. Specifically, the section examined the nature of usable security problems in MFS and who it affects. It also sought to provide insights into current practices in addressing usable security problems and their potential applications in MFS.

## 2.6 USABLE SECURITY

Usable security exists at the intersection of human behaviour and cybersecurity. It was acknowledged within the Cyber Security Body of Knowledge, which dedicates a key pillar of the knowledge area to human factors, with usable security as a central component. Usable security encompasses the design and implementation of cybersecurity measures that account for users' behaviours, knowledge, experiences, and cognitive ability as well as environmental factors. The primary objective of usable security is to enhance the effectiveness of cybersecurity solutions by mitigating vulnerabilities that arise from user-related issues (Nocera et al., 2023; Furnell, 2024). However, several research challenges persist in this domain. These include the absence of comprehensive design guidelines that address user behaviour, the lack of explicit requirements for usable security, and the need for standardised documentation and guidelines to support the development of usable security frameworks (Nocera et al. 2023).

### 2.6.1 The Nature of Usable Security

Studies have been conducted to understand why usable security has not worked for end-users. The need to involve users was identified as essential for aligning user needs and security objectives. An approach for how user feedback would be incorporated into security design was also proposed (Lead 2020). Similarly, the need for the consideration of user behaviour to improve usable security for users was identified. For instance, in a study that examined factors impeding the adoption of two-factor authentication, it was opined that usable security mechanisms should not introduce additional complexity for users. The study proposed a study of user behaviours to facilitate a better adoption of security mechanisms by users (Das et al. 2018). In a similar study that investigated the usability of secure passwords, a study of user interaction with security mechanisms was proposed as a means of identifying variables that will make security measures more acceptable to end-users. Furthermore, it was also asserted that to improve usable security, it is imperative to build a system that aligns security design to users' mental model of use of technology (Grobler et al. 2021). To provide the necessary insights needed to address usable security issues, a study that would provide empirical data on user attributes and contextual factors and how they affect their security behaviours was recommended (Grobler et al. 2021, Alt and Von 2019).

In highlighting the need for usable security for users, it has been noted that users have various levels of experience and knowledge that impact their right use of security mechanisms in MFS. The nature of the mobile device, consideration for demographic

peculiarity for diverse groups of users, and accessibility needs are key in inclusive security design (Jain et al. 2021, Zhou et al. 2019, Ndibwile et al. 2019).

While it is important to address the usable security concerns of end-users, it has been opined that it is also important to examine the usable security practices of developers who design the system. It has been found that most usable security studies have focused on end-users and little effort is made to examine the impact of usable security on developers which ultimately reflects itself in poor considerations for usable security to the detriment of the end-users. To that effect, the need to investigate developers' experience with usable security was proposed. For instance, a study also observed that developers might lack good understanding of security practices, which makes them develop systems without proper integration of security controls. The study recommended an approach that will better guide developers on security practices and how best they can be integrated into a system (Naiakshina et al. 2017). Delivery of solutions promptly is essential to a developer's work. However, developers tend to overlook usable security principles and prioritise functionality above security when developing systems. Integrating usable security early in the development lifecycle and improving usable security awareness for developers was recommended (Gutfleisch et al. 2022). Furthermore, developers do not have a sufficient understanding of user behaviour, and this might lead to building security mechanisms that might not be effective due to cognitive overload or misalignment of the developer's intention and the user's eventual experience. While some studies on user behaviours have been conducted, they do not provide actionable insight for developers. Another study has identified limited guidance on usable security for developers as a key usable security concern. The study noted that developers mainly rely on UX principles which might not necessarily address usable security challenges. It went on to opine that a framework that integrates human-computer interaction (HCI) and security elements is required, and proposed a set of usable security guidelines for developers that will incorporate usable security elements that impact end-users (Wiefling et al. 2020). Other usable security issues that affect developers include the complexity of security API, the lack of a mechanism to evaluate the usable security effectiveness of a system, and the difficulty in complying with complex regulatory requirements (Lead 2020).

In their study on this debate, Lennartsson et al. (2021) posited that usability should be addressed in the context of security, and went on to propose fourteen factors believed to be solution-agnostic and generally applicable to addressing usability in the context of security. The study identified the need to have a deeper analysis of

these factors and how they can mitigate usable security trade-offs (Lennartsson et al. 2021).

The need to focus on human behaviours in addressing functional security problems was buttressed by (West cited by Algarn and Chan 2017), where they posited that a better understanding of why users make lousy security decisions, and their cognitive limitations, would help developers better develop usable security interfaces. The requirement for usable security is also a problematic area as most studies simply merge usability and security requirements without a rigorous process of analysing the problem space (Feth and Polst 2019).

### 2.6.2 Addressing Usable Security Challenges

Both users and developers are confronted with usable security challenges. While some of these challenges have been identified and enumerated, the need for an empirical study of both user and developers' usable security behaviours was recommended. Furthermore, the need for a guideline that can integrate usable security into a system and an approach to evaluate usable security was proposed (Feth and Polst 2019).

Addressing usable security concerns presents a challenge that affects both the end-user and the developer and affects the efficacy of cybersecurity measures. Studies have been conducted on how best to address usable security concerns for end-users and developers. One such study proposed the adoption of security-by-design where usable security is integrated into system design early in the development lifecycle. This approach enables a more thoughtful integration of usable security principles during system development and addresses the concern of just fitting in security. While this approach helps in addressing this challenge, it requires developers to have good knowledge of usable security and also puts more constraints on scarce development time (Niekerk 2022).

The active participation of end-users throughout the development lifecycle makes it possible for developers to have a better understanding of their needs, behaviours, and even goals through a user-centred design approach. This model makes it possible to minimise user-related errors and makes security mechanisms more suitable to users' cognitive ability and task goals. However, this approach will add to development time and require users to understand the security implications of their actions which might not be always feasible (Feth and Polst 2017). A similar approach is to provide a proportionate security solution based on user risk profile. This approach ensures provision of security measures relevant to user risk appetite.

However, users can overlook security settings when they become too flexible (Wiefling et al. 2020).

Furthermore, heuristics evaluation has been used to evaluate usability and security flaws in a system. This method provides a systematic approach to assessing usable security and helps in the timely detection of usable security problems. The process involves the development of a set of usable security heuristics to guide developers in designing more secure applications. These heuristics are then refined through multiple iterations and validated by expert reviews (Quiñones and Rusu 2017).

While adopting a user-centred approach and security-by-design provides a means for integrating usable security into systems development, heuristics offer a structured and flexible approach for incorporating usable security into system design and help with the quick identification of usable security issues. User-centred design and security-by-design approaches require significant user involvement and can be time-consuming. The nature of heuristics enables the developer to address usable security without developing new criteria for every system. Heuristics are also cost-effective when compared to other approaches and they can be applied across a wide variety of contexts. Also, it has been asserted that heuristics adopts a balanced approach that can easily adapt to new security threats when compared to other approaches to addressing usable security (Niekerk 2022, Wiefling et al. 2020, Feth and Polst 2017). This section has highlighted the relationship between usable security and cybersecurity. It examined the nature of usable security problems, and current approaches to addressing these problems. The next section sought to examine how heuristics can be used as an approach to addressing usable security problems, based on the benefits it holds above other methods based on insight from literature.

## 2.7 HEURISTICS IN USABLE SECURITY

Decision-making in systems design seeks to address the problem from the viewpoint that activities and their interrelationship are linear and measurable (Gorod et al. 2017). This traditional approach is not well suited for an environment with a complex relationship between entities requiring decisions to be made within a limited time and computational power. While not discarding the advantage of optimisation, where decisions are taken based on a complete analysis of the problem set in the domain, Gorod et al. (2017) proposed that system engineering effectiveness will improve if a methodology can be used to decide when to optimise and when to satisfice based on the complexity of the environment (Gorod et al. 2017).

Heuristics are tools for decision-making under uncertainty and have proven suitable in situations with limited knowledge, time, and resources. They support in handling complex choices with minimal cognitive workload. They are also simple and efficient to apply irrespective of the level of expertise of the decision maker. For instance, it has been argued that simple decision-making strategies like heuristics can outperform optimal models when the environment is uncertain. This assertion was based on the study that compared heuristics with optimal models using criteria like accuracy, frugality, and computational simplicity (Wang et al. 2022). However, other authors argue that heuristics might be inferior to rational decision-making processes. Deploying the concept to ecological rationality, another author examined this claim and concluded that decision-making should be evaluated based on their fit to the environment rather than adherence to a rational model, which further buttresses the strength of heuristics when compared to other models when applied in an uncertain environment (Luan et al). Similarly, another study compared the performance of heuristics against optimal decision models to examine trade-offs between decision-making accuracy and cognitive effort. The study concluded that the heuristic has better time utilisation but might trade-off quality when compared to optimal models (Methling et al. 2022). Another study investigated how heuristics can help improve decision-making while reducing cognitive overload. The study deployed a scenario-based training set and NASA-TLX in a military environment. The study found that heuristics help in making decisions with levels of accuracy comparable to optimal models with less cognitive workload (Banks et al. 2020). Furthermore, it has also been argued that heuristics support decision-making irrespective of the experience level of the decision-maker (Garcia-Retamero and Cokely 2017).

Heuristics studies have also been conducted in the context of cybersecurity. For instance, heuristics were applied in a study that explored how emotions and feelings affect risk perception in cyberspace. The study opined that people may underestimate the cybersecurity risk of online activity they enjoy, and as such, messaging should focus on the benefits of secure behaviour rather than the negative impact of cybersecurity risk. The study did not give much insight into how heuristics were applied (Van Schaik et al. 2020). Another study that leveraged heuristics to address mobile malware threats reported a high detection rate for malware. The study did not discuss how heuristics could be integrated into mobile security infrastructure (Nguyen et al. 2018). However, how cognitive heuristics influence judgment in the context of cyberspace was investigated. The author argued that decision-makers, especially non-experts, tend to rely on heuristics due to the unpredictable nature of cyberspace. The study focused on the psychological aspect of cybersecurity decision-making as

it affects users with respect to the source of the threat. Like the previous studies, this study also did not give much insight into how heuristics can be integrated into everyday cybersecurity tasks (Gomez and Villar 2018).

Domain-specific heuristics have been developed in other studies and applied to address usability problems. For instance, a study that sought to address usability challenges in ubiquitous systems adapted Nielsen's heuristics with consideration for context and mobility requirements to develop a set of heuristics that was validated by experts. The study provided an approach to how heuristics can be developed and applied (Rocha et al. 2017). Also, another study developed 11 heuristics for evaluating usability problems in mobile commerce solutions and for the smartphone domain (Ajibola and Goosen 2017; Bashir and Farooq 2019). While the domain-specific heuristics examined adapted Nielsen's usability heuristic, a study leverages thematic analysis to identify usability challenges for users and supply-side actors like developers and systems administrators (Lennartsson et al. 2021). Although these studies have highlighted how heuristics can be developed and applied, application to real-world problems to address usable security challenges has not been fully examined.

## 2.8 USABILITY AND SECURITY EVALUATION

Usability and security evaluations are conducted by applying heuristics to identify cybersecurity problems. Heuristics evaluation is concerned with how to evaluate interface design quality in a fast and cost-effective manner when compared to empirical methods. The heuristics evaluation process entails several evaluators, mostly between 3 to 5, evaluating user interface using some heuristics principles to identify usability problems in terms of frequency, criticality, and severity of the problems evaluated (Quiñones and Rusu 2017).

Quiñones and Rusu (2017) conducted a systematic review of 73 usability heuristics papers to provide a guide on how the heuristics are developed. They presented a summary of various approaches to developing heuristics and the activities conducted. Table 2.2 provides an overview of the process for developing heuristics as presented by the paper (Quiñones and Rusu 2017).

| SN | Approach for developing heuristics | Activity |
|---|---|---|
| 1 | Based on existing heuristics | • Review existing heuristics, and identify limitations for evaluating domain-specific usability problem |

| | | |
|---|---|---|
| | | • Identify features of specific domains to be considered in the new heuristics<br>• Propose a new set of heuristics |
| 2 | Based on methodologies | Adopt an existing methodology for developing heuristics |
| 3 | Based on the literature review | • Review literature and understand how existing heuristics can be applied<br>• Define a new set of usability heuristics<br>• Validate the set of heuristics via expert opinion, scenarios, thinking, or questionnaires. |
| 4 | Based on usability Problems | • Identify and analyse usability problems based on usability evaluation or documented usability problems in the specific domain<br>• Group problems into categories<br>• Create heuristics of how the problem can be solved. |
| 5 | Based on guidelines, principles, or design recommendations | • Identify and analyse standards, guidelines, and design principles for specific domains<br>• Propose a set of heuristics based on gaps identified<br>• Validate heuristics through case studies |
| 6 | Based on Interviews | • Identify usability problems in specific application domains via interviews<br>• Analyse and categorise problems<br>• Propose heuristics |
| 7 | Based on theories | • Analyse theories<br>• Develop heuristics |

Table 2.2: Process for Developing Heuristics (Quiñones and Rusu 2017)

In addition to evaluating the usability of user interface design by heuristics principles, usability metrics also exist. For instance, the System Usability Scale (SUS) and the Quality in Use Integrated Map (QUIM) have been used to measure the usability of user interface design in specific application domains (Lewis 2018; Galli et al. 2020).

## 2.9 CHAPTER SUMMARY

This chapter examined critical literature to understand current conversations in cybersecurity as it relates to MFS to understand what has worked and can be adapted to the current research problem and the research gap that needs to be addressed. The chapter analysed the MFS threat landscape from literature and identified the need to address the human factor element as the implementation of technical countermeasures, though useful, have not been able to address cybersecurity.

Furthermore, the chapter examined the literature to observe the relationship between usable security and cybersecurity. The need to incorporate user behaviour and cognitive ability in designing a workable, usable security solution was highlighted. While most usable security studies focused on the end-users, other studies also identified usable security as a challenge for developers.

The chapter identified the need for an empirical study to understand the usable security behaviours of users and developers and the key to addressing usable security. Also, the need to develop usable security requirements was identified. A guideline on how to integrate usable security into system design was also identified. The application of usable security heuristics in real-life scenarios was also recommended.

While the literature provided insight into usable security challenges and domain-specific studies have been conducted on how they can be addressed, most MFS studies are focused on identifying factors that affect MFS adoption based on various adoption theories. To the best of my knowledge, no study has been conducted on how to improve cybersecurity in the MFS domain by improving usable security.

Based on the gaps identified in the literature, this PhD thesis will examine the MFS ecosystem to gain more understanding of the domain in practice. It will also examine the behaviours of users and developers of MFS to develop a requirement that can be used in proposing usable security solutions for MFS in line with the objective of the PhD study.

# CHAPTER THREE: METHODOLOGY

The literature review in Chapter Two has shed light on the current state of cybersecurity as it relates to mobile financial services (MFS). The literature emphasised the need to address usable security in MFS to complement and enhance existing technical safeguards. Also, the reviewed literature revealed that most implementations of usable security are domain specific. Furthermore, empirical studies were recommended to gain a deeper understanding of user and developer behaviours in order to establish requirements that address usable security within the specific context of this study. Another identified gap was the need for an approach to integrate usable security elements into system development to improve cybersecurity for both developers and end-users.

To explore the gaps identified in the literature and in line with the objectives of this PhD, as outlined in Section 1.4, the researcher adopted a research methodology framework that is theoretically grounded and applicable to real-world scenarios. The following approach was thus employed:

| # | Item | Justification | Reference |
|---|---|---|---|
| 1 | Investigate MFS domain to have a domain specific insight into how cybersecurity impacts MFS | Usable security literature mostly focuses on domain specific solution and no study exists investigating the nature of cybersecurity in MFS domain | Lennartsson et al. (2021)<br>Ambore (2017)<br>Feth and Polst 2019<br>Gupta and Dhingra (2022) |
| 2 | Conduct empirical studies of user and developer behaviours and how they impact usable security in MFS | Empirical studies were recommended by literature to better help in understanding of insight to usable security problems from users and developers of the system. | Das et al. (2018)<br>Grobler et al.2021<br>Alt and Von 2019<br>Naiakshina et al. (2017) |
| 3 | Investigate how usable security requirements can be developed and integrated into MFS development process | Most studies derived usable security requirement by fusing usability and security requirement. This study seeks to investigate how to develop requirement addressing usable security problems in MFS | Feth and Polst (2019)<br>Nocera et al (2023)<br>Wiefling et al. (2020) |

| | | | |
|---|---|---|---|
| 4 | Investigate how usable security requirements can be applied in real-world scenarios | The need to investigate solutions grounded in theory and implementable in practice | Lead (2020)<br>Gutfleisch et al. (2022) |

Table 3.1: Research Approach

The overarching research methodology adopted for the thesis is design science, which is an approach that facilitates the development of artefacts that will be used to address real-world problems. It brings both practical relevance and rigour (Baskerville et al. 2018; Vom et al. 2020). The activities in design science include problem identification and motivation, defining the objectives for the solution, design and development, demonstration, evaluation, and communication. The high-level design research process includes awareness of the problem, suggestion, development, evaluation, and conclusion (Baskerville et al. 2018). The choice of design science was predicated on the focus of this research which sought to develop artefacts that would be applied to address real-world problems in MFS security. The artefacts were developed in an iterative manner using Action-Research (A-R). A-R is an iterative process that changes and improves knowledge and understanding to be achieved at the same time (Myers 2019; Evered and Roger 2022). The process of A-R is made of five phases that are iterated, including; diagnosis, action planning, action taking, evaluating, and specifying learning (Cornish et al. 2023; Evered and Roger 2022). Human factor approaches and other techniques were used in contextualising the problem space. Details of the other approaches and techniques used are provided in section 3.3 of this thesis.

The use of the Saunders research onion was proposed for addressing the essential perspectives of a research layer by layer (Melnikovas 2018). This section adopted the research “onion” approach in using a layer-by-layer approach to discuss the overall methodology of the research.

## 3.1 RESEARCH DESIGN

This section provides an overview of the overall design of the PhD research and how the studies conducted tie into the overall research objective.

A 5-stage process which includes initialisation, exploration, solution design, confirmation, and finalisation was adopted for this PhD research. Whereas the first two stages focused on understanding the problem and the problem space, the last three stages focused on developing and validating the proposed solution. Figure 3.0 depicts the research design showing the 5 stages.

### 3.1.1 Initiation

This stage of the process defined the motivation of the study and examined existing literature with a view of contextualising the problem space. The stage also defined the research objectives and contributions. The primary strategy used in this stage is the literature review. The output of this stage feeds into the second stage, exploration.

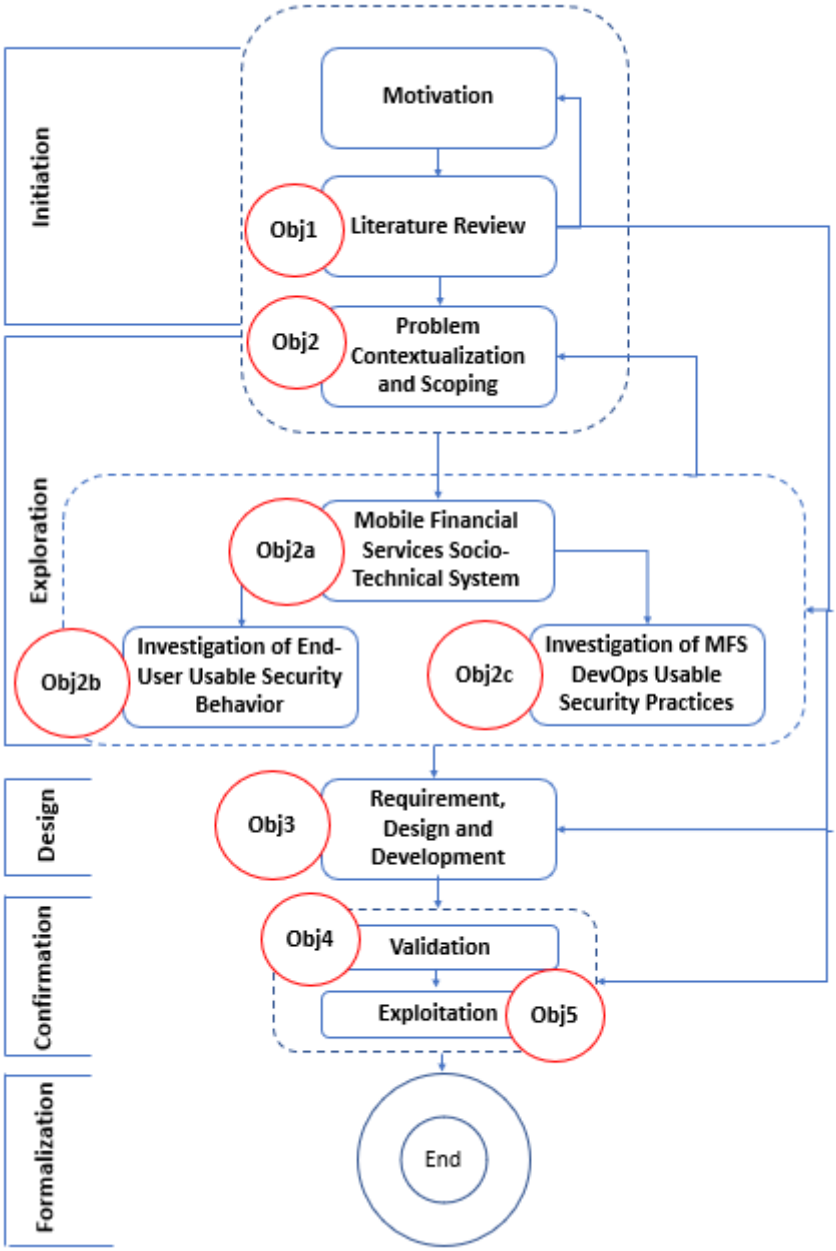



Figure 3.0 Research Design Stages

### 3.1.2 Exploration

Based on the findings of the 1st stage and the philosophy and approach adopted for this thesis, the exploration phase analysed the problem space from the perspective of key stakeholders in the ecosystem. The 1st component of this stage, the mobile financial system sociotechnical system, analysed the MFS ecosystem and the threat of cybersecurity from a stakeholder perspective. Based on the findings from the MFS STS, an investigation was conducted into the usage, development, and deployment practices of key MFS stakeholders. To achieve the objective of developing the MFS

STS, rich picture, interactive management, and interpretive structural model techniques were deployed.

### 3.1.3 Stage 2b: Investigation of MFS Usage, Development, and Deployment Practices

This stage is an offshoot of stage 2a. The study that defined the MFS STS identified usable security as a major issue in the MFS STS. In this stage, a study to understand how the identified elements affect usable security and trust in MFS STS was conducted. The study explored the end-user perspective by surveying MFS users. It also examined DevOps and Chief Information Officers' (CIO) implementation practices and the impact on usable security and trust in MFS STS. Semi-structured interviews, thematic analysis, and card sorting were the major qualitative analysis tools used while Principal Component Analysis (PCA), Confirmatory Factor Analysis (CFA), and Structural Equation Model (SEM) were key qualitative analysis tools used. The outcome of this stage highlighted the impact of *supply-side* (DevOps, CIO) and *demand-side* (end-user) behavioural dynamics on usable security and trust. This phase addresses the 2$^{nd}$ objective of this PhD research.

The output of this phase feeds into the contextualisation of the problem space and the design phase.

### 3.1.4 Stage 3: Design Phase:

The design phase consists of designing a proposed solution for individual components of security issues in MFS and the integration of the components into a single approach. This was carried out iteratively to come up with the heuristics that would address usable security in MFS. This phase addresses the 3$^{rd}$ objective of this research. The output of this phase is the proposed solution.

### 3.1.5 Stage 4: Confirmation

The confirmation phase includes validating the proposed solution through a focus group and exploiting it by applying it to the unbanked through developing and testing fintech solutions, addressing objectives 4 and 5 of this research. To achieve this, case studies were conducted. The first case study demonstrated how the developed heuristics would be integrated into real-life solution development. A hackathon was organised to achieve this objective, where 49 applicants participating in teams entered the competition with 9 participating in the last stage. The winning group and first two runners-up received cash gifts, but most importantly recommendations on how usable security was integrated into the development of minimum viable products were noted. Furthermore, a second use case focused on using the developed heuristics to conduct black-box testing for existing solutions. These also revealed some learnings that served as recommendations for the use of the heuristics. The

third case study was the evaluation of usable security in MFS as it related to the concerns of the visually impaired.

### 3.1.6 Stage 5: Formalisation

The formalisation phase addressed the academic requirement of documenting the PhD research in a thesis and undertaking a verbal examination to defend the research work.

## 3.2 FLOW OF RESEARCH ACTIVITIES AND OUTPUT

While section 3.1 of this thesis shows the thought behind the design adopted for this PhD research, this section shows the flow of activity from one stage of the research work to the other. It shows input at every stage, action taken, and approach adopted.

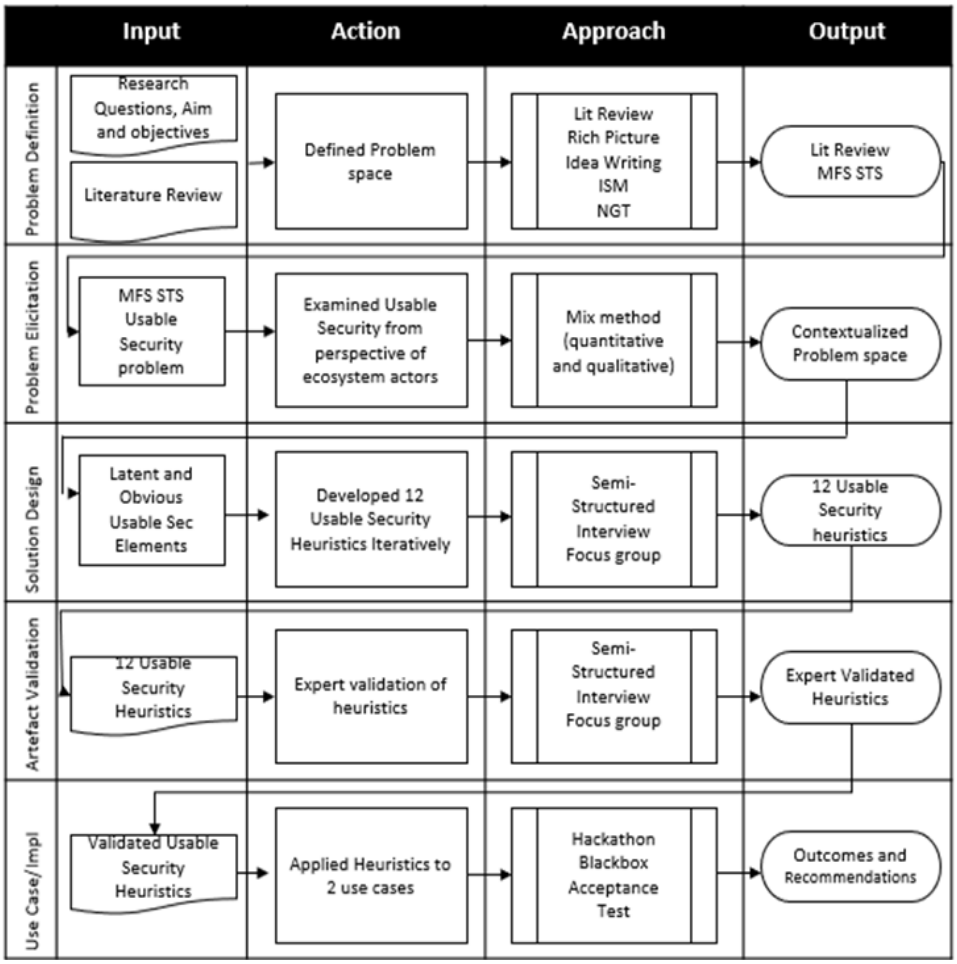



Figure 3.1: Flow of Research Activity

It also shows the major output at each stage of the PhD as shown in Figure 3.1.

## 3.3 RESEARCH PHILOSOPHY

A critical element of this thesis is developing knowledge in the area of mobile financial services security to facilitate answering the questions raised by this research intending to contribute new knowledge to the existing body of knowledge. The research philosophy adopted influences the process taken to develop this knowledge (Melnikova 2018,). To determine the research philosophy to adopt for this research, the researcher adopted the research philosophy diagnosis template (Melnikova 2018). The model contains ten questions each to be answered on a Likert scale with six options ranging from “Strongly Disagree” to “Strongly Agree”. The diagnostics seek a subjective rating of issues relating to research realities, the relationship between the researcher and the phenomena being studied, methodology choices, whether the research should be practical or applied, etc.

This thesis adopts a pragmatic research philosophical stance in the sense that the research question helped in determining the philosophy adopted. In completing the philosophy diagnostic, the researcher strongly agreed that for the topic being researched, there is one single reality and that it is the task of the researcher to discover it. Furthermore, the researcher also assumes that the reality of the topic being researched exists somewhat separately from the researcher, even though the researcher would benefit from the solution discovered to the research question as a social actor.

More so, the researcher believes the phenomena researched in this study—the security concerns of MFS and how to resolve them—are created by the actions and inactions of social actors concerned with the existence of the phenomena. As such, subjectivism as against objectivism as an aspect of ontology drives his research philosophical choice. This is necessary for helping to discover motivations for the actions and inactions of social actors in a way that would help the researcher address the research question.

The research reflects the philosophy of positivism in that the researcher prefers working with observable social reality with the outcome of the research being a law-like generalisation of how to secure MFS.

In summary, the researcher adopts a pragmatic approach to this research as he believes the research question is fundamental to the philosophy adopted. Furthermore, the researcher adopted subjectivism as an aspect of ontology as he believes the phenomena being investigated are created by the actions and inactions of social actors. This thesis reflects a philosophical stance of positivism as the

researcher prefers to work with observable social reality. The next section addresses the research approach.

## 3.4 RESEARCH APPROACH

The second layer of the research "onion" is determining the research approach. The two main approaches are the deductive and the inductive methods.

Research studies involve the use of certain theories. The approach adopted is a function of the level of clarity of the theory to the researcher at the beginning of the research journey (Melnikova 2018).

While deduction can be said to tend toward the left on a theory-data continuum, induction tends toward the right. Deduction emphasises moving from theory to data while stressing the need to explain the causal relationships between variables. Furthermore, deduction underscores collecting quantitative data, a highly structured approach, and the generalisation of conclusions. On the other hand, induction emphasises understanding of meanings humans attach to the event, collection of qualitative data, progressive elaboration to accommodate changes as the research progresses, and less concern about generalisation (Melnikova 2018).

This thesis combines both approaches as it starts from known theories based on the research questions and has an exploratory part that is expected to reveal new meanings from data informing the selection of some of the techniques used in the research strategy. The use of both quantitative and qualitative approaches for data collection makes it expedient to use a combined approach, as it will better address the research question. Due to the limited time for this research, the inductive approach will help focus the work on the time horizon. Though the conclusion of this thesis generalised findings that can be applied to all implementations of MFS, tilting towards a deductive approach, this will be done in such a way that the solution will be refined as the research progresses, giving it an inductive focus.

In summary, this thesis leverages the strength of both the deductive and inductive approaches to address the objective of the PhD study.

## 3.5 RESEARCH STRATEGY

This section describes the strategies used to gather and analyse data. The research "onion" identified seven different strategies which include experiment, survey, case study, action research, grounded theory, ethnography, and archival research (Melnikova 2018). However, this section focuses on describing the strategies adopted for this research.

### 3.5.1 Experiment

In a classic experiment, two groups are set up—a control group and an experimental group—to measure the dependent variables in both the control and experiment groups. Experimental design can be of three types. Independent measures, where different actors participate in each condition of the independent variables, refers to measuring subjects in multiple conditions. In a within-subject design, there are two conditions—a treatment and a control—and each subject goes through both conditions. Another type of experiment design is repeated measure design where the same participants participate in each variable. Counterbalancing is a type of experiment design that helps control for other effects (McLeod 2023). In this research, experiment as a methodology was used in an implementation case study. Specifically, repeated measure with counterbalancing was used. The benefit of using this approach was that cost and time were reduced. Furthermore, to the extent that a theoretical hypothesis (improvement in MFS security will enhance trust) was defined, and that a sample of individuals was selected from a known population of MFS users, principles of experiment were used as a strategy for this research.

### 3.5.2 Survey

The survey strategy was adopted in this research to help collect data from MFS users to understand their user behaviour with a bid to understanding variables that affect trust. Statistical methods were then used to analyse the data. This research has two major phases, a discovery phase which helps analyse the problem space, and a solution phase where a proposed solution will be proffered. A major part of the discovery phase depends on using surveys to conduct exploratory studies.

### 3.5.3 Case Study

Four case study strategies based on two dimensions exist, single vs. multiple and holistic vs. embedded (Melnikova 2018). This PhD study evaluated the finding of the developed solution using a single case study of MFS for the unbanked due to the large number in this group and the potential impact on MFS adoption.

### 3.5.4 Action Research

This is the strategy adopted for developing artefacts in this research, as it follows the action research spiral which starts from context and purpose, then diagnosing, then planning, then acting, and then evaluating, before repeating the spiral (Melnikova 2018). This research started by providing the context of the problem and the purpose of the study. It further explored the problem space to have a better understanding of the problem from the stakeholder perspective, before developing a solution that would address the gap which will be evaluated before applying to the unbanked.

### 3.5.5 Grounded Theory

This thesis involved collecting data through interviews. The collected data was analysed to reveal insight and possibly inductively build theory. Thematic analysis was applied in this regard due to its ability to expose both observable and latent constructs from the analysed data (Braun and Clarke, 2019, Braun and Clarke, 2021).

In summary, this thesis adopted several strategies as appropriate to achieve the intended objective of this study.

## 3.6 RESEARCH METHOD CHOICE

To achieve the aim of this research and in line with the research philosophy and approach, this thesis adopted mixed-method research for collecting and analysing data. Mixed-method research uses both quantitative and qualitative data collection techniques and analysis procedures either in parallel or sequentially (Saunders et al. 2016). This section describes the details of the various techniques and the justification for choosing them.

### 3.6.1 Qualitative Techniques

To achieve the objective of this PhD research, some qualitative techniques were applied. This subsection describes these techniques.

#### *3.6.1.1 Rich Picture*

To have a customer-centric understanding of cybersecurity challenges in the MFS ecosystem, it was imperative to gain an understanding of the ecosystem from the perspective of its stakeholders. In considering the right methodology to analyse the ecosystem, the rich picture technique was adopted. It is an action-oriented process of inquiry into ill-defined problems (Checkland and Poulter 2020). The approach was preferred to hard systems and other human factor approaches because it clearly defines conceptual problems from the user's perspective. Two soft systems techniques were specifically applied; *the Rich Picture* technique provides a pictorial view of key stakeholders and their interactions and *the root definition and conceptual model* provides an understanding of various stakeholder world views and key requirements for security concerns in the ecosystem *(*Checkland and Poulter 2020*).* The combined use of these techniques, along with a systematic literature review, helped in the identification of stakeholders as well as providing an understanding of the differences and similarities in their perception of the MFS STS.

#### *3.6.1.2 Interactive Management*

Interactive management (IM) techniques—idea writing (IW), nominal group techniques (NGT), and interpretive structural modelling (ISM)—were used to generate issues and objectives for mitigating them, and how they influenced each

other. Interactive management techniques are group decision-making techniques suited for analysing complex environments (Ward et al. 2017). Specifically, IW was used to generate ideas by brainstorming on human-factor-related cybersecurity challenges in the problem space. The technique helps in avoiding a situation where early focus would be on the solution before a proper understanding of the problems. NGT provides an understanding of key objectives of mitigating challenges identified while ISM links objectives to determine relationships and influences.

#### *3.6.1.3 Semi-Structured Interviews*

Semi-structured interviews were conducted for data collection and artefact validation. In the first study, it was used as an independent validation of the output by subject matter experts, while in the second study, it was used to understand MFS development and procurement practices of the MFS development team group (DevOps) and Bank CIOs respectively.

#### *3.6.1.4 Thematic Analysis*

Thematic analysis is a qualitative research analysis tool that provides a systematic approach to interpreting collated data and a coherent narrative leading to rich insights that explain the phenomena observed in the data. Though other qualitative analysis methods such as discuss analysis, decomposition analysis, grounded theory, and interpretative phenomenological analysis exist, the thematic analysis provided the tool necessary to analyse apparent and latent phenomena that would ultimately address the research question in the study conducted to understand usable security factors (Braun and Clarke 2019).

#### *3.6.1.5 Card Sorting*

Card sorting helps classification of related phenomena for meaningful analysis (Janssens et al. 2018). In this research, card sorting helped in arriving at the key factors that affect usable security from the perspective of the stakeholders.

#### *3.6.1.6 Hackathon*

Hackathon is a problem-focused approach to innovation that originated from the field of computing and the need to enlist innovative ideas to solve problems through crowdsourcing. In hackathons, teams come together to compete on how to solve a real-life problem through creating a prototype often for a reward. For instance, technology companies like Alphabet and Meta put out hackathons to promote product innovation. While hackathons are not an explicit research technique, this thesis developed a set of heuristics that need to be integrated into solution development innovatively (Medina et al. 2020; Nolte et al. 2020). Since mobile financial services solutions are fintech and fintech mostly evolved out of hackathons, adopting hackathons will not only demonstrate the applicability of the heuristics in solution

development but also provide a few more ideas that could facilitate the adoption and usage of the heuristics for fintech development.

#### *3.6.1.6 Black-box Testing*

Black-box testing is a software testing method that focuses on validating the functionality of a system without focusing on internal working mechanisms. Testers do not need to understand the internal workings of the code but focus on input from requirement specification and output. Software testing is a very important part of solution development as it makes up over 50% of development costs. The objective of testing is to find loopholes or issues in a system which is cheaper to correct before the final system is produced. A good test would mitigate cybersecurity vulnerability in a system. White-box testing also exists but will require a working knowledge of the code and expertise in code development. In this thesis, black-box testing was adopted to allow users without coding experience to use the developed heuristics to test existing solutions for usable security compliance. This testing technique avoids developer bias and is suitable for acceptance tests (Verma et al. 2017).

#### *3.6.1.7 Heuristics*

Section 2.6.2 of this thesis explored several approaches to integrating usable security into systems design. The advantage heuristics offer above other methods is the ability to work better in an environment with constraints on knowledge, time, and resources which is a typical development environment for MFS developers. Furthermore, the details of heuristics development were highlighted in section 2.8 of this thesis. This PhD study seeks to develop heuristics and integrate them into the MFS development process.

### 3.6.2 Quantitative Techniques

This section describes the quantitative techniques deployed and used in this research.

#### *3.6.2. 1 Survey*

To better understand the impact of balance between usability and security in the use of MFS, an end-user survey was conducted. The survey questionnaires were distributed via electronic and paper-based correspondence. The completed questionnaires were then analysed and presented. The survey questionnaire was developed based on usability, security, and usable security criteria derived from the literature that highlighted elements of usability, security, and usable security, and critical examination of the current threat landscape for MFS as highlighted in Chapter Two of this PhD thesis. Frequency and descriptive statistics tools in the Statistical Package for the Social Sciences (SPSS) and Bristol Online Survey were then used to analyse the survey feedback.

#### *3.6.2.2 Principal Component Analysis (PCA)*

The principal component analysis (PCA) is a technique for investigating the interdependence within groups of variables. It is concerned with the relationships between observable variables and unobservable latent variables presumed to be generating the observations (Xie 2019). In this research, PCA helped to expose latent variables not visible by using simple correlation techniques and cross-tabulation.

#### *3.6.2.3 Confirmatory Factor Analysis (CFA)*

The principal component analysis conducted on the survey data revealed the existence of some observable and latent factors. To explore this finding, it is imperative to test the hypothesis that a relationship exists between the observed variables and their underlying latent variable. CFA is a statistical technique that helps to achieve this objective. Because the number of consideration factors has been discovered in advance through PCA, CFA was preferred above exploratory factor analysis (EFA) (Shrestha 2021).

#### *3.6.2.4 Structural Equation Model (SEM)*

Based on the data obtained from the survey conducted in this study, structural equation model (SEM) was used to assess the impact of some latent variables on trust. SEM was chosen above methods like path analysis and multiple regression model due to its ability to use latent variables (Mueller and Hancock 2018).

## 3.7 RESEARCH TIME HORIZON

The strategy for data collection employed in this research recognises the time constraint of research of this nature and therefore depends on instruments like surveys and interviews to collect data which represents data taken at a particular time as against data taken over a while. Consequently, the preferred time horizon for this research is cross-sectional since it deals with snapshots and not longitudinal which deals with data collection over a while.

The innermost layer of the research “onion” considers data collection and analysis techniques, which have been discussed in the research choice section.

Using the research “onion” as a guide provided insight into the research philosophy adopted for this research. The philosophy adopted reflects pragmatism, subjectivity, and positivism. Furthermore, an approach that combined both deduction and induction was adopted. More so, the strategies and methods used for the research were discussed, and the reason for the choices provided.

## 3.8 ETHICAL CONSIDERATION

The research approach adopted a hybrid of deduction and induction as described in section 3.4. A key reason for considering the inductive component of the approach

was the anticipation of changes during the research and an approach to integrate necessary changes as the need arises. To that end, the researcher obtained approval of the Research Ethics Committee (REC) on a modular basis, as against a single approval for the entire thesis. Furthermore, based on the ethics checklist, this research is low-risk research. However, the researcher adhered to the research code of conduct of the university. More so, the researcher has completed the mandatory ethics module as part of this PhD study.

## 3.9 RESEARCH LIMITATION

The time horizon for this research means a longitudinal approach to data collection and analysis was not deployed. The research depended on data from selected participants representing their responses at a given time. The researcher is aware that additional insight might be obtained if a longitudinal approach was available for the research, but due to the maximum allowable time for the PhD, a cross-sectional approach which depends on a snapshot of data will be adopted as against methodologies that will require a longer time horizon. This limitation notwithstanding, the researcher is committed to delivering high-quality research in line with established theories.

## 3.10 CHAPTER SUMMARY

This PhD research work leverages design science as the overarching methodology for this study as it facilitates the development of artefacts that can be applied in a real-world use case. The artefacts would be developed using action research. The research work adopted a pragmatic philosophical stance. It also reflects the philosophy of positivism as the outcome is a generalisation of how to secure MFS. Furthermore, the research adopted inductive and deductive approaches. The combination stems from the reason that it starts with known theories based on research questions and has an exploratory part that reveals latent data. The time horizon for this research is cross-sectional given that this study is expected to be concluded within the time frame for a PhD study.

This chapter details the mixed method technique used to collate, analyse, and present the findings of this research work. It justifies every technique used. More so, it applied non-conventional research techniques like a hackathon and black-box testing during the implementation of the artefact. The chapter also provides a graphic flow of the research phase and the flow of activity.

# CHAPTER FOUR: CYBERSECURITY IN MOBILE FINANCIAL SERVICES SOCIOTECHNICAL SYSTEM

## 4.1 INTRODUCTION

The literature review in Chapter Two of this thesis, as highlighted in section 2.6.2, has shown a domain focus on usable security problems. While the MFS adoption literature analysed in section 2.2 has provided some insight into the MFS ecosystem, the nature of the human elements problem that leads to cybersecurity threats has not been fully explored. Furthermore, cybersecurity is a sociotechnical problem (Ambore et al. 2017). As such, to understand the nature of usable security problems in MFS, it is imperative to explore the MFS ecosystem with the view to understanding the human elements and the related cybersecurity concerns that may lead to cybersecurity attacks as highlighted in section 2.5 of this study.

While the scope of this study is limited to exploring usable security for MFS to improve cybersecurity for MFS, this chapter seeks to explore cybersecurity issues in the MFS ecosystem, to understand usable security challenges that might lead to cybersecurity gaps in MFS. This is in line with the action research methodology adopted and highlighted in section 3.5.4 which focuses on establishing context and purpose as a precursor to drilling down to the problem space.

This study sought to contextualise the MFS ecosystem from the viewpoint of stakeholders in the ecosystem to gain an understanding of them, their experience and challenges regarding usable security in MFS, and what insight can be learned from that.

This study commenced by conducting a broad overview of human factor related issues in cybersecurity. It provides an overview of MFS and sociotechnical systems. Output from this study provided the necessary input to developing usable security requirements for MFS.

## 4.2 STUDY METHODOLOGY

This exploratory study plans to examine cybersecurity concerns in MFS STS from the viewpoint of the actors in the ecosystem to contextualise the problem space and come up with a prioritised list of recommendations and requirements for addressing usable security problems in MFS. The research leverages human factor techniques to

analyse the sociotechnical system. Human factor approaches help contextualise ill-defined complex social technical systems like that of mobile financial services (Pollini et al. 2022). A major objective of contextualising the problem space is to develop user-centric requirements for usable security in MFS. The study identified and prioritised requirements for addressing specific cybersecurity concerns in MFS. The next section describes the approach adopted for this study.

### 4.2.1 Study Approach

Various human factor techniques and their suitability for achieving the objective of the study were examined, and the ones that align with the strategy of the study were applied. Table 4.1 describes the techniques adopted and the justification for the choices.

| SN | Methodology | Technique | Justification |
|---|---|---|---|
| 1 | Soft systems | Rich picture | Provides an understanding of the problem space from a stakeholder viewpoint in line with the study objective |
| 2 | | Root definition and conceptual model | Provides an understanding of stakeholder worldview, and key requirements for addressing cybersecurity concerns in the ecosystem |
| 3 | Interactive management | Idea writing | Help actors generate a list of problems by brainstorming. The technique helped avoid a situation where the focus would be on a solution even before the problem was critically analysed. |
| 4 | | Nominal group technique (NGT) | Helps stakeholders to prioritise challenges with the view of addressing the ones with the most impact on MFS |
| 5 | Interpretive structural model | Interpretive structural model | Consolidate perspectives and varying stakeholder worldviews, requirements, and objectives to come up with a common understanding of human factor |

| SN | Methodology | Technique | Justification |
|---|---|---|---|
| | | | elements that affect usable security in the ecosystem and the relationship among them |
| 6 | Expert interview | Semi-structured | Validation of workshop outcome to come up with recommendations |

Table 4.1 Techniques Adopted for the Study.

Soft systems methodology was developed out of a need to adopt an action-oriented approach for examining an undefined problem space. It guides thinking about problematic situations in such a way that action to bring about improvement can be taken. It provides for various stakeholder worldviews to be analysed to come up with a common understanding of the process. Furthermore, it provides techniques to contextualise the problem space in a way not possible by word alone and allows different interpretations based on mental models; *rich picture*, formulation of a relevant system of purposeful behaviour; *root definition*, building a human activity model and comparing it to the real-world, and development of a *conceptual model.* The soft systems approach was preferred to hard systems and other human factor approaches as the combined use of the techniques helped achieve the study objectives via clarifying the problem space by consolidating various worldviews. Soft systems allow differences in understanding of problems based on mental models to be entertained, to facilitate an agreeable interpretation in a rational and defendable way. Furthermore, it provides a model to structure discussions amongst ecosystem actors about desirable versus feasible solutions by comparing the model to the real world (Checkland and Poulter 2020).

The flow of activity in this study was guided by a high-level design research process based on design science research, in line with the overarching research philosophy of this PhD thesis (Berkerville et al. 2018). The study followed five steps as shown in Table 4.2.

| High-Level Design Process | Approach | Action | Output |
|---|---|---|---|
| Awareness of problem | Soft system methodology (SSM). Rich picture conceptual model | Define problem space | Soft systems model |

| | | | |
|---|---|---|---|
| Suggestion | Interactive management workshop (idea writing, nominal group techniques) | Generate and prioritise problem | Prioritised problem list |
| Development | Interpretive structural model | Determine relationships and influences within problems and objectives | Prioritised objectives |
| Evaluation | Semi-structured interviews | Validate outcome | Validated results and recommendations |
| Conclusion | MoSCoW | Analysis of validated results to determine the requirement | High-level requirements for addressing cybersecurity concerns in MFS STS |

Table 4.2: High-level Study Process

In the *awareness of the problem* process step, the six stakeholder groups that participated in the study provided their understanding of the problem space from their worldview. Due to the mental model, and environment of operations, various perspectives were presented. Rich picture and conceptual models were applied in this phase. The objective of the phase was to define the problem space from the perspective of the stakeholders, which was presented in a soft systems model. In the *suggestion* process step, an interactive management workshop was convened where participants, through brainstorming, generated a list of issues leading to cybersecurity concerns in MFS STS. The identified issues were prioritised through the nominal group technique. Furthermore, the development process step focused on applying the interpretive structural model to prioritise objectives for addressing cybersecurity concerns in MFS STS and the relationships between these objectives. Five experts with an average of 18 years of working experience in various information technology disciplines validated the output of the *evaluation* phase and presented recommendations for addressing the problem of cybersecurity in MFS STS. Finally, the *conclusion* process step focused on developing high-level requirements based on the recommendation of the experts and other insights gained from the study.

The next section provides details of various stakeholders that participated in the study.

### 4.2.2 Participants Profile

To commence this section, three important questions need to be answered as follows:

i. Which stakeholders were most suited to participate in this study?
ii. How can these stakeholders be identified?
iii. How can they be invited to participate in this study?

These questions were germane because the study would involve institutional actors who might encounter bureaucratic bottlenecks in participation. Given that this research is not a longitudinal study, time was also a major constraint. To address the questions raised, a stakeholder analysis was conducted to identify relevant stakeholders for this study. The support of the apex regulator in financial services was requested in reaching the stakeholders as the outcome of the study would be beneficial to the entire financial sector. As an early incentive during initial contact with participants, their contribution to addressing the menace of cybersecurity in MFS STS was highlighted. In line with research ethics expectations, assurances were provided that only information approved by participants would be documented in the study. Table 4.3 shows an analysis of the stakeholders selected to participate in the studies (Varvasovszky and Brugha 2000).

| # | Stakeholder | Characteristic/ Involvement | Interest | Influence | Position | Impact of Study on Actors | Engagement strategy |
|---|---|---|---|---|---|---|---|
| 1 | Financial regulators | Provide the framework for MFS and provide oversight | H | H | Supportive | H | Keep informed |
| 2 | Banks | Deploy MFS | H | M | Supportive | H | Show the impact of the outcome on customer satisfaction |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | Underserved /No MFS | Candidates for MFS adoption might be hindered by a lack of trust in the system | M | L | Indifferent | H | Respect opinion |
| 4 | Bank customers | Existing users of MFS | M | L | Supportive | M | Listen more |
| 5 | Infrastructure services providers | Provide enabling services for MFS | M | H | Non-committal | M | Seek support |
| 6 | CERT | Cybersecurity experts | M | M | Cautious | H | Seek support |

Table 4.3: Stakeholder Analysis

While this study will benefit the entire MFS ecosystem in the long run, it was important to ensure the interests and concerns of all participating stakeholders are considered and analysed in such a way that they will be comfortable providing the necessary support for the studies. Furthermore, some stakeholders were very supportive while some were more cautious, especially with information sharing. Also, the infrastructure service provider group only participated as required but was not interested in any long-term engagement in the event any useful recommendations came out from the study. The financial systems regulators played a big part in rallying other stakeholders to participate effectively in the study owing to their understanding of the long-term

impact of the study. The regulators also accommodated most of the IM workshops.

| Group 1: Financial Systems Regulator | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Male | Payment Systems | 13 |
| P2 | Male | Mobile Financial Services | 6 |
| P3 | Female | Compliance and oversight | 5 |
| P4 | Male | Payment Security | 9 |
| P5 | Female | Financial Inclusion Expert | 5 |

| Group 2: Banks | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Female | eBusiness | 6 |
| P2 | Male | Mobile App Deployment | 3 |
| P3 | Female | Client Support | 6 |
| P4 | Male | Head e-Banking | 10 |
| P5 | Male | Banking Officer | 4 |

| Group 3: Underserved/No MFS | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Male | Medical Doc | 9 |
| P2 | Male | Civil Servant | 11 |
| P3 | Male | Post grad Student | - |
| P4 | Female | Post grad Student | - |
| P5 | Female | Unemployed | - |

| Group 4: Bank Customers/MFS Users | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Female | Teacher | 6 |
| P2 | Female | Trader | 4 |
| P3 | Male | Banker | 6 |
| P4 | Female | Lawyer | 6 |
| P5 | Male | Student | - |

| Group 5: Infrastructure Service Providers | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Male | Telco Regulator | 10 |
| P2 | Female | Mobile Network Operator | 8 |
| P3 | Male | Broadband expert | 3 |
| P4 | Male | Network expert | 7 |
| P5 | Male | Head of IT | 15 |

| Group 6: CERT | | | |
|---|---|---|---|
| Participant ID | Gender | Expertise | Years of Experience |
| P1 | Male | Lawyer | 9 |
| P2 | Male | SOC expert | 4 |
| P3 | Male | Consumer Protection Expert | 10 |
| P4 | Male | Cybersecurity | 3 |
| P5 | Male | Cybersecurity | 5 |

Figure 4.1: Participants' Profile

Figure 4.1 provides details of the participants' profile.

The stakeholders listed participated in the interactive management workshop. In determining participants for Group 4, the researcher ensured that the right mix of mobile financial services products like mobile banking, mobile payment, and mobile money users were represented. It is also worthy of note that all sections of society in terms of gender, employment status, and academic qualification were represented in the workshops. After the workshops, five experts were involved in the validation of the outcome of the workshop. The most experienced in this group has 22 years of experience in his field of expertise while the least experienced has 14 years of expertise. Their expertise covers the fields of quality assurance, business analysis, software engineering, service desk, and consumer protection. All participants in this study are resident in Nigeria.

### 4.2.3 Session Plan

Six workshop sessions were held over five months depending on the schedule and availability of group participants. The researcher served as a facilitator but did not interfere with group decisions. The researcher also provided the venue, with tools like laptops, flip charts, sticky notes, and a market in addition to refreshments for participants. Each session commenced with an introduction of participants. The facilitator then took participants through a presentation of workshop objectives and expectations, as well as the following presentations:

- Presentation on overview of mobile financial services and cybersecurity concerns
- A brief explanation of human factors with a focus on soft systems and interactive management
- Use of ATM transaction as an example for soft systems.
- Description of the process involved in idea writing and nominal group technique

After the presentations, participants were allowed to seek clarification and share their thoughts on how to make the sessions more effective. Each group nominated someone to take notes and another member to keep time. The workshop session lasted for an average of three hours.

The expert validation session was a one-on-one session with each expert at the premises of the expert based on availability. The expert session took two months to complete, and each session lasted an average of 40 minutes.

## 4.3 RESULTS

This section summarises key findings from the study conducted. It presents the findings from each workshop, the interpretive structural model, and recommendations from the expert reviews.

### 4.3.1 Financial Systems Regulators Group: Summary of Findings

The rich picture produced by this group was focused on the direct link between strengthening mobile money operations and financial inclusion. They observed that the adoption of mobile money amongst the unbanked and awareness of the products was low. They further noted that while players in the ecosystem have implemented several initiatives to improve trust by improving cybersecurity, trust was still low. Furthermore, they noted that responsibilities, boundaries, and handshakes were not too clear. The group also raised concerns about the possibility of regulatory arbitrage in the space. While a fraud forum exists, it focuses more on the financial services space, while the telco regulator focuses more on mobile network operator-related

concerns. Responsibility for consumer protection is also split between the Telco and financial services regulator. Figure 4.2 shows the rich picture of the financial services regulator group. The root definition of the group focuses on implementing an industry-wide information security operations centre that will facilitate information sharing on cybersecurity incidents by participants (all stakeholders in financial services) to minimise the risk of cybercrime and boost end-user confidence in the financial sector.

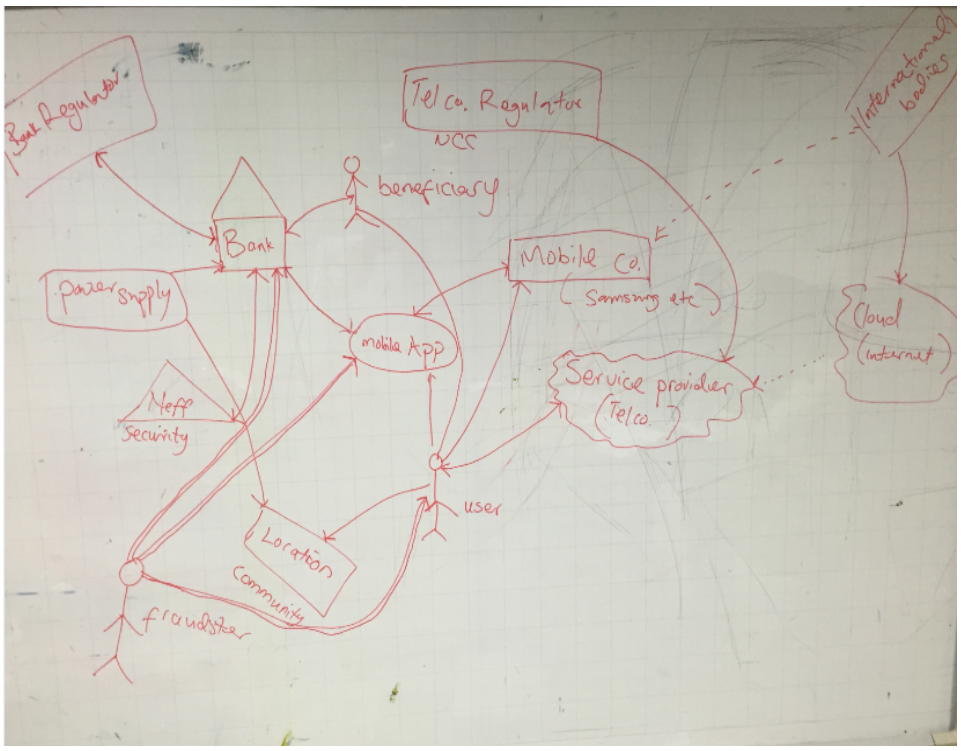



Figure 4.2: Photograph of Rich Picture for the Banked Focus Group (personal collection 2017)

All the thirty-four issues generated through idea writing from the world view of the stakeholders in the ecosystem were categorised into four broad buckets based on affinity, namely process-related, people-related, technology-related, and regulations-related. Some issues identified through the soft systems model by the team include the lack of sufficient intelligence and collaboration in the financial services space leading to gaps in cybersecurity in MFS. The group also raised concerns about the lack of emphasis on cyber resilience in some of the technology-dependent processes in the ecosystem leading to issues like SIM card swap which has led to financial loss through MFS. The group also noted that the delay in the reconciliation of e-float and actual bank accounts by MFS operators might lead to cybercrime. Furthermore, the group noted that while the Unstructured Supplementary Service Data (USSD) channel presents an opportunity for the underserved to access financial services via

feature phones, the vulnerability in the channel might be exploited by cybercriminals thereby further impacting trust in the system amongst the unbanked. The concern about the existence of clones and rogue apps, and their impact on unsuspecting users, was raised.

Using the nominal group technique, the group prioritised some suggestions on how to address the issues in the ecosystem. Each participant (P1 to P5) in the group ranked each objective on a scale of 1-5, 5 being the highest and 1 being the lowest. The total for each objective was then summed. The objective that carried the highest weight was considered the most important by the group as shown in Figure 4.4. The group believes information sharing within the MFS ecosystem is the most important human factor priority for addressing cybersecurity in MFS; this objective has the total highest score of 17 as shown in Table 4.4. Similarly, they believe cybersecurity in MFS can be proactively mitigated when banks provide some level of market-level oversight to MFS operators. The group also noted the need to address infrastructural-related issues that could be exploited by cybercriminals. Also, the need to develop, adopt, and implement appropriate standards and ensure compliance with these standards was very important in mitigating human factor-related cybersecurity concerns in MFS. The details of all the 34 issues raised by this group, the soft systems output, and the details of the idea writing workshop, are presented in Appendix I.

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Ensure compliance to standards | 4 | 1 | 2 | 4 | 2 | 13 |
| 2 | Set up an industry wide cybersecurity operations centre | 3 | - | 4 | 5 | 5 | 17 |
| 3 | Ensure deposit money banks implement necessary oversight for cybersecurity | 5 | 2 | 3 | 3 | 1 | 14 |
| 4 | Mitigate risk associated with poor infrastructure (e.g. power, internet, technology) | - | 4 | 5 | 1 | 4 | 14 |
| 5 | Improve user awareness on mobile banking security and general technology security | 1 | 5 | 1 | 2 | - | 9 |
| 6 | Develop strategy for external dependency management | 2 | 3 | - | - | 3 | 8 |

Table 4.4: Nominal Group Technique Output for Financial Systems Regulators

### 4.3.2 Banks Group: Summary of Findings

The group raised concerns about the activities of actors that are external to the ecosystem and the impact they have on ecosystem players. One such actor was government at the national and subnational level and the burden of multiple taxes they place on MFS operators, increasing their service cost to the underserved and further impacting trust in MFS. The group highlighted the transaction process between the MFS operators and the banks, noting how third-party access could lead to man-in-the-middle attacks. Furthermore, the group raised concerns about the quality of the Subscriber Identification Module (SIM) registration data, its impact on identification, and how it could be exploited for fraud. The group stated that to make compliance with policy and regulations more effective for MFS, the communication channels between MFS and other ecosystem actors should be streamlined. The group identified various technology components of the MFS ecosystem and noted vulnerabilities related to them and how they can be exploited to perpetuate cybercrime in MFS. The need to identify and mitigate risk introduced into the system by third-party vendors was also identified. Similarly, the group noted that the user, the mobile phone device, the MFS agents, and the mobile app are key components in the ecosystem. They noted that a proper analysis of these components would further reveal vulnerabilities in MFS that could be exploited. The details of the rich picture and other soft system output from this group are in Appendix I.

Thirty-eight issues affecting cybersecurity in MFS were identified by the group through idea writing. These issues were put into four broad categories; awareness-related issues, infrastructural-related issues, process-related issues, and cross-cutting issues. Some identified issues by this group include various levels of lack of cybersecurity awareness amongst key ecosystem players. For instance, many users have an awareness gap on malware and how to avoid them, while some are ignorant of some actions they take to compromise privacy. The issue of the knowledge gap in managing mobile applications to keep them safe from cybercrime was noted. Insider abuse and its impact on cybersecurity for the front-end-user of MFS was also noted. Vulnerability related to lack of timely updates for mobile apps and OS was also noted. Other issues raised include the risk associated with missing devices, poor mobile app design, and failing infrastructure. Details of the thirty-eight issues generated by the group through idea writing are presented in Appendix I.

The group prioritised objectives on how to mitigate human-related cybercrime in MFS through the nominal group technique. The group identified the need for a robust social engineering awareness programme for MFS users as by far the most important priority with the highest score of 20 as shown in Table 4.5. Three of the objectives

focus on addressing back-end issues as it relates to infrastructure and insider-related vulnerability. The need for regular updates and patching was also identified. Table 4.5 shows the nominal group technique outcome from the group.

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Enforce segregation of duty in banks to minimise possibility of insider abuse | | 4 | 4 | 4 | 5 | 17 |
| 2 | Provide redundancy for infrastructure to mitigate against service downtime | 5 | 3 | 5 | 1 | 3 | 17 |
| 3 | Eliminate reconciliation issues between mobile money operators and their agents | 4 | 1 | 1 | | 1 | 7 |
| 4 | Implement robust awareness programme on social engineering for users | 3 | 5 | 3 | 5 | 4 | 20 |
| 5 | Set up cybersecurity response units in banks | 2 | 2 | 2 | 2 | 2 | 10 |
| 6 | Ensure regular system upgrade and patching by banks | 1 | | | 3 | | 4 |

Table 4.5: Nominal Group Technique Outcome for the Bank Group

### 4.3.3 Underserved (No MFS Account) Group: Summary of Findings

This group's root definition focused mainly on three areas i.e., the need to address information asymmetry, the need to design and deliver a suitable cybersecurity awareness programme for the underserved, and the implementation of a robust consumer redress mechanism by financial services providers. The rich picture focused on the need to strengthen the feedback mechanism by MFS providers. The need to keep customers and intending customers informed was also identified. The group called on MFS providers to examine why the action taken in the past has not significantly increased the adoption of MFS. The group placed a lot of emphasis on the mobile phone as the central element of the ecosystem. They believe mobile phone repairers and technicians are also important actors in the ecosystem and the risk they might pose to MFS should be examined. Like the two previous groups, this group also identified underlying infrastructural concerns and their impact on cybersecurity in the MFS ecosystem.

The group categorisation of the thirty-five issues identified was focused on stakeholders. The issues by this group were categorised into four. They include issues related to financial services providers, issues related to the users themselves, issues related to DevOps and infrastructural service providers, and the last category which was tagged “hackers” focused on issues related to unauthorised actors that look to exploit vulnerabilities in the system. Some of these issues raised by the

participants at this workshop include mobile app developers' understanding of user ability and preference. Participants believe MFS would be more secure if sufficient time and resources were invested in understanding the user side of the story before the development of MFS solutions. Consumer redress also came up as an important discussion topic. Participants believe cycle time to respond to cybersecurity concerns in MFS by banks must be drastically reduced as most of the time requests related to cybersecurity by users are SOS messages. The cybersecurity skill level of bank staff and the users of the app were both noted to be a concern that should be investigated. The secondary risks introduced by technology and the high cybersecurity knowledge level of some unauthorised actors were also raised by the group. Details of the soft systems output and idea writing workshops are presented in Appendix I.

The nominal group technique results from the group can be summarised in one word: awareness. All the top objectives border on improving the awareness of key players in the ecosystem. Participants consider the need to increase stakeholder awareness of technology and cybersecurity as an important objective in addressing cybersecurity in MFS. The need to have a general awareness of attack vectors on MFS by examining the MFS threat landscape was considered of equal importance as awareness of technology and cybersecurity. A functional consumer redress mechanism and users' need to have a basic understanding of mobile phone security and privacy were also ranked high. Table 4.6 presents the nominal group technique output, showing the top objectives for addressing cybersecurity in MFS from the participants of the "underserved group".

| SN | Objective | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Improve awareness on technology and information security | 2 | 2 | 4 | 5 | 5 | 18 |
| 2 | Understand familiar phone hackers' mode of operation | 1 | 4 | 5 | 4 | 4 | 18 |
| 3 | Understand consumer compliant process | 4 | 1 | 1 | 1 | 3 | 10 |
| 4 | Take responsibility for basic level phone security | 3 | 5 | 3 | 3 | 2 | 16 |
| 5 | Capacity building of mobile money operation staff | 5 | 3 | 2 | 2 | 2 | 13 |

Table 4.6: Nominal Group Technique Output for the "Undeserved" Group

### 4.3.4 Banked (MFS Account Owners) Group: Summary of Findings

The mobile app was central to the rich picture of participants from this group. The participants identified the links and relationships of international institutions and the requirements and standards they provide to the MFS ecosystem. Participants noted the relationship between MFS users and beneficiaries, the components involved in such transactions, and the risk they pose to MFS. They noted that unauthorised actors can also have similar access to beneficiaries through the mobile app just like any genuine user. The mobile device itself and the risk inherent as a vector for cybersecurity concerns in MFS were also noted. The root definition of this group focuses on usable security. It seeks an effective alternative banking channel that will not add additional demand for the customer or expose the customer to the threat of financial loss. A feedback mechanism that will provide transaction transparency for users was also central to the conceptual model of participants in this group. Details of the soft systems model from this group are presented in Appendix I.

Participants in this group presented the second highest number of issues, fifty-three, from the interactive management workshops. Participants' opinions on the categorisation of idea writing issues generated were divergent. After the engagement that ensued, the group also adopted a stakeholder-based categorisation like the "underserved" group. The categories include the financial services supply side (banks and regulators) related issues, the demand side (consumer) related issues, the issues related to MFS operators, and issues related to mobile network operators as a platform for MFS.

Usability and usable security issues resonated with participants in this group. Also, awareness and quality of user support were identified as customer-related problems. The habits of phone owners—how they share it, and how they secure it—was identified as a possible vector for cybersecurity in MFS. The multiplicity of service providers and unsolicited messages was a worry to the participants of this group as they viewed it as a risk that could be exploited by malicious actors. The lack of sufficient understanding of how to advise users appropriately on security controls due to the knowledge gap by financial services providers was also raised as an issue that has led to cybersecurity vulnerabilities in MFS. The soft system model from this group and the output of the interactive management workshop are presented in Appendix I.

The nominal group technique workshop identified the need to improve trust, the need to implement a user education programme to boost awareness, an approach to gauge the adequacy of security control, and a challenge to users to be "open to change" as major objectives for mitigating cybersecurity concerns in MFS. Participants shared

their various experiences and their initial unwillingness to adopt MFS, as it felt strange to “put my money in a phone”. Some of the fears expressed that can lead to a lack of openness were the fear of misplacing the mobile device, the fear of modern technology, and privacy-related issues due to a lack of transparency on what providers do with the user data they collect from users. To improve trust, participants believed it was important to ensure MFS is more user-friendly and that the security mechanism should be more usable to users and understandable by providers, to enable them to provide appropriate support to users. The need to improve trust by helping users understand the security put in place was considered the most important objective by the participants of this group. However, the group extensively discussed the measurement of trust; while some participants believe it is in the perception of the users, others believe it can be empirically measured. Table 4.7 shows the output of the nominal group technique workshop.

| SN | Issues | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Address lack of users’ education on password management | 4 | 3 | 1 | 4 | 2 | 14 |
| 2 | Banks to provide assurance of adequacy of security measures | 5 | 4 | 2 | 2 | 3 | 16 |
| 3 | Understand security put in place for mobile banking to improve trust in the process | 3 | 5 | 3 | 5 | 4 | 20 |
| 4 | Be open to change | 2 | 2 | 5 | 3 | 5 | 17 |
| 5 | Improve awareness on technology | 1 | 1 | 4 | 1 | 1 | 8 |

Table 4.7: Nominal Group Technique Output for the “Banked” Group

### 4.3.5 CERT/Incidence Response Group: Summary of Findings

Participants in this group adopted a policy-based approach to addressing cybersecurity issues for the MFS ecosystem. The root definition from this group seeks to implement an industry-wide user awareness programme, delivered by the industry, in order to ensure support personnel and end-users have a basic awareness of cybersecurity concerns in MFS and how they can help to mitigate them. The soft systems model from this group had a national outlook for solving cybersecurity problems in MFS. Participants believe identifying key institutions and infrastructure in the financial transaction value chain and classifying them as national security infrastructure will ensure the necessary attention is granted by all players to any issue that relates to the transaction flow in financial transactions. However, the concern would be the threshold of transaction value that this should fall into. Participants

consider the end-user external to critical security decisions. They believe if the foundational element that would mitigate the risk of cybercrime is put in place, the end-user would also benefit from a secure ecosystem.

The output of the interactive management workshop includes concerns about the decentralised nature of cybersecurity incident management and the absence of a centralised fraud reporting portal for MFS cybersecurity cases. The participants also noted the difficulty in managing the chain of custody for mobile devices as a challenge that might encourage fraud in MFS. While the Judiciary is committed to addressing issues related to cybercrime, the lack of capacity amongst lawyers regarding cybersecurity was noted as a concern. The duplication of effort by agencies in the ecosystem and the impact of that on the fight against cybercrime in the MFS ecosystem was also noted as a concern. The need to strengthen coordination in addressing cybersecurity-related issues was also flagged by the group. The low adoption of MFS amongst the intended target beneficiaries due to trust concerns was noted by the participants of the group. Furthermore, like the previous groups, participants in this group identified the need to improve awareness. However, they were specific in noting that any awareness programme that would be meaningful in addressing the challenges raised must be fit for purpose. Also, concerns about the high cycle for consumer redress were noted. A detailed output of the soft system model and interactive management workshop, including all forty-four issues raised during the workshop, are presented in Appendix I.

The nominal group technique outcome proposed an objective that would be beneficial to “all key stakeholders” in the ecosystem. This objective includes the review of key policies for cybersecurity, the development of a robust cybersecurity capacity-building

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Develop and implement a fit-for-purpose user awareness programme | 1 | 3 | 5 | 1 | 5 | 15 |
| 2 | Revise current cybersecurity act with input from all key stakeholders | 3 | 4 | 4 | 4 | 1 | 16 |
| 3 | Set up sectorial CERTS | 2 | 1 | 2 | - | - | 5 |
| 4 | Set up cybercrime help desks in all banks and telcos | - | - | 1 | 3 | 4 | 8 |
| 5 | Develop capacity building programme on cybersecurity for all key players | 4 | 5 | 3 | 2 | 2 | 16 |
| 6 | Set up a Risk and Incidence Response Centre | 5 | 2 | - | 5 | 3 | 15 |

Table 4.8: Nominal Group Technique Result for the “CERT” Group

plan, and awareness programmes. Table 4.8 shows the nominal group technique output from the participants of this group.

### 4.3.6 Infrastructure Service Providers Group: Summary of Findings

The sixth and final group workshop was the service provider group. The root definition for the group was to implement an approach that would ensure performance standards for every service provider were defined, measured, and complied with. They believed it would help reduce possible risks introduced by service providers in the ecosystem and further reduce the threat of cybercrime. Connectivity was central to the rich picture and conversation of participants in this group. The rich pictures show a new entity called “gateway” which was introduced between user transactions. Similarly, an entity called “service provider” was placed behind the user and has direct interactions with the “user agent” and the gateway. The participants believed the impact of this relationship in the ecosystem should be analysed to better understand their impact on information sharing and cybersecurity. Participants in the space noted that the telco regulator is the one with a direct relationship to ecosystem actors and relates with other regulators. This raises the concern of regulatory arbitrage in the ecosystem.

This group generated the most issues; fifty-nine. One major discussion in the group was the trivialisation of cybersecurity issues in MFS because of the value involved when compared to an attack on a bank database. The group encapsulated this by noting that “only big fraud gets big attention”. The details of the soft systems output and interactive workshop output are in Appendix I.

The nominal group technique output details the need for MFS providers to include cybersecurity in their business strategy and elevate business resilience as a key objective of mitigating cybercrime in MFS. Participants also prioritised the need for a minimum standard for availability and consumer redress as a measure to mitigate the

risk of cybersecurity in MFS. Table 4.9 shows the nominal group technique result for this group.

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Ensure every service provider has a business continuity strategy | 3 | 4 | 2 | 3 | 4 | 16 |
| 2 | Define minimum performance and availability level for all service providers | 1 | 3 | 3 | 5 | 3 | 15 |
| 3 | Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers | 2 | 5 | 1 | 4 | 5 | 17 |
| 4 | Develop end-to-end process on complaint management | 4 | 1 | 5 | 2 | 1 | 13 |
| 5 | Educate client on cybersecurity | 5 | 2 | 4 | 1 | 2 | 14 |

Table 4.9 Nominal Group Technique Output for the “Service Provider” Group

### 4.3.7 Consolidated Soft Systems Model

The engaging workshop sessions by the six participating groups provided rich insights into the human factor-related cybersecurity issues in the MFS ecosystem from their worldview through the soft systems model and interactive management workshop. The soft systems model provides a rationale and basis for comparing models to real-world situations so that grounded recommendations can be proffered for issues raised. The consolidated model derived from the workshop feedback classified all issues raised into four broad categories: *Awareness*, *Policy*, *Process Optimisation,* and *Infrastructure/Transaction*.

i. Awareness

Awareness is a cross-cutting concern for all ecosystem stakeholders. The soft systems model reveals that end-users and even solution providers require some level of awareness. “Fear of the unknown” is a leading cause of lack of awareness amongst the end-users. The nature of the fear was also attributed to uncertainty due to a lack of understanding of those involved in a transaction flow and what they do. This was important due to the real risk of actual loss of funds. “Consciousness of security control”, is a situation where users do not even know or understand if a control put in place is even available or do not even know when and how to activate it. This problem also affects application developers and their awareness of certain security APIs. “Carelessness” and “resistance to change” were also identified as possible root causes for the gap in awareness. To improve cybersecurity in MFS, there is a need to improve awareness for all stakeholders in the value chain.

ii. Policy

The concern about compliance with extant guidelines and the need to improve oversight in the ecosystem was noted. It was also noted that the ecosystem does not exist in isolation from other jurisdictions due to the electronic nature of MFS transactions and its impact on cross-border related issues like Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT). The decision about cost versus security in deploying mobile applications was also highlighted here. To improve cybersecurity in MFS, extant regulations need to be revised to strengthen oversight with an eye on cross-border implications.

iii. Process

Poor user experience, weak redress mechanisms, and fraud-related issues have led to lack of trust in MFS apps, which has impacted adoption. Issues about frequency and timeliness of security updates and who is ultimately responsible for that were flagged. Furthermore, lapses in SIM registration and poor security control processes were some process challenges that were identified. While most issues raised here would depend on the service provider to address, it has a direct impact on cybersecurity for MFS end-users.

iv. Infrastructure/Transaction

Two main issues that were repeatedly flagged here are related to the vulnerability of the mobile app and transmission channels. Specifically, concerns were raised on the possibility of cloning of MFS apps, the implication on unsuspecting users, poor app design, and the vulnerability it introduces. Vulnerability concerns in the USSD channel were also noted. Transparency of the transaction channel and the need for appropriate and timely feedback were also raised. Similarly, issues related to various human-related vulnerabilities in the mobile app and transaction channels were raised. Addressing these human-related infrastructure and transaction-related issues would improve the security of MFS.

### 4.3.8 Interpretive Structural Model (ISM) Output

To explore the relationships between the issues raised and how to address them, an interpretive structural model was conducted. The interpretive structural model presents an unbiased way to analyse the relationship between all prioritised objectives presented by the group, to come up with prioritised requirements.

The rigorous process of ISM began by taking prioritised objectives from the nominal group technique sessions as input to develop a structural self-interaction matrix. As part of the process, the antecedent set analysis revealed the relationship and

influences within prioritised objectives. The model shows that openness to change is directly influenced by improvement in trust due to increasing awareness of MFS operations and security controls. It also reveals policies that foster better coordination of information sharing, like an industry-wide security operations centre, will drive improvement in awareness and mitigate infrastructural-related vulnerabilities. A detailed output of the ISM is presented in Appendix I.

### 4.3.9 Semi-Structured Interview Expert Validation Results

A lot of useful insights were revealed from the SSM and IM workshops conducted. The ISM also showed the relationships and impact of the factors for addressing cybersecurity on one another. The expert review further fine-tuned the requirements for improving cybersecurity in MFS based on the output from the workshops. The semi-structured interview requested participants to list key players in the ecosystem and explain their roles. In response, the list provided tallies with what was captured in the SSM. The only additions were the breakdown of various categories of end-users and the addition of intermediary institutions like switching companies. The experts expressed their satisfaction in terms of critical stakeholder identification in the ecosystem as presented in the SSM. The second question requested experts add any element they believe was omitted from the SSM. In response, experts requested that some of the components be further decoupled to enable the implementation of specific responses to issues. The experts believed addressing communication failures, partial commitment in the event of infrastructure failure, and the need to expand infrastructure to the underserved are gaps that should be addressed to better information flow. Furthermore, human factor issues raised by the experts largely align with what was identified in the SSM workshops. They noted the importance of improving trust and addressing concerns related to unsecured third-party applications, irregular applications, OS updates, and compliance-related concerns. In addition, the experts felt addressing sociocultural and behavioural concerns should also be addressed. They believed developing a secure mobile app with forensic capability, and ensuring the app is kept updated, is important to achieving the objective. They suggested the need to “harden” the user interface and ensure the security controls are usable. They also suggested the use of biometric authentication as much as possible. The semi-structured interview questionnaire and responses are attached in Appendix I.

The experts believe the ecosystem would benefit from a clearly defined role and responsibility. While they agree with most of the objectives of the SSM, they believe requirements to improve cybersecurity in the MFS ecosystem should prioritise improving trust by improving the usability of the MFS solution.

## 4.4 CHAPTER SUMMARY

This study highlighted domain-specific information from the perspective of players in the ecosystem with a view to developing usable security requirements for MFS. The need for security awareness by all stakeholders involved was echoed by almost all participating groups. The study has provided further insight into the MFS domain as it affects cybersecurity from various stakeholder groups, including regulators, potential MFS users, current MFS users, and solution providers, as highlighted in Figure 4.1.

While this PhD thesis focuses on improving usable security for MFS, this study has provided domain-specific context that would strengthen the development of usable security requirements.

# CHAPTER FIVE: USER BEHAVIOURS AND DEVOPS PRACTICES THAT IMPACT USABLE SECURITY IN MOBILE FINANCIAL SERVICES

## 5.1 INTRODUCTION

The investigation of the nature of usable security in MFS in sections 2.5 and 2.6 of this PhD thesis reveals that users' behaviours might lead to vulnerabilities in MFS. It emphasised that security design must have consideration for users' mental model, level of experience, and knowledge to be effective. Similarly, the literature highlighted that the perception of cybersecurity by end-users is crucial to addressing usable security.

Furthermore, the literature review in section 2.6 of this study also highlighted the need to examine usable security practices of supply-side actors like developers and the need to close the gap for empirical study of usable security behaviours of users and developers.

The MFS sociotechnical system study in Chapter Two provided insight into cybersecurity in the MFS domain and the need to improve awareness and information sharing in the ecosystem. This study sought to examine the behaviour of MFS users and the development practices of MFS providers with the aim of having better insight into usable security requirements that will improve usable security in MFS for users and supply-side actors like developers and others involved in developing and deploying MFS solutions. The supply-side actors will be referred to as DevOps stakeholders going forward. DevOps consists of stakeholders involved in the development and operations of the MFS solutions, like developers, systems administrators, quality assurance experts, and supply-side actors (Erich et al. 2017). The study would provide empirical evidence on usable security behaviours for users and developers.

## 5.2 STUDY DESIGN

The design of the study had consideration for both the end-user and DevOps. A mixed method was adopted for the studies, with surveys deployed for the end-user study and semi-structured interviews deployed for the supply-side studies, as highlighted in section 3.5 of this PhD thesis.

The survey questionnaire was developed based on usability, security, and usable security criteria derived from the literature (Ahmed et al. 2017, Hadlington 2017,

Muniandy et al. 2017, Ambore et al. 2018), and threat landscape review in Chapter Two of this thesis.

The survey instrument for the end-user surveys was deployed both electronically and via hard copies. The final questionnaire was deployed after it was piloted with 15 participants using the paper-based survey and 7 participants using the online version. Participants include both MFS users and non-users. The survey was administered physically in Nigeria and electronically.

Due to the nature of the population samples, it was imperative to design suitable studies for the selected stakeholder group. For MFS users, a survey was used as a tool for data collection, which was suitable for the large sample size, while data from the DevOps group was collected using semi-structured interviews. Another decision that was taken was to conduct two separate studies to enable each individual study properly address the peculiarity of the groups. The first study was called *the demand-side* study as it focused on demand-side actors, primarily the users. The second study was called the *supply-side* study as it focuses on supply-side actors; the DevOps team. The studies were conducted sequentially. The supply-side study was conducted after the demand-side. This provided additional insights to enable a more robust engagement with the supply-side actors. The study approach section provides details of both studies.

### 5.2.1 Study Approach: Demand-Side (End-User) Study

The cross-sectional time horizon for this study meant a choice of method that would be concluded within the time horizon of this PhD study. The MFS adoption and usable security literature examined in Chapter Two of this thesis deployed a survey questionnaire to gather end-user data. Adapting relevant constructs from the literature with input from the findings in Chapter Four, a demand-side questionnaire was designed. In addition to the background section, the instrument administered 43 main questions, 5 profile-based questions, and 21 secondary questions in 9 sections. Table 5.1 provides further details on the questionnaire that was deployed.

| # | Section | # of Questions | Question Type |
|---|---|---|---|
| 1 | Participants' details | 5 | Multiple choice |
| 2 | Product type and means of use | 8 | Multiple choice (4 singles, 4 "select all that apply") |
| 3 | Experience | 7 (One question had 6 secondary questions) | 1 Multiple choice, 6 Likert scale. All 6 sub-questions are also Likert scale |

| | | | |
|---|---|---|---|
| 4 | Awareness | 11 (Two questions have a combined 15 secondary questions) | 1 Multiple choice, 22 Likert scale, 2 Boolean |
| 5 | Maintenance | 6 | 2 multiple choice, 4 Likert scale |
| 6 | Usability | 4 | Likert scale |
| 7 | Security | 3 | Likert scale |
| 8 | Social context | 5 | 3 Likert scale, 2 multiple choice |
| 9 | Additional Information | 1 | Open-ended |

Table 5.1: Survey Instrument Description

The first section examined participants' profiles and economic conditions. The second section analysed infrastructure/transaction issues identified in the high-level requirement in section 4.5.7 and section 4.6.2 of this thesis. The section examined device type, transaction channels, and onboarding preferences. The behavioural question in this section examined the major drivers for the use of MFS by end-users. The section also examined the authentication options of the users. In addition to infrastructure and transactions, the “experience” section examined how various experiences of use influence users' usable security behaviours. For instance, one question examined the difficulty level of completing a financial transaction through MFS while another examined the rating of the complexity of the system. An entire section was dedicated to examining several dimensions of awareness. The section gauges awareness of privacy, awareness of basic cybersecurity expectations, risky behaviours, controls, and some other related items. The social context section examined the alignment of MFS and MFS security control to users' social interaction patterns, preferences, and environmental issues. Questions from the questionnaire align with all high-level requirements in section 4.6.2 which include awareness, infrastructure/transaction, process, and policy. Additionally, it also addresses behavioural and environmental issues based on the objective of the chapter. The questionnaire instrument is attached in Appendix II.

The process of developing the instrument included a pilot deployment with a small size of participants and a focus group review by senior academics. The review process also included a review of the time required to complete the questionnaire. The refined questionnaires required a maximum of 11 minutes and a minimum of 9 minutes to complete. The survey was deployed via emails, social media, and in-person. Out of 1000 surveys distributed, 698 feedback responses were received, 29 of which were from non-MFS users, representing the underserved stakeholders. The survey ran for two months after which 616 responses were analysed. Bristol Online

Survey (BOS), SPSS, and Microsoft Excel were the tools deployed to analyse the collated data.

#### 5.2.1.1 Survey Participant Profile

An analysis of the "participants' details" section of the survey instrument shows that all age demographics in financial services were represented in the distribution. The largest participating age group were aged 35-44, (36.7%), and ages 25-34, (35.6%). The elderly had the smallest representation at 1%. Table 5.2 shows the profile.

| **Age** | % |
|---|---|
| 18-24 | 20 |
| 25-34 | 35.6 |
| 35-44 | 36.7 |
| 45-60 | 6.7 |
| = or > 61 | 1.0 |
| **Educational Qualification** | % |
| Primary school certificate | 0.5 |
| Secondary school certificate | 8.4 |
| Diploma | 12.3 |
| Undergraduate degree | 42.7 |
| Postgraduate degree | 35.2 |
| Others | 0.8 |
| **Monthly income** | % |
| < = N 20,000 | 18.2 |
| N 21,000 – N 50,000 | 15.6 |
| N 51,000 - N 100,000 | 20.3 |
| N 101,000 - N 250,000 | 23.4 |
| N 251,000 - N 500,000 | 14.9 |
| >= N 501,000 | 7.6 |

Table 5.2: Participants' Profile. *1 USD exchanged for N315 during the study (N-Naira is the currency of use in the country where the study was conducted)

A descriptive statistical analysis was conducted on the survey data using SPSS to determine occurrence rates, mean, median, mode, and other descriptive statistics about the data. Furthermore, a bivariate analysis was conducted on the data to understand the relationship between the variables and their linkages. Also, an

exploratory multivariate analysis was conducted on the data using principal component analysis to reveal observed and latent variables from the responses.

To test the model fit and to analyse the impact of the variables on trust, a confirmatory factor analysis (CFA) and a structural equation model (SEM) were conducted using Analysis of Moment Structures (AMOS). AMOS-24 was chosen above SPSS in conducting CFA and SEM as it provides a graphic description and details not available in SPSS which only includes regression analysis details.

### 5.2.2 Study Approach: Supply-Side (DevOps) Study

DevOps in the context of this study represents experts who work in the value chain of mobile application deployment. The group consists of business requirement analysts, solution architects, software engineers, quality assurance, deployment, and maintenance experts. The providers of MFS solutions were under the broad category of *service providers* in section 4.4.2. To answer the question of this study, the first step taken was to determine and identify participants. The next step was to determine the type of data to collect from the study participants and to develop a data collection instrument that suits the purpose. The interview data were then analysed and validated. Most banks are at the forefront of mobile financial services development and also have long-term experience in financial services delivery. It was decided to interview the CIOs of those banks to understand their thoughts on the usable security of MFS. For the DevOps team, it was important to verify the track record of participants and this was done via upwork.com. Recruitment of most DevOps participants was conducted via the platform.

The phases of a typical software development lifecycle were used as a guide to critically examine usable security practices at all phases of MFS development. The section of the semi-structured interview developed mirrored these phases. Similarly, the phases of the IT procurement lifecycle were used as a guide to develop the semi-structured interview questionnaires for the bank's chief information technology officers (CIOs). Usability and security sections were included in both questionnaires. The choices of this approach were made with a focus on providing a step-wise way of analysing usable security decisions of these stakeholders based on practices they are familiar with. The DevOps semi-structured interview questionnaire has 45 questions while that of the CIOs had 39 questions. The questions are a mix of multiple-choice, Likert scale, Boolean, and open-ended questions. Table 5.3 shows the sections of the two questionnaires. The brackets beside the ticks show the only sections addressed by the questionnaire. No ticks mean the questionnaire did not include the section.

| # | Questionnaire Section | CIO Instrument | DevOps Instrument |
|---|---|---|---|
| # | Questionnaire section | | |
| 1 | Requirement/need analysis | √ | √(Requirement ) |
| 2 | Procurement and development practices | √ | √ (Development) |
| 3 | Design | | √ |
| 4 | Testing and product acceptance | √ | √ (Testing) |
| 5 | Deployment/decommissioning and configuration | √ | √ (Deployment and implementation) |
| 6 | Training and awareness | √ | √ |
| 7 | Maintenance and evaluation | √ | √ |
| 8 | Usability | √ | √ |
| 9 | Security | √ | √ |
| 10 | General | √ | √ |

Table 5.3: Semi-Structured Interview Instrument Details

The participants in both groups are busy individuals. For instance, to secure a CIO interview required an average of five contacts. Based on that, the questions had to be streamlined to be completed within the minimum possible time while not compromising the quality of engagement and feedback. The feedback from the interview was analysed using thematic analysis and card sorting. NVivo version 10 was used to conduct the thematic analysis, while UsabilitiTest was used to conduct card sorting. The semi-structured interview instruments for the CIO and DevOps are attached in Appendix II.

#### *5.2.2.1 Semi-Structured Interview Participant Profile*

The CIO group consisted of 15 bank CIOs in Nigerian banks that have deployed fintech solutions, specifically MFS. While 11 CIOs participated in person, 4 were represented by their deputies due to availability constraints. DevOps participants cut across 7 countries. This provides an avenue to compare practices from various markets. All phases of the system development lifecycle have at least one expert as a participant in the study. This enabled the researcher to examine any phase-specific differences in usable security practices. Developers are the highest number of participants in the DevOps group. Participants also have development expertise for the two major mobile phone operations systems, Android and iOS. Participants mostly have more than one expertise but have captured their expertise based on current projects or positions. The highest number of participants was from India, seven, while the lowest number was from UAE, Pakistan, Ukraine, and Serbia, one each. Table 5.4 provides details of participants from the DevOps interviews.

| # | Alias | Expertise | Years of Exp | | Gender | Location |
|---|---|---|---|---|---|---|
| 1 | USA1 | Business systems analyst | 10+ | | Male | USA |
| 2 | USA2 | Software tester/QA | 12 | | Male | USA |
| 3 | USA3 | Senior performance specialist | 13 | | Male | USA |
| 4 | USA4 | Senior cybersecurity expert | 15 | | Male | USA |
| 5 | AFR1 | Full stack developer | 15 | | Male | Nigeria |
| 6 | ASI1 | Mobile app developer | 6 | | Male | India |
| 7 | ASI2 | Mobile application developer (iOS) | 5 | | Male | India |
| 8 | ASI3 | iOS developer | 5+ | | Male | Pakistan |
| 9 | ASI4 | iOS developer | 4 | | Female | India |
| 10 | AFR2 | Software developer/trainer | 6 | | Male | Nigeria |
| 11 | ASI5 | Project manager | 9 | | Female | India |
| 12 | ASI6 | Front and back-end mobile developer | 9 | | Female | India |
| 13 | AFR3 | Software engineer | 5 | | Male | Nigeria |
| 14 | ASI7 | Android and iOS mobile developer | 4+ | | Male | India |
| 15 | AFR4 | Switching and routing | 7 | | Male | Nigeria |
| 16 | AFR5 | Software developer | 12 | | Male | Nigeria |
| 17 | EUR1 | UI/UX designer | 5 | | Male | Serbia |
| 18 | AFR6 | Business relationship expert | 8 | | Female | Nigeria |
| 19 | ASI8 | Quality assurance expert | 10 | | Female | India |
| 20 | ME1 | Solution architect | 8 | | Male | UAE |
| 21 | AFR7 | QA tester | 15 | | Female | Nigeria |
| 22 | EUR2 | QA engineer/tester | 4 | | Male | Ukraine |

Table 5.4: DevOps Study Participants Profile

In all, 60 participants accepted to participate in the interview, but only 22 eventually did. For the bank CIO group, 24 were contacted but only 15 accepted to participate. The major selling point for the recruitment of participants was explaining to them the potential impact of their participation in improving trust in MFS, consequently improving the quality of life of over 1.4 billion people globally. The apex financial services regulator in Nigeria was very instrumental in getting the CIOs to participate in the interview, while the DevOps were solely recruited by the researcher.

## 5.3 STUDY FINDINGS

This section presents findings from user experience in the usable security of MFS from a behavioural perspective. It also presents insights from principal component analysis (PCA), confirmatory factor analysis (CFA), and structural equation model

(SEM). PCA is a technique that helps in identifying the interdependence within variables. It highlights the relationships between observable variables and unobservable or latent variables. While PCA provides important insight into observable and latent factors that affect cybersecurity in MFS, CFA and SEM provide insight into the relationship of the PCA variables with trust.

### 5.3.1 User Behaviours and Impact on MFS Security

Analysis of variables from the survey findings provided insight into various aspects of user behaviours and their impact on usable security. For instance, respondents who had no form of training or awareness before they started using MFS outperformed those who had prior knowledge of the system. 60.1% of respondents who ensure their MFS application is up-to-date as a measure of preventing cybersecurity concerns and improving users had no prior knowledge or training on the MFS application before they had one. In terms of maintaining their MFS application to avoid cybersecurity concerns, irrespective of whether they receive any form of awareness or not, users generally exhibit good behaviour, as 57.4% of the respondents ensure their MFS application is up-to-date. On the other hand, 41.4% of respondents who received training before they started using MFS do not bother about regular updates. Only 13.8% of those who received any form of awareness before use always keep their MFS application up-to-date. Furthermore, those who have used the application for one year or longer performed better than those who have used MFS for a lesser duration, when it comes to keeping the MFS application updated, with 49.5% keeping the MFS application updated. Furthermore, 61.8% of respondents who received any form of awareness training in the use of MFS, believe the training was not sufficient, and they are 54.5% more likely to exhibit good application maintenance behaviour than those who believe it was sufficient.

The data was also analysed to understand the impact of awareness on usability, privacy, and security in the use of MFS. The result shows that respondents generally struggle with maintaining the privacy of their financial transactions on MFS as 79.7%

**Awareness of Privacy**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | high privacy | 125 | 20.3 | 20.3 | 20.3 |
| | low privacy | 491 | 79.7 | 79.7 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table 5.5: Level of Privacy Awareness

rated their privacy knowledge low. Table 5.5 shows a low level of privacy awareness among respondents.

The outlook was positive for usability and security as awareness seems to improve privacy and security. When the duration of use was applied as a variable as against the timing and sufficiency of awareness, the outcome showed that low privacy was still a concern while both usability and security get better with use. In the same vein, awareness and understanding of a consumer redress mechanism and transparency improves user trust in the system. While respondents prefer more stringent security

**Complexity**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | ease | 66 | 10.7 | 10.7 | 10.7 |
| | neutral | 8 | 1.3 | 1.3 | 12.0 |
| | complexity | 542 | 88.0 | 88.0 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table 5.6: Complexity of MFS Security Controls

control to financial loss, they believe not much should be required from genuine users to access the system. They believe no matter how complex the security mechanism is, users should not require more than just a PIN to unlock the security. Users are likely to compromise privacy to improve memorability as most respondents tend to write down login credentials to enable easy recall. Table 5.6 shows users' perception of the complexity of MFS security controls.

Only about 13% of the respondents believe MFS was challenging to use, and 20.8% of the respondents perform a single task several times due to the complexity of the MFS. 12.6% of the respondents believe the reason they need to complete a task more than once was a lack of sufficient knowledge of how to use the system. 44.2% think MFS meets their needs and 18.3% believe MFS is secure. 26.6% of MFS users often experience errors in their transactions.

Older respondents (60 years and above) tend to recall their authentication credentials more than younger respondents. 26.6% of respondents tend to forget their login credentials easily. Most participants have a below-average understanding of cybersecurity attacks (mobile malware, smishing, spyware, ransomware, etc.) and how to mitigate them. Table 5.7 shows the details of respondents' understanding of cybersecurity problems in MFS and how to mitigate them.

**Cybersecurity**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | None | 152 | 24.7 | 24.7 | 24.7 |
| | Basic | 148 | 24.0 | 24.0 | 48.7 |
| | Average | 119 | 19.3 | 19.3 | 68.0 |
| | Above average | 97 | 15.7 | 15.7 | 83.8 |
| | Advanced | 76 | 12.3 | 12.3 | 96.1 |
| | Expert | 24 | 3.9 | 3.9 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table. 5.7: Cybersecurity Vectors and How to Mitigate Against Them

A similar number of respondents (27%) write down their login credentials on their phones to enhance easy recall.

Only 78 of the respondents (about 12%) have experienced unauthorised access to their MFS accounts. Out of this group of respondents, 69% share their phones with their acquaintances, and out of the 88% that have not experienced unauthorised access to their MFS, 62% also share their phones with their acquaintances. The group of respondents that have experienced unauthorised access to their MFS were overwhelmingly (86%) satisfied with the control put in place to mitigate unauthorised access to their MFS solutions.

### 5.3.2 Observable and Latent Variable Analysis Result

The section presents a PCA analysis of observable and latent variables impacting cybersecurity in MFS.

Analysis of feedback from the completed surveys generated 106 variables from respondent feedback from the 43 survey questions deployed. PCA was applied to the

variables as it helps reduce the dimensionality of large data sets like the one generated from this survey. PCA was applied to transform the large set of variables into six, as described in Table 5.8. PCA was preferred to a similar technique like factor analysis (FA) because while both are reduction techniques, PCA analyses all the variance of data and FA focuses on common variance to indirectly measure underlying constructs.

| # | Variable | Description | Alias |
|---|---|---|---|
| 1 | Complexity of system | Measures user perception of the complexity of MFS and its security mechanism | CS |
| 2 | Awareness of privacy | Measures awareness of privacy in the use behaviour of MFS. | AP |
| 3 | End-user patching | Measures user behaviour in maintaining critical updates for MFS, mobile phone antivirus, and underlying mobile phone operating system | EP |
| 4 | Usability | Measures user perception of usability of MFS | U |
| 5 | Security | Measures user perception of security of MFS | S |
| 6 | Environmental impact | Measures impact of environmental factors on usable security of MFS | EI |

Table 5.8: Six Observable Variables

The descriptive statistics of the component show that environment (1.7) and security (1.9) have the lowest standard deviation while complexity (6.6) and patching (5.6) have the highest standard deviation. Analysis of the correlation matrix shows that the complexity of the system negatively impacts all variables except maintenance behaviours. Awareness of privacy has a positive correlation with three variables — usability, security, and environmental factors — but has a negative correlation with complexity (-0.376) and patching (-0.100). Maintenance behaviour has a positive correlation with all other variables except for the awareness of privacy (-0.100) where it has a negative correlation. Usability has a negative correlation with complexity (-0.302) but has a positive correlation with other variables. Both usability and security have the highest positive correlation with each other (0.552) when compared to other variables on the matrix. Details of the descriptive statistics and correlation matrix are attached in Appendix II.

The Kaiser-Mayer-Olkin (KMO) measure of sampling adequacy shows a 36% variation in sampling adequacy. The model was optimised to account for the variation and examine commonalities within components by examining correlation on latent components. The model was optimised to account for 82% variation to make the model a good fit. The first component (complexity) accounted for 33.788 of the variances. The cumulative value for item two (awareness of privacy) accounted for 55.817%. The third component accounted for 71% while the fourth accounted for

| | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings[a] |
|---|---|---|---|---|---|---|---|
| Component | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total |
| 1 | 2.027 | 33.788 | 33.788 | 2.027 | 33.788 | 33.788 | 1.833 |
| 2 | 1.322 | 22.029 | 55.817 | 1.322 | 22.029 | 55.817 | 1.126 |
| 3 | .931 | 15.514 | 71.331 | .931 | 15.514 | 71.331 | 1.055 |
| 4 | .685 | 11.421 | 82.751 | .685 | 11.421 | 82.751 | 1.421 |
| 5 | .602 | 10.026 | 92.777 | | | | |
| 6 | .433 | 7.223 | 100.000 | | | | |

Table 5.9: Total Variance Explained. Extraction Method: Principal Component Analysis.

82.75%. Table 5.9 provides details on the total variance.

Furthermore, commonalities indicate the percentage of variance accounted for by each variable. Environmental contributed the most during the decomposition with a value of 0.987, while privacy had the lowest value of 0.605. Table 5.10 provides details on commonalities.

| | Initial | Extraction |
|---|---|---|
| Complexity | 1.000 | .662 |
| Privacy | 1.000 | .605 |
| User Patching | 1.000 | .638 |
| Usability | 1.000 | .702 |
| security | 1.000 | .686 |
| Environmental | 1.000 | .987 |

Table 5.10: Commonalities Extracted by PCA

A scree plot was generated to further examine the latent variables. The plot shows that the first three slopes were steep and the last two slopes did not show sufficient variation between the eigenvalue and number of components. This implies the components that explain the variation lie within the first three slopes. The total number of points within the three slopes is four. To further investigate the relationship between the observable and latent construct a pattern matrix was generated, as shown in Table 5.11.

| | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Usability | .869 | | | |
| Security | .841 | | | |
| Patching | | .947 | | |
| Environmental | | | .992 | |
| Privacy | | | | .973 |
| Complexity | -.388 | .316 | | -.526 |

Table 5.11: Pattern Matrix -Extraction Method: Principal Component Analysis

The pattern matrix shows a strong positive loading of usability (0.869) and security (0.841) on the first component. However, complexity loads negatively on the same component. Patching only loads on the second component, but has a strong positive correlation with the component. Similarly, environmental (0.992) and privacy (0.973) also load positively on one component each. Complexity is the only variable that loads on more than one component with a negative correlation on two of the components and a positive correlation on one component.

Furthermore, to analyse the impact of the variables on trust, a structural equation model (SEM) linking the constructs with trust was developed. The model shows the correlation of all observable factors to usability and security and their relationship to trust. The maximum likelihood estimate (MLE) for the SEM shows that though usability and security have a significant influence on trust, security (0.263) has a much higher impact on trust when compared to usability (0.055). The model also shows that security loads more on end-user patching (0.785), the highest of any of the components. On the other hand, there is a significant inverse relationship between

the usability and complexity of the system (-0.735). The SEM result shows that a good fit was achieved for the model, as follows:

I. CMIN/DF (relative chi-square) = 11.763 [dropped too many paths if >3]
II. GFI (goodness of fit index) = 0.938 [ideal should exceed 0.9 for a good model]
III. NFI = 0.940 [above .95 are good]
IV. RFI = 0.895 [close to 1 indicates a very good fit]
V. IFI = 0.945 [close to 1 indicates a very good fit]
VI. TLI = 0.903 [close to 1 indicates a very good fit]
VII. CFI = 0.945 [close to 1 indicates a very good fit]
VIII. RMSEA (root mean square error approximation) = 0.132 [ideal should be <0.5 for good fit]
IX. RMR = 1.565 [for comparison smaller is better]

### 5.3.3 Supply-Side (CIOs and DevOps) Study Results – Interviews Findings

Only 30% of bank customers have an MFS. The least MFS adoption rate was 16% while the highest was 65%. Participants reported that most MFS issues customers deal with are related to authentication, transaction failure, feedback-related concerns, infrastructure, usability, and availability-related issues. Some of the banks regard Unstructured Supplementary Service Data (USSD) payment as a form of MFS. Banks have various motivations for deploying MFS. While some deploy as a competition strategy, some deploy as part of the overall business strategy. Cost optimisation was at the centre of some deployments. The need to decongest the banking hall was also an important objective. All banks have a customer need analysis process for MFS deployment but only two banks have a process for a rigorous collection of market data to ensure customer needs are well captured. Usability and security requirements were captured by all banks during the need analysis phase. However, the internal control team is responsible for ensuring the appropriate security requirements. There was no team responsible for usability requirements.

The participants overwhelmingly believe there is a need to implement usability and security together during system development as implementing both separately will make both weak. Specifically, one of the participants responded thus: “Security and user experience should be addressed together to create a balance between control and good customer experience otherwise, the control may become too stiff and staring users in the face, making adoption difficult and product un-usable”. Another participant noted that “both should be addressed together to achieve a balance. Poor security or excessive security deployments could impact usability negatively and vice

versa". The key word that came out of usability and security was "balance". To make both effective, participants believe balance is important.

The participants reported that some of the guidelines they adhere to during product development include secure coding principles, The Open Web Application Security Project (OWASP), Software Development Lifecycle (SDLC) framework, Payment Card Industry Data Security Standard (PCI-DSS), ISO 2000, extant regulatory standards and guidelines, and some standards to strengthen security through authentication. Some participants define security as part of usability criteria. Before deployment, most MFS pass through quality assurance which includes simulating different threat scenarios through vulnerability assessment and penetration testing.

Usability and security were identified by participants as important for the development of a secure MFS. Consideration for both is done right from needs analysis. Compliance with standards and regulations was emphasised as a way of integrating usability and security in the development process. Threat landscape analysis and various types of tests are also used to ensure both usability and security is addressed in systems development. While issues around authentication, transaction failures, and lack of transparency in transaction status continue to negatively impact adoption, participants observe that integrating usability and security in the design of MFS will address some of the issues raised.

### 5.3.4 Usable Security Imperatives for Mobile Financial Services

To further understand the imperatives of usable security from the viewpoint of the CIOs and the DevOps team, a thematic analysis was conducted as described in section 3.4.1.4 of this study following the guidance provided on thematic analysis by Braun and Clarke (2019), which includes analysing the data, developing suitable codes, developing themes inductively or deductively, reviewing the generated themes and providing exemplars from interview data. Card sorting was also applied to assist in analysing the data as described in section 3.4.1.5. The outcome of the thematic analysis is herewith presented as subsections of this section.

#### *5.3.4.1 How to Approach Usability and Security in MFS*

i. Implementing usability without downplaying security and vice versa

Participants currently have consideration for both usability and security when developing MFS. Most participants include this in their requirement and need analysis phase and have consideration for both through the system development lifecycle. Some participants focus usability requirements on the voice of the customer while some develop these requirements as part of customer feedback or as a reaction to

competition. While both usability and security are important, it is difficult to achieve both at the desired level, in practice. Buttressing this point, one of the participants mentioned that “Usability and security are two ends of the pole. One must be compromised for the other to achieve extreme value. E.g. if you want good security on Mobile Financial Services, you might need to use two-factor authentication for every step, which is very secure and highly cumbersome. On the other hand, if you want high usability, and want to navigate freely from function to function, you will not require that level of security, or at best only when you need to move value.” However, for usability and security to be effective, balance is important. To achieve a good balance between usability and security it is best to have an approach of implementing both together as a single requirement not as a separate requirement as currently practiced. At the minimum, usable security requirements should address security, assurance, updates, availability, integrity, and usability.

ii. A documented approach is required for usable security in MFS

While various good practices exist on how to implement usable security, the application is based on the experience of the DevOps team member, the time horizon and urgency for solution development, and the savviness of the procuring entity. Participants believe a documented approach on how to address usable security in MFS will strengthen its impact. To emphasise the need for a documented approach one participant from the DevOps team noted as follows, “A documented approach to finding an optimal balance between these important concepts will greatly assist developers and project owners in developing successful mobile apps for financial services.”

iii. Usable security will improve trust in MFS

Improvement in usable security will improve trust in MFS. “User confidence” was used to describe a situation where users were comfortable using MFS because the usable security requirement was addressed in development. Participants believe providing a level of assurance for usable security will improve trust in MFS.

iv. Roles and responsibilities for usable security need to be clearly defined within DevOps

Clear roles and responsibilities must be defined to ensure usable security requirements are considered in the entire lifecycle of solution requirement. While most banks have internal control teams to address security requirements for the backend, security during MFS development might be left to the developer who might not be well-equipped to do the right thing. Similarly, usability at times is left to the UX team

where one exists. The developer is responsible for it sometimes, while users might only have the full experience during the pilot, where changes are likely to cost more.

#### *5.3.4.2 Designing MFS for Usable Security*

i. Usable Security Requirement

Usable security requirements should be properly captured and considered during every phase of the development lifecycle. The requirement should not be restricted to knowledge of the development team or “internal customers” but should incorporate input from extensive user surveys.

ii. Impact of development methodology on usable security

Though the predominant development methodology for MFS development is the agile methodology, there is no evidence that any methodology is better than others in improving usable security. Buttressing the inherent provision in methodology to improve usable security even when a change is required, one of the participants noted as follows: “The agile methodology, which provides backtracking at every end of development, means that new modules can be added whenever the client wants.” Another participant shared the following thoughts: “Agile development tends to reveal security loopholes at early stages of development before it becomes expensive to effect the necessary changes to address it.”

iii. Scope of usable security

Participants attempted to define the scope of usable security in MFS. While a usable security approach would benefit the translation of human activity systems into addressing real-world concerns, the scope for usable security in the design of MFS should cover technical requirements, functional requirements, transition requirements, and continuous improvement plans, all of which should originate from stakeholder need analysis.

iv. User-focused and user-centred

Though usable security is about the usability of security control, it is more about protecting the legitimate human actor in the cybersecurity value chain. As such, usable security considerations should be from a human perspective. The mental model of the users, their behavioural patterns, and the nature of frequently raised complaints by existing and prospective users should be considered when designing MFS for usable security. Any good approach for usable security should have a

consideration for the involvement of users from need analysis to customer satisfaction rating as part of quality assurance.

v. Proportionality in usable security

Usable security is not one size fits all. One of the biggest challenges that should be addressed during design is ensuring that usable security in MFS is proportionate to the user's knowledge and experience in the use of MFS, mobile, and technology generally.

#### *5.3.4.3 Communication and reliability of transaction information*

i. Transparency in usable security

Security controls hardly “communicate” to users. Understanding security controls is often presented as exclusive to experts. MFS security control should be transparent to users in such a way that users will understand when it is activated or not and what it affects.

ii. A good feedback mechanism improves trust

Transaction failures and lack of feedback from some transactions are two of the highest complaints received from MFS customers. Unfortunately, feedback mechanisms have been weak and ineffective. A robust feedback mechanism will improve trust in MFS. One user proffered guidance on how to address the feedback issues: “Make sure the transaction is fully complete or track the transaction status.”

iii. Reliability and Integrity

Users consider MFS unreliable if it cannot provide adequate feedback on transactions. Lack of proper feedback also affects the integrity of financial transactions in MFS. One of the participants expressed his concern about reliability issues: “Some of the applications destroy the session so the user needs to log in again.”

#### *5.3.4.4 Addressing Quality-Related Concerns through Appropriate Requirement Elicitation*

i. Compliance to standards

While the need for compliance was agreed upon by participants, how to ensure adherence to such standards is a concern in a developing environment where a top priority is time to market. Addressing compliance will improve privacy and address

third-party-related risks amongst other benefits. Buttressing the gap in lack of enforcement of extant standards, one developer said he ensures “compliance by heart”, meaning that he implements only the standards he deems necessary.

ii. Measurement of quality

To ensure quality in MFS, a robust requirement elicitation process is important. In addition, to ensure continuous improvement, the measurement of factors that impact quality needs to be addressed. Some of these quality measurements include transaction error rates, consistency, customer satisfaction, effectiveness and efficiency, deviation from standards, and usability and security variables.

#### *5.3.4.5 Dealing with Environmental Factors that Affect Usable Security*

i. Transaction channel security

Transaction channels are the platform leveraged to access MFS. The update and maintenance of the mobile app itself if not timely and properly done could be exploited by cyber criminals. Upgrades are meant to address system vulnerabilities, but in some instances, they create vulnerabilities themselves. User feedback from some of the app stores shows user frustration with some updates. Similarly, the Unstructured Supplementary Service Data (USSD) has become a channel for reaching customers without smartphones. Other customers have also found it convenient to use. However, the USSD has known vulnerabilities that should be addressed so that the financial transactions of users are not compromised. DevOps teams conduct threat landscape analysis to enable them identify vulnerabilities associated with transaction channels so that they can be addressed. User awareness of some of these vulnerabilities, and good cybersecurity behaviours on the part of users, can help in mitigating this.

ii. Consumer redress mechanism

While all participants indicated the availability of a customer redress function in one form or the other, it was obvious that existing mechanisms were not sufficient, as they at times did not meet user expectations or were modelled after a normal banking customer service approach and given the same priority as other customer complaints. It was noted that cybercrime is fast, it can lead to immediate loss of value, and it has a real and direct negative impact on the human condition and should be treated as such. It was agreed that for a consumer redress function to be effective, it should consider the specific characteristics of all customer bases and provide robust feedback and tracking mechanisms.

iii. User support and awareness

User support and awareness have resonated throughout this study. Participants believe a robust awareness programme will improve usable security for the user and even the developer of the system. MFS providers should ensure such a programme as part of their adoption drive. While most MFS have frequently asked questions (FAQs) on cybersecurity, they are lumped with frequently asked questions for other aspects of use. It was suggested that the frequently asked questions on cybersecurity for MFS should be separated from the other questions and presented in a simple way that can easily be understood by all customers. MFS providers are also encouraged to provide and equip a customer service section on their app that specialises in addressing cybersecurity-related issues. While all these measures would improve usable security, it was agreed that MFS solutions and their security control should be implemented in such a way that it would empower users to get the support they need by themselves and only escalate on rare occasions.

iv. Others

The growth of MFS was based on the ubiquitousness of mobile technology. Mobile network carriers make it possible for phone operating systems and apps to be updated. Delays in these updates might lead to vulnerability. One issue raised by participants is the concern with the failure of the internet services. They suggested that it is important to check signal strength before commencing any financial transaction on the mobile phone. Phones can get missing. However, standards exist that enable remote wipe, should this happen. Mobile financial services providers are expected to educate their customers on this. Furthermore, there are peculiarities with the mobile phone that might affect the security of financial transactions using mobile phones. MFS providers ought to address them so they don't lead to cybersecurity concerns for users. Ensuring high availability in the MFS system is a shared responsibility between MFS solution providers and service providers. The responsibility to ensure that should be spelled out to ensure users have a more seamless experience. DevOps team members attached various levels of importance to usability and security factors. To ensure efforts are channelled to the ones that have the most impact on users and the systems, the user perspective on these factors should be paramount.

## 5.4 CHAPTER SUMMARY

This chapter examined how the use behaviour of MFS impacts usable security. It also examined how the use practice of two key supply-side actors, the chief information officers and the DevOps team, affect usable security in MFS.

The study uncovered user behaviours and DevOps practices that affect the usable security in MFS. For instance, while participants indicated that they would prefer a more secure system than a usable one, they also value convenience and ease of use. Although participants demonstrated an above-average theoretical understanding of cybersecurity, their actual security decisions did not align with this knowledge. Users found the security mechanisms of MFS to be complex. Additionally, DevOps participants highlighted the need for clear guidelines to help developers seamlessly incorporate usable security into system design. This observation aligns with findings from the literature review in Chapter Two (Nocera et al., 2023), which emphasised the necessity of comprehensive design guidelines and requirements for usable security.

This study has provided empirical evidence of user behaviour and development practices that would facilitate the development of usable security requirements for MFS.

This chapter contributes to the second objective of this PhD thesis namely “To contextualise the problem space from the perspective of MFS stakeholders”. It also forms an input into the third objective, “To design and develop an approach to address usable security solutions for mobile financial services based on the requirement developed, together with an implementation approach”.

# CHAPTER SIX: REQUIREMENTS FOR USABLE SECURITY HEURISTICS

A major gap identified in the literature review is the lack of requirements for usable security, which can help developers easily integrate usable security into the development process, as highlighted in Chapter Two of this study. While Chapter Four has identified some domain-specific requirements for the MFS ecosystem, Chapter Five identified requirements related to user behaviour and development practices. This chapter seeks to develop usable security requirements leveraging findings from literature and studies conducted in Chapters Four and Five.

The chapter seeks to highlight the requirements for usable security in MFS and prioritise them, leveraging the must-have, should-have, could-have, won't-have (MoSCoW) technique, which was originally developed to assist teams in prioritising tasks within the rapid application development (RAD) project. MoSCoW was preferred over other prioritisation techniques like the Analytical Hierarchy Process (AHP), Kano Model, and bubble sort techniques because it is more effective in an Agile environment and works better in a resource-constrained environment (Miranda 2022). Specifically, this chapter sought to:

1. Define requirements: The study aims to provide a clear and comprehensive set of requirements for the development of usable security heuristics for mobile financial services. It outlines the functional, non-functional, technical, and transition requirements, covering various aspects of issues raised in Chapters Four and Five of this thesis.
2. Prioritise requirements: The study applied the MoSCoW prioritisation technique to categorise requirements as must-have, should-have, could-have, and won't-have. This prioritisation helps stakeholders understand the criticality of each requirement and guides decision-making in the development process.
3. Validation and approval: The study serves as a basis for validating and approving the requirements. It outlines the process of how the requirements were gathered, validated, updated, and approved across all stakeholders. This ensures that the requirements meet the necessary criteria for implementation and are aligned with the project objectives.
4. Provide reference and documentation: The document aims to serve as a reference for all the identified requirements. It provides an overview of the requirements, categorises them based on different perspectives, and includes

a detailed description of each requirement. This ensures that the requirements are well-documented and can easily be accessed and referred to throughout the development lifecycle.

By achieving these aims, the requirements set a foundation for the development of usable security heuristics for mobile financial services.

## 6.1 REQUIREMENTS SCOPE

Considering the aims and objectives of this study, as well as the derived research questions, vis-à-vis the various applicable domains of usable security heuristics, it was necessary to define the scope of this requirement-gathering phase, as this will impact the kind of requirements gathered and their application. As such, the in-scope and out-of-scope definitions are presented hereafter:

**In Scope:**

- Functional requirements for security heuristics: This includes identifying and documenting the specific functionalities and features that the usable security heuristics for mobile financial services should encompass. It involves capturing the necessary actions, behaviours, and interactions required for a secure and usable system.
- Non-functional requirements: This focuses on the usability aspects of the security heuristics, such as the system's performance, responsiveness, user interface design, and user experience. It ensures that the security measures are user-friendly, intuitive, and effective.
- Technical requirements for implementing heuristics: This involves identifying the technical specifications and considerations necessary for implementing the security heuristics. It includes aspects such as technology platforms, programming languages, security protocols, and integration requirements.
- Transition requirements for a smooth deployment: This encompasses the requirements and considerations for transitioning from the current system to the new security heuristics. It includes data migration, system configuration, user training, and any other aspects necessary for a seamless transition.
- Prioritisation of requirements using MoSCoW: This involves prioritising the requirements based on the MoSCoW technique, categorising them as must-have, should-have, could-have, and won't-have. It helps in identifying and focusing on the most critical and high-priority requirements.

- Validation and approval processes: This includes reviewing, validating, and obtaining approval for the requirements. It involves engaging stakeholders, gathering feedback, and ensuring that the requirements are complete, consistent, and aligned with stakeholder expectations.
- Requirement documentation: This involves establishing a structured process for managing and documenting the requirements throughout the project lifecycle. It includes change management, version control, traceability, and maintaining accurate documentation of the requirements.

Business requirements aim at the overarching business objectives, functional requirements concentrate on the system's functions and user interactions, while non-functional requirements emphasise system performance and quality attributes.

**Out of Scope:**

- Detailed system design and architecture: The requirement-gathering process does not delve into the specifics of system design and architecture. It focuses on capturing high-level requirements rather than the technical implementation details.
- Implementation specifics and coding details: The requirement-gathering process does not involve specifying the detailed implementation approach or coding details for the usable security heuristics. It focuses on defining the functional and non-functional requirements rather than the technical implementation specifics.
- Infrastructure and network considerations: The requirement-gathering process does not encompass the infrastructure and network considerations necessary for implementing the security heuristics. It focuses on the requirements from a user-centric perspective rather than the underlying infrastructure.
- Financial institution-specific regulations and compliance: The requirement-gathering process does not address the specific regulations and compliance requirements of individual financial institutions. It focuses on the general principles and best practices rather than the institution-specific legal and regulatory aspects.
- Backend system integrations and data migrations: The requirement-gathering process does not encompass the detailed requirements for backend system

integrations or data migrations. It focuses on the user-facing requirements rather than the technical aspects of integrating with existing systems or migrating data.

- Mobile device hardware and operating system functionalities: The requirement gathering process does not include the requirements related to mobile device hardware or operating system functionalities. It focuses on the usable security heuristics at the application level rather than the device-specific features.

- Business process re-engineering beyond the usable security heuristics: The requirement gathering process does not encompass extensive business process re-engineering beyond the scope of the usable security heuristics. It focuses on the requirements directly related to security and usability rather than broader business process improvements.

- Training and user adoption strategies: The requirement-gathering process does not include detailed requirements for training or user adoption strategies. It focuses on capturing the functional and non-functional requirements rather than the specific training programmes or change management strategies.

## 6.2 REQUIREMENT GATHERING APPROACH

This section presents the approach that was employed to gather and document requirements for this study, with particular attention to incorporating best practices from the field of business analysis and aligning with industry standards.

For this thesis, the requirement-gathering approach adopted the framework proposed by the International Institute of Business Analysis (IIBA). The IIBA approach is widely recognised and utilised in the field of business analysis, providing a comprehensive and structured methodology for gathering requirements. Indeed, the IIBA approach stands out for its emphasis on stakeholder collaboration and the utilisation of various techniques for eliciting and documenting requirements. It aligns with industry best practices and offers a systematic framework that ensures a thorough understanding of stakeholder needs and project objectives (Gobov 2020). It can be surmised that by adopting the IIBA approach, this PhD study will benefit from its established guidelines and techniques, leading to more effective requirement gathering and documentation.

It is also important to note that the IIBA approach emphasises the importance of documentation, providing guidelines for creating clear and unambiguous requirement artefacts such as business requirements documents (BRDs), which is essential to this

study (Lal 2020). These artefacts serve as a valuable reference throughout the project lifecycle, enhancing communication, and minimising misunderstandings.

As a result of adopting the systematic approach to requirement gathering, documentation, and management outlined by the IIBA, the following steps were taken:

1. Identify stakeholders: The first step in the requirement-gathering process is to identify the key stakeholders who will be involved in the project. The stakeholder identification has already been conducted in Chapter Four of this study. Their input and perspectives will provide valuable insights for understanding the requirements and achieving the objectives of this thesis.

2. Plan requirement gathering: A well-defined plan is essential to ensure an effective and systematic approach to requirement gathering. This is a major first step in the development of the heuristics.

3. Elicitation techniques: A combination of techniques were applied in Chapters Four and Five of this study to elicit requirements, some of which include user surveys and semi-structured interviews.

4. Prioritisation of requirements using the MoSCoW technique: After gathering requirements, the MoSCoW technique was employed to prioritise them. The prioritisation process involved engaging stakeholders to assess and assign the appropriate MoSCoW priority to each requirement.

5. Document requirements: The gathered requirements, including their prioritisation using the MoSCoW technique, were carefully documented to ensure clarity, accuracy, and traceability.

6. Validation: The documented requirements, including their MoSCoW prioritisation, went through a validation process to ensure their completeness, consistency, and alignment with stakeholder expectations. Validation was conducted through review sessions with stakeholders, where feedback and suggestions for improvement were collected.

## 6.3 STAKEHOLDER ANALYSIS

The objective of the stakeholder analysis in this chapter is to analyse how the requirement would benefit various stakeholder groups. During the problem contextualisation phase a stakeholder analysis of the mobile financial services sociotechnical system was conducted to understand the key stakeholders in the ecosystem and gather information on cybersecurity concerns in MFS from their point

of view. The stakeholder analysis is presented in Table 4.3 of section 4.4.2. Feedback from this exercise formed an input into this requirement elicitation process. Furthermore, in Chapter Five, to understand the usable security behaviours of end-users and DevOps team members, further studies were conducted which also contributed to the requirement for developing usable security heuristics for MFS. The requirements gathered from stakeholders from Chapters Four and Five were tailored to meet the needs of financial institutions, the DevOps team, testers who would use the heuristics to evaluate existing systems, and end-users of the product. Table 6.1 shows details of revised stakeholders' analysis.

| # | Revised Stakeholder List | Stakeholders from Chapters Four and Five | Description | Role/Interest |
|---|---|---|---|---|
| 1 | Financial institutions | Financial services regulators, banks, CERT | Organisations providing financial services, such as banks and credit unions | Contribute to industry-specific requirements and workflows.<br><br>Ensure regulatory compliance.<br><br>Protect customer data. |
| 2 | DevOps | DevOps, infrastructure service providers | Professionals are responsible for implementing usable security heuristics in MFS applications and systems. | Translate design principles into practical solutions. |
| 3 | Testers | Quality assurance from the DevOps team | Individuals who will deploy usable security heuristics to evaluate existing MFS solutions | Conduct rigorous testing and identify vulnerabilities.<br><br>Provide feedback to improve usable security measures. |
| 4 | End-Users | Banked and underserved | MFS existing and potential end-users | Benefit from a more usable secure system |

Table 6.1: Revised Stakeholder Analysis

By conducting a comprehensive stakeholder analysis, this study acknowledges the diverse perspectives and contributions of financial institutions, developers, testers, and end-users in implementing usable security heuristics. Understanding their needs, challenges, and roles will guide the design and implementation process, ensuring that the final solutions effectively balance usability and security requirements.

## 6.4 REQUIREMENT CATEGORISATION AND PRIORITISATION

To effectively manage and analyse requirements, a classification framework based on industry best practices was implemented. The classification of requirements helped to organise and understand the different types and nature of the requirements provided by stakeholders. The following classification, based on widely recognised categories proposed by the IIBA was used: business requirements, stakeholder requirements, solution requirements (functional and non-functional), and transition requirements (Meredith et al. 2019; Hales 2014).

1. Business requirements: Business requirements represent the high-level goals, objectives, and needs of the stakeholders as a whole. They focus on the strategic and business aspects. These requirements address the "why" behind the study and provide the foundation for subsequent requirement activities (Weese and Wagner 2017).

2. Solution requirements: Solution requirements further elaborate on the business requirements and define the specific capabilities and features that the solution must deliver. Solution requirements can be further classified into functional and non-functional requirements (Weese and Wagner 2017).

    a) Functional requirements: Functional requirements describe the specific functionalities and behaviours that the solution must exhibit. They define what the solution should do to meet the business and stakeholder needs. Functional requirements are typically documented using techniques such as use cases, user stories, or process flows and focus on the system's expected behaviour, inputs, outputs, and interactions (Weese and Wagner 2017).

    b) Non-functional requirements: Non-functional requirements specify the qualities, attributes, or constraints that the solution must possess. They address aspects such as performance, security, usability, scalability, reliability, and regulatory compliance. Non-functional requirements provide criteria against which the solution can be evaluated beyond its functional capabilities. These requirements help ensure that the solution meets the desired quality standards (Meredith et al. 2019).

3. Transition Requirements: Transition requirements capture the necessary actions, activities, and considerations required to successfully transition from the current state

to the desired future state. These requirements focus on the implementation, deployment, and adoption of the solution (Weese and Wagner 2017).

By classifying requirements into these categories, the study effectively managed, prioritised, and traced the requirements from the problem contextualisation stage.

### 6.4.1 Business Requirements

A total of 14 business requirements were documented as shown in Table 2. These requirements serve as the premise for the stakeholder requirements and also serve as the catalysts for the solution requirements, which include functional and non-functional, as well as the transition requirements thereafter. Table 6.2 shows the business requirement based on findings from the problem space contextualisation.

| # | Business Requirements | Affected Stakeholders |
|---|---|---|
| **1** | Stakeholders should not have a hard time understanding or applying security mechanisms in MFS | Financial institutions, DevOps, testers, end-users |
| **2** | Security mechanisms in MFS should encourage good use behaviours, not discourage them. | DevOps, testers, end-users |
| **3** | MFS security mechanism should have considerations for all categories of users from novices to experts | Financial institutions, DevOps, testers, end-users |
| **4** | User trust in MFS should improve due to better usable security | Financial institutions, DevOps, testers, end-users |
| **5** | DevOps team members should have a documented approach to applying usable security principles in the development of MFS | Financial institutions, DevOps, testers, end-users |
| **6** | Testers should have a guide for evaluating usable security in MFS | Financial institutions, DevOps, testers, end-users |
| **7** | MFS transaction feedback should be more reliable and effective | Financial institutions, DevOps, Testers, End-users |
| **8** | MFS security should have consideration for user behaviours | Financial Institutions, DevOps, testers, end-users |
| **9** | MFS security should have consideration for DevOps practices | DevOps, testers, end-users |
| **10** | MFS security should have consideration for the human element | Financial institutions, DevOps, testers, end-users |
| **11** | Users should feel at home with security provisions when conducting MFS transactions | Financial institutions, DevOps, testers, end-users |
| **12** | DevOps members should feel empowered to apply security requirements and standards when developing MFS | Financial institutions, DevOps, testers, end-users |
| **13** | MFS security mechanism should be inclusive | Financial institutions, DevOps, testers, end-users |
| **14** | MFS solution should comply with all extant standards and guidelines | Financial institutions, DevOps, testers, end-users |
| **15** | MFS users should have sufficient awareness of cybersecurity | Financial institutions |

Table 6.2: Business Requirements

### 6.4.2 Solution Requirements

Considering the business and stakeholder requirements gathered thus far, the next set of requirements to be documented was the solution requirements, comprising of the functional, non-functional, and transition requirements as shown in Table 6.3, Table 6.4, and Table 6.5. A total of 83 requirements were gathered for these 3 requirement categories.

| Requirement | Type | MoSCoW |
|---|---|---|
| **The system shall ensure that no unauthorised access occurs to user transactions or data** | Functional | Must-have |
| **The system shall provide a mechanism to ensure that any change or modification to user data or transactions can be tracked.** | Functional | Should-have |
| **The system shall provide inclusive security controls** | Functional | Must-have |
| **The system shall offer adjustable security settings to allow users to customise the level of security.** | Functional | Should-have |
| **The system shall communicate to the user in a clear and understandable manner** | Functional | Must-have |
| **The system shall ensure status information is transparent and consistent.** | Functional | Should-have |
| **The system shall allow users to set their security preferences and customise security settings.** | Functional | Must-have |
| **The system shall provide users with the ability to modify some security choices** | Functional | Should-have |
| **The system shall support multiple authentication options.** | Functional | Must-have |
| **The system shall ensure that security does not add additional an burden to users** | Functional | Should-have |
| **The system shall have a communication channel with users.** | Functional | Must-have |
| **The system shall have robust error handling mechanisms to recover from errors and ensure reliable execution of security functions.** | Functional | Should-have |
| **The system shall provide help in such a way that it does not add additional work to users** | Functional | Must-have |
| **The system shall provide relevant security information and instructions without overwhelming the user.** | Functional | Should-have |
| **The system shall have consideration for accessibility** | Functional | Must-have |
| **The system shall provide alternative modes of interaction and accommodate users with visual or hearing impairments.** | Functional | Should-have |
| **The system shall have a mechanism to ensure trustworthiness.** | Functional | Must-have |
| **The system shall have a means of identifying rogue applications** | Functional | Should-have |
| **The system shall adhere to relevant industry regulations, data protection laws, and privacy policies.** | Functional | Must-have |
| **The system shall provide necessary audit logs** | Functional | Should-have |
| **The system shall have consideration for MFS user behaviours** | Functional | Must-have |
| **The system shall have consideration for various user mental models** | Functional | Should-have |
| **The system shall provide users with various options for security measures.** | Functional | Must-have |

| Requirement | Type | MoSCoW |
|---|---|---|
| **The system shall allow users to adjust security settings in a manner that will not compromise the system.** | Functional | Should-have |
| **The system should ensure the mobile app is updated** | Functional | Should-have |

Table 6.3: Functional requirement

| Requirement | Type | MoSCoW |
|---|---|---|
| **The system shall provide fast and responsive security controls and actions.** | Non-functional | Must-have |
| **The system shall handle concurrent user transactions efficiently and without significant performance degradation.** | Non-functional | Should-have |
| **The system shall have an intuitive and user-friendly interface for ease of use.** | Non-functional | Must-have |
| **The system shall minimise user cognitive load when interacting with security features.** | Non-functional | Should-have |
| **The system shall employ encryption mechanisms to protect user data during transmission and storage.** | Non-functional | Must-have |
| **The system shall enforce strong access controls to prevent unauthorised access to sensitive information and functions.** | Non-functional | Must-have |
| **The system shall implement secure authentication mechanisms to verify user identity and protect against unauthorised access.** | Non-functional | Must-have |
| **The system shall have mechanisms in place for monitoring and detecting security breaches or suspicious activities.** | Non-functional | Should-have |
| **The system shall ensure high availability and minimal downtime to facilitate continuous access to services.** | Non-functional | Must-have |
| **The system shall have mechanisms to recover from failures and restore data integrity in case of system disruptions.** | Non-functional | Must-have |
| **The system shall maintain consistent performance and functionality even under peak load conditions.** | Non-functional | Should-have |
| **The system shall be compatible with a wide range of mobile devices and operating systems.** | Non-functional | Must-have |
| **The system shall integrate with existing mobile financial service platforms and systems seamlessly.** | Non-functional | Should-have |
| **The system shall be scalable to accommodate an increasing number of users and growing transaction volumes.** | Non-functional | Should-have |
| **The system shall handle future enhancements and additional security features without significant performance degradation.** | Non-functional | Could-have |
| **The system shall be modular and well-documented to facilitate easy maintenance and future updates.** | Non-functional | Must-have |
| **The system shall have mechanisms to apply security patches and updates in a timely and efficient manner.** | Non-functional | Should-have |

| | | |
|---|---|---|
| **The system shall adhere to privacy regulations and protect user data from unauthorised access or disclosure.** | Non-functional | Must-have |
| **The system shall provide users with clear information about the collection, use, and sharing of their data.** | Non-functional | Should-have |
| **The system shall generate comprehensive audit logs for security-related events and actions.** | Non-functional | Must-have |
| **The system shall provide mechanisms for administrators to review and analyse security-related logs and reports.** | Non-functional | Should-have |

Table 6.4: Non-functional requirement

| Requirement | Type | MoSCoW |
|---|---|---|
| **Documentation shall be provided detailing the usable security heuristics** | Transition | Must-have |
| **A knowledge base or FAQ section shall be available to provide self-help resources for users during the transition.** | Transition | Should-have |
| **The usable security heuristics shall undergo thorough validation to ensure their effectiveness and reliability.** | Transition | Must-have |
| **Test scenarios and conditions should be effective and efficient.** | Transition | Should-have |
| **Mechanisms should be in place to collect user feedback on the usability and effectiveness of the usable security heuristics.** | Transition | Should-have |
| **Feedback from users and stakeholders shall be used to refine and improve the usable security heuristics through iterative processes.** | Transition | Could-have |

Table 6.5: Transition Requirement

The requirements gathered for the business, stakeholder, solution, and transition requirements were validated with the stakeholders, as presented hereafter, to confirm their relevance and validity before implementation. The validation exercise recommended modifications on eight out of the twenty-five functional requirements. It was suggested that one of the functional requirements should be deleted. The modifications were in terms of change in priority of the requirement from one level to another. Six changes were recommended for the non-functional, while four modifications were recommended for the transitional requirements as presented.

### 6.4.3 Requirement Validation and Approval

The validation and approval process for the business, stakeholder, solution (functional and non-functional), and transition requirements is crucial to ensure alignment, accuracy, and consensus among all stakeholders. This section outlines the steps taken to validate, and update, the requirements across all stakeholders involved in the development of usable security heuristics for mobile financial services.

1. Business Requirements Validation:

- The initial set of business requirements was gathered through the problem conceptualisation process and validated by subject matter experts.
- A thorough review and analysis of the gathered business requirements were conducted to ensure clarity, completeness, and feasibility.
- The business requirements were then presented to the stakeholders for validation, feedback, and further refinement.
- Feedback and suggestions from stakeholders were incorporated into the requirements, and any conflicts or discrepancies were resolved.

2. Solution Requirements (Functional and Non-functional) Validation
    - The solution requirements, including functional and non-functional requirements, were derived from the validated business and stakeholder requirements.
    - The solution requirements were reviewed by subject matter experts, architects, and DevOps teams to ensure their technical feasibility, compatibility, and alignment with industry best practices.
    - Feedback from the technical experts and DevOps teams was incorporated into the solution requirements, and necessary updates and refinements were made.
3. Transition Requirements:
    - The transition requirements, which address the process of transitioning to usable security heuristics, were reviewed by relevant stakeholders, including IT teams, project managers, and change management personnel. The transition requirements were validated through discussions,
    - Any necessary updates or adjustments to the transition requirements were made based on the feedback and input from the stakeholders.

Ultimately, the requirements were validated without amendments. However, recommendations for exclusions and alterations to requirement prioritisations were made to the functional, non-functional, and transition requirements, and 63.3% of the requirements were validated, with 14.4% removed for duplications and redundancies. Subsequently, the requirements were amended, re-validated, and confirmed, resulting in 52 final requirements used to assess the development, testing, and

adoption of usable security heuristics for MFS. Table 6.6 shows an extract of validated requirements. The detailed requirement documentation is presented in Appendix III.

| ID | Requirement | Type | MoSCoW | Validation Feedback |
|---|---|---|---|---|
| | | | | |
| **FR001** | The system shall ensure that no unauthorised access occurs to user transactions or data | Functional | Must-have | Validated |
| **FR002** | The system shall provide a mechanism to ensure that any change or modification to user data or transactions can be tracked | Functional | Should-have | Change to must have |
| **FR003** | The system shall provide inclusive security controls | Functional | Must-have | Validated |
| **FR004** | The system shall offer adjustable security settings to allow users to customise the level of security | Functional | Should-have | Change to must have |
| **FR005** | The system shall communicate to the user in a clear and understandable manner. | Functional | Must-have | Validated |
| **FR006** | The system shall ensure status information is transparent and consistent. | Functional | Should-have | Change to must have |
| **FR007** | The system shall allow users to set their own security preferences and customise security settings. | Functional | Could-have | Remove |
| **FR008** | The system shall provide users with the ability to modify some security choices during transactions. | Functional | Should-have | Should not only be for transactions |

Table 6.6: Definitive Requirement after Validation
FR= Functional Requirement.

## 6.5 CHAPTER SUMMARY

This requirement documentation serves as a comprehensive guide for developing usable security heuristics for mobile financial services. Through a systematic requirement-gathering process, involving stakeholders such as financial institutions, developers, testers, and end-users, the document outlines the functional, non-functional, technical, and transition requirements necessary to achieve secure and user-friendly mobile financial services. Additionally, by addressing the functional, non-functional, technical, and transition requirements and by considering stakeholders,

the document lays the foundation for a secure, user-friendly, and compliant mobile financial services system. The chapter contributes to achieving objective three (3) which sought to answer the question “What are the key usable security requirements for MFS?” This chapter also contributes to objective four (4): to validate the proposed approach through expert reviews, and objective five (5): to exploit and disseminate the validated solution including recommendations.

# CHAPTER SEVEN: DESIGN, DEVELOPMENT, AND VALIDATION OF USABLE SECURITY HEURISTICS

## 7.1 INTRODUCTION

Chapter Five of this study highlighted usable security requirements for MFS based on literature review and contextualisation studies in Chapters Four and Five of this PhD thesis.

This chapter sought to achieve the third objective of this PhD thesis, which is to develop an approach on how to integrate usable security consideration into MFS development to improve usable security for the end-user and DevOps stakeholders of MFS.

Section 2.6.2 of this study examined various approaches to achieving this integration, such as security-by-design, involving end-users in the development process, or developing heuristics. Heuristics development was preferred to other options because it provides a systematic approach to achieve this integration, facilitates timely detection of errors in solution development, and is adaptable to new situations. Furthermore, heuristics have been successfully applied to address both usability and cybersecurity problems in the mobile phone environment (Nguten et al. 2018). This study adopted an iterative approach, as proposed by Quinones and Rusu (2017), in developing usable security for MFS as it provides a streamlined approach for heuristics development compared to other methods (Quinones and Rusu 2017).

While other heuristics exist, to the best of my knowledge, no heuristics have been developed in the context of MFS, considering user behaviour and development practices. For instance, Nielsen's ten heuristics focus only on usability and do not consider security. Moreover, it has been argued that the heuristics would require an update to meet current usability needs (Gonzalez-Holland et al. 2017). Similarly, Feth and Polst (2019) have developed a set of heuristics that identified elements like *transparency, authentication,* and *user support.* This study took into cognisance such elements as indicated in, Table 7.1. However, these elements were further strengthened by findings from other studies. For instance, *transparency* in the context of MFS was expanded to include trust relationship between the user and the security mechanism and awareness of the status of their interaction with the mechanism (Gaehtgens et al. 2017; Eskandari et al. 2018).

This study developed heuristics for usable security for MFS building on existing heuristics with consideration for MFS user behaviour and DevOps perspectives.

## 7.2 STUDY DESIGN

The study took into consideration findings from studies in Chapters Four, Five and Six of this PhD thesis and adopted an iterative approach for the development of the heuristics: thematic analysis of literature for usable security evaluation. This is similar to the approach adopted by Feth and Polst (2019) where heuristics were developed by collecting data from the literature, and refining, categorising, and prioritising the collated data. Semi-structured interviews of experts were conducted and their feedback was incorporated into the development of the heuristics.

While literature shows that various approaches were adopted, all approaches involve a method of identifying the heuristics, ensuring the address of some identified requirements, and validating and refining the heuristics.

To achieve the objective of this study, an iterative approach was adapted as shown in Table 7.1.

| # | Steps | | Objective | Reference |
|---|---|---|---|---|
| 1 | Extract | Iteration I | To identify factors central to usable security in the use behaviour of MFS | Quinones and Rusu (2017)<br><br>Feth and Polst (2019) |
| | | Iteration II | To identify usable security factors by supply-side actors like the DevOps team and CIO | |
| | | Iteration III | To identify usable security heuristics from related literature, standards, and guidelines | |
| 2 | Synthesise | | To consolidate heuristics derived from iterations | |
| 3 | Map | | To map heuristics to the requirements specified in Chapter Six. | |
| 4 | Validate | | To conduct expert validation of heuristics | |
| 5 | Refine | | To refine heuristics based on validation feedback | |
| 6 | Propose | | To propose a final set of heuristics for usable security evaluation for MFS and a usable security guide for MFS developers | |

Table 7.1: Heuristics Development Approach Adopted for This Study

The first step focused on leveraging an iterative approach to extract heuristics from the studies conducted in Chapter Five of this thesis and a comprehensive review of the literature, standards, and guidelines. The first iteration identified usable security heuristics from principal component analysis of the survey finding of 698 MFS users. The second iteration identified some heuristics from a thematic analysis of the study of 37 supply-side actors in Chapter Five of this study. In the third iteration, heuristics were identified from related literature and a review of standards and guidelines related to cybersecurity and usability of mobile financial services.

In the second step, the heuristics extracted from the iterations were then synthesised and revised. They were mapped to the requirements for usable security developed in Chapter Six in the next phase. These heuristics were then validated by experts and further refined to reflect feedback from the validation exercise and presented as proposed heuristics.

## 7.3 ITERATION PROCESS

### 7.3.1: Iteration 1: Principal Component Analysis of End-User Survey

Principal component analysis was conducted on data obtained from the survey of 698 MFS users in sections 5.3.1 and 5.3.2 of this thesis. The analysis revealed elements that when addressed will improve both the usability and security of MFS as follows:

i. Complexity: The complexity of security control had an impact on user usable security choices
ii. Awareness: Contradiction in the perception of awareness of privacy in theory and actual application has an impact on users' usable security behaviours
iii. Environmental impact: Social and environmental context has an impact on the usable security behaviour of users
iv. Maintenance and updates: While users generally exhibited good maintenance behaviour, this behaviour has an impact on users' security choices

### 7.3.2: Iteration 2: Analysis of Supply-Side Study Data

The second iteration involved the analysis of data obtained from the interviews of 37 DevOps and bank CIOs presented in sections 5.3.3 and 5.3.4 of this thesis. The data revealed elements central to usable security from the practices of MFS solutions providers. Elements identified include:

i. Design for usable security: This factor ensures that consideration for usable security starts during requirements gathering and the choice of development methodology. It proposes that design should be user-centred, user-focused, and inclusive.

ii. Communication: Communication and reliability of transaction information should be transparent, provide the capability for feedback, and ensure the reliability and integrity of the transaction.
iii. Quality: This factor emphasises that requirement elicitation should be a basis for quality. The factor also emphasises the need for compliance with regulation and the need to ensure quality is tracked and measured.
iv. Operations and infrastructure: This factor focuses on addressing transaction channel security, consumer redress, and user awareness-related concerns.

### 7.3.3: Iteration 3: Thematic Analysis of Literature

The third iteration of this study focused on a review of usable security evaluation literature intending to identify elements central to usable security, through a thematic analysis of identified literature. While this is not a systematic literature review, the approach adopted ensured all relevant models were identified. A population, intervention, comparison, and outcome (PICO) table was first developed based on the search objective which was to identify elements central to usable security. Table 7.2 shows the detail of the PICO table.

| Population | Intervention | Comparison | Outcome |
|---|---|---|---|
| End-users and Developers | Usability of Security Mechanism | Evaluation | Approaches |
| End-Users<br>Users<br>Customers<br>Client<br>App Developers<br>Programmers<br>System Administrators<br>Coders<br>Developers<br>Testers<br>DevOps<br>App Designers | Usability of Security<br>Usable Security<br>Usability and Security | Evaluation<br>Testing<br>Validation<br>Examination<br>Verification<br>Implementation | Approaches<br>Method<br>Methodology<br>Guides<br>Heuristics<br>Framework<br>Model<br>Mechanism<br>Control |

Table 7.2: PICO Table

Six search strings were derived from the table as follows:

i. (Usab* AND Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model

OR Mechanism OR Control*) AND (End-User* OR User* OR Customer OR Client OR Consumer*)

ii. (Usable Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model OR Mechanism OR Control*) AND (End-User* OR User* OR Customer OR Client Or Consumer*)

iii. (Usability of Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model OR Mechanism OR Control*) AND (End-User* OR User* OR Customer OR Client Or Consumer*)

iv. (Usab* AND Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model OR Mechanism OR Control*) AND (App* Developer* OR Mobile Developer* OR Mobile App* Developer* OR Programmer* OR Sys* Admin* OR Coder* OR App* Designer*)

v. (Usable Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model OR Mechanism OR Control*) AND (App* Developer* OR Mobile Developer* OR Mobile App* Developer* OR Programmer* OR Sys* Admin* OR Coder* OR App* Designer*)

vi. (Usability of Security) AND (Evaluat* OR Test*OR Exam* OR Verif*) AND (Approach OR Method* OR Guide* OR Heuristic* OR Framework OR Model OR Mechanism OR Control*) AND (App* Developer* OR Mobile Developer* OR Mobile App* Developer* OR Programmer* OR Sys* Admin* OR Coder* OR App* Designer*)

The search was conducted on the following sources: ACM Digital Library, USENIX, Science Direct, IEEE Explorer Digital Library, Scopus, Google Scholar, Springer, and ResearchGate, from 2017 to 2023. The search identified 88 peer-reviewed literature, out of which 31 met the final selection criteria and were analysed for this study. Table 7.3 shows the usable security factors derived from the literature.

| # | Model | Derived Usable Security Factor | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Integrity | Proportionality | Transparency | Empowerment | Identity | Reliability | User Support | Accessibility | Authenticity | Compliance | Alignment | Freedom |
| 1 | Gaehtgens et al. (2017) | √ | | √ | | √ | | | | | | | |
| 2 | Feth and Polst (2019) | √ | √ | √ | √ | | √ | √ | √ | | | | |
| 3 | Lennartsson et al. (2021) | √ | | | √ | √ | √ | √ | | √ | | | |
| 4 | Liu et al. (2017) | √ | | | | √ | | | | √ | | | |
| 5 | Weber et al. (2017) | √ | | | | | | | | | | | |
| 6 | Naqvi and Seffah (2018) | √ | | | | | | | | √ | | | |
| 7 | Wang et al. (2017) | √ | | | | | | | | √ | | | |
| 8 | Kumar et al. (2020) | √ | | | | | | | √ | √ | | | √ |
| 9 | Mohamed et al. (2017) | | | | | | | | | | | √ | |
| 10 | Das et al. (2018) | | √ | √ | | | | | | | | √ | |
| 11 | Reuter et al. (2022) | | √ | √ | | | √ | | | | | √ | |
| 12 | Realpe et al. (2017) | | √ | | | | | √ | √ | | | | |
| 13 | Oliveira et al. (2018) | | √ | √ | | | | √ | | | | √ | |
| 14 | Eskandari et al. (2018) | | | √ | √ | | √ | √ | | | | | |
| 15 | Alarifi et al. (2017) | √ | √ | | √ | √ | √ | √ | √ | √ | √ | | |
| 16 | Pearman et al. (2019) | | √ | | √ | | | √ | | | | | |
| 17 | Schiller and Adamsky (2021) | | | | | | √ | √ | | | | | |
| 18 | Galanská (2017) | | √ | | √ | | | √ | | | | √ | √ |
| 19 | Gordieiev et al. (2019) | | | | | √ | | | | | | | |
| 20 | Wijayarathna and Arachchilage (2019) | | | | | | | √ | | | | | |
| 21 | Naiakshina et al. (2017) | | | | | | | √ | | | | | |
| 22 | Mindermann and Wagner (2018) | | | | | | | √ | | | | | |
| 23 | Parizi et al. (2018) | | | | | | | √ | | | | | |
| 24 | Acar et al. (2017) | | | | | | | √ | | | | √ | |
| 25 | Gutfleisch et al. (2022) | | | | | | | √ | | | | √ | |
| 26 | Nocera et al. (2023) | √ | | | | | | | √ | | | √ | √ |
| 27 | Kaur et al. (2017) | | | | | | | | √ | | √ | | |
| 28 | Reese et al. (2019) | √ | | | | | | | | √ | | | |
| 29 | Halunen et al. (2017) | | | | | | | | √ | | | | √ |
| 30 | Fanelle et al. (2020) | | | | | | | | √ | | | | |

| # | Model | Derived Usable Security Factor | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Integrity | Proportionality | Transparency | Empowerment | Identity | Reliability | User Support | Accessibility | Authenticity | Compliance | Alignment | Freedom |
| 31 | Fassl et al. (2021) | | | | | | | | | √ | | √ | √ |

Table 7.3: Usable Security Factors for Iteration 3

The objective of the analysis of the identified model is to derive usable security factors that can be applied in the development and evaluation of mobile financial services. However, the analysis also provided further insight as follows:

a. Requirements for Usable Security Trade-off

The need for the right trade-off between usability and security has been thoroughly debated in the literature. The need to factor in user behaviour has also been emphasised. A study of 55 participants opined that in addition to consideration for this trade-off, other efforts have focused on authentication and helping developers improve usability, influencing user behaviour through capacity building (Norcera et al. 2023). Similarly, another model also considered usability and security requirements for usability security trade-off from the viewpoint of software requirements documentation. It takes an interesting approach to making security the central objective and analysing usability requirements based on a conflict of usability attributes with security, then prioritising requirements based on the scale for usability problems (Naqvi and Seffah 2018). Another paper viewed usability from a security perspective. It examined the usability of information security models to identify usability issues and recommended the examination of the constraints of the usability domain and its consequence on security (Wang et al. 2017). While some usable security elements were derived from these models, handling security and usability requirements separately, as against addressing elements central to both, will not only increase the workload for implementers but encourage disparate implementation of usability and security which has been identified as a major concern leading to considering one above the other.

b. Usable Security Beyond End-User Needs

While conversations on usable security have mainly been about making security controls more usable for the end-user, others have focused on the need to make them

easy to use for supply-side actors like developers and programmers. Literature has highlighted the need to strengthen usable security for supply-side actors (Mindermann and Wagner 2018; Wijayarathna and Arachchilage 2019; Acar et al. 2017; Gutfleisch et al. 2022). While supply-side and demand-side imperatives for usable security might differ, this study focused on identifying elements central to usable security to examine the impact on usable security for MFS.

c. The End Game is Trust

Trust underpins every transaction and in the digital space must be established instantaneously without any initial ceremonies. While the objective of the review of this model is to identify usable security elements, the relationship between the elements and how they impact trust for MFS leading to adoption would benefit from the implementation of these factors. This study revealed the correlation between usable security elements and trust (Gaehtgens et al. 2017).

d. Learning Across Domains

The usable security evaluation model considered was applied in various domains like e-banking, health, websites, and cryptocurrency. This approach enabled us to learn from the experiences in other domains in adopting a human-centred approach to develop an evaluation model for mobile financial services (Alarifi et al. 2017**;** Parizi et al. 2018; Eskandari et al. 2018; Kumar et al. 2020).

e. Other Aspects

Other models examined the role of mental modes and tacit knowledge in improving usable security. One of the papers noted that the mental models of users may not be in alignment with the conceptual model of the system due to the presence of exogenous factors that have influenced the formation of the users' mental model (Mohamed et al. 2017). Examining usable security from a historical perspective, it was noted that a one-size-fits-all approach to encourage good use behaviour does not yield much. The authors opined that one reason why the one-size-fits-all approach might not work is the use of context and personalisation requirements to achieve that. Furthermore, it was noted that it is important to consider the user as central to any workable usable security solution (Reuter et al. 2022).

The models evaluated provided useful insight into developing usable security heuristics. The next section describes how usable security factors are derived from the models.

### 7.3.4: Usable Security Factors

This section presents the details of the factors derived from the models and presented in Table 7.3.

i. Integrity

Actual financial loss is possible during transactions in mobile financial services and has led to a lack of trust in the system. A major objective of a usable secure system is to mitigate against this. This factor examines measures put in place to protect transactions against unauthorised access or modification. The factor was examined as an aspect of digital trust which can be directional, bidirectional, or transitive between transacting entities. To achieve that, it seeks to address actions taken to ensure the transactions can be trusted at all times, and that unauthorised parties do not have access to the transactions (Gaehtgens et al. 2017). This was also examined from the perspective of developers and administrators, with a focus on ensuring the presence of an effective measure for protecting transaction data, the failure of which would have a negative effect on trust. The protection of transaction data was derived as a goal for usable security from the model (Feth and Polst 2019). Another model emphasised the need to prevent unauthorised access to transaction data from the viewpoint of usability of confidentiality as a usable requirement, and measures put in place against unauthorised modification from the viewpoint of usability of data integrity as a usable security requirement. Furthermore, the model proposed the need to provide confidence that any change in a transaction is intended as a measure of the level of trust. The model proposed the need to ensure the implementation of this requirement in the early development stage (Naqvi and Seffah 2018). It was noted that ensuring transaction integrity should commence from authentication. It was also recommended to be considered as part of the access control and storage mechanism. This is to enable the effective identification of any state change in transaction data (Liu et al. 2017; Weber et al. 2017; Naqvi and Seffah 2018; Wang et al. 2017). These factors should be implemented in a way that would yield optimal outcomes for usable security, preserve trustworthiness, and ensure data reaches the intended recipient in an accountable way (Kumar et al. 2020). While the need to restrict unauthorised access to the asset that hosts the system was raised, in the case of this research, the mobile phone, this research focuses on the MFS solution (Alarifi et al. 2017).

In summary, nine models contributed to this theme as an important factor for usable security. To achieve the objective of this factor, the models have suggested the need to ensure the transaction is trustworthy throughout its lifecycle, right from authentication, and that only authorised actors can conduct a direct, bidirectional, and

transitive interaction with transaction data to ensure trust. While some of the models focus on specific beneficiaries like developers, others are generic.

To come up with a description for this factor, several considerations were made. The proposed options included *confidence, authorisation, immutability, and integrity.*

*Integrity* was adopted as the name of the function as it better describes the objective of the factor. However, the downside of this choice was that it might be misconstrued as an attribute of security. Based on the outcome of the analysis of the models presented, some of the attributes underpinning *integrity* as a factor for usable security include:

- Unauthorised parties should not have access to the transactions
- Transactions should be trustworthy at all times
- Effective measures for protecting transaction data should be put in place
- Measures to prevent unauthorised modification of transactions should be put in place
- Provide confidence that any change in a transaction is intended
- Measure to ensure transaction integrity should commence from the authentication process
- Access control and storage mechanisms should be considered
- Preserve trustworthiness by ensuring data reaches the intended recipient in an accountable way

ii. Proportionality

A one-size-fits-all usable security approach might lead to as many unintended consequences as a security mechanism without usability consideration. Applying the same intervention to all user groups may not be as effective as desired, because user contexts are different (Reuter et al. 2022). This aspect examined how security mechanism caters to various types of stakeholders with different levels of technology appreciation, cognitive ability, knowledge of mobile financial services, and cybersecurity risks. A usable security mechanism should be inclusive and not discriminate based on the level of expertise (Galanská 2017). One of the models demonstrated that security must be made to work for non-experts through the right tailoring, and novice users should be able to perform simple transactions efficiently. It further noted that even where the level of expertise for usable security is low, users can attain higher knowledge of the system, effectively distinguishing knowledge of usable security vs. how to effectively use a system. It was further noted that users'

resources in terms of knowledge, time, and cognitive capacity should be considered in coming up with a usable secure control. Users have different security demands in different situations and effective controls should reflect that (Feth and Polst 2019). While all users cannot be made experts, a good feedback mechanism can help translate improved usability to acceptability (Das et al. 2018).

Several codes were analysed to arrive at a suitable description of this factor. Some of the words considered are *tailoring, inclusivity, flexibility, user-centricity, universality, and proportionality. Proportionality* was adopted as it provided the most suitable description for the context the factor seeks to address.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *proportionality* as a factor for usable security include:

- Usable security mechanisms should not discriminate against users' technical skill level.
- Usable security mechanisms should have consideration for various levels of cognitive capacity.
- The level of user expertise in cybersecurity should not limit the ability to identify and apply the right controls.
- Usable security mechanism must work for non-experts.
- Usable security should work well for urgent transactions as it would for normal transactions.
- Usable security mechanisms should not put much burden on users.

iii. Transparency

‘In traditional trust, certain ceremonies are carried out before trust can be established. In digital transactions, however, trust relationships are instantaneous. It is, therefore, imperative to ensure trust elements are clear, instantly established, and understandable between transacting entities. To adopt a usable secure mechanism, a trust relationship must be present between the user and the mechanism. Transparency of interaction is a key driver for this level of trust (Gaehtgens et al. 2017). Usable secure controls should not be a black-box to the intended beneficiary. Users should have clarity as to the implications of applying it or not applying it. It should also not be considered an “advanced option” in a security setting. Feth and Polst (2019) examined and analysed transparency as a goal of usable security and opined that it is a very important prerequisite for trust as it enables the formation of user perception of security. Furthermore, it was also suggested that users should be

aware of the status of their transactions at any time and should also know when the transactions are completed (Eskandari et al. 2018). Transparency needs might be diverse as users might have different expectations of transparency. This difference should be considered in the development of security mechanisms (Reuter et al. 2022).

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *transparency* as a factor for usable security include:

- Users should be aware of their transaction status
- Incorrect application of security control should lead to recognisable error
- The impact of any choice of security preference should be understood by users
- Security information should only be relevant to current activity
- Security information should be in clear and easy-to-understand language
- The user should be aware of whether they are in a secure or insecure state throughout a transaction session
- Users should know where to find relevant security information
- Users should be aware when security control becomes inactive
- Users should be aware of the mandatory security actions required of them

iv. Empowerment

Users at times have a perception that taking certain security actions is beyond them or is against their interest. To improve trust and confidence in security mechanisms, and help users cooperate with security controls, users need to have a sense of being in control of their security decisions, so they can take responsibility for their security actions and improve their security behaviours (Lennartsson et al. 2021). The security system should encourage users to comply with security controls and not bypass them where possible. A usable security mechanism should not restrict users but enable them. When users feel enabled they are more likely to cooperate with security mechanisms. This can only be possible if users are allowed to express their security needs efficiently and if a system exists to enforce such decisions. This level of user enablement was described by Feth and Polst (2019) as “self-determination” as a goal of usable security. Furthermore, the focus of the security mechanism should be user protection, not system protection as the end-user is the one to be impacted by loss of funds if any successful attack is carried out on his account. While there might be some need to place some minimal security restrictions on users, such a decision should be

evaluated and only implemented if it is the most cost-effective decision from the user perspective (Galanská 2017).

Some of the words considered as code for this factor are *control* and *empowerment. Empowerment* was adopted as it better describes the problem the factor seeks to address.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *empowerment* as a factor for usable security include:

- Users should have the freedom to customise their security preferences.
- Users should be able to reverse certain levels of wrong security choices.
- Security choices should be such that users do not think someone else is responsible for their bad security choices.
- Users should be able to learn and use security control within a specified time limit.
- Users should have confidence that the system behaviour will be as intended.
- Users should be able to recover from non-critical errors.
- Users should have a perception of having control over the security mechanism.
- Users should feel empowered to make security decisions.
- Security mechanisms must be centred on enabling users not restricting them.

v. Identity

Authentication and authorisation are required at the access level of any secure system. This ensures the trust relationship between the transacting entities. This is concerned with ensuring that the verified identity of transacting entities remains the same, throughout the lifecycle of a transaction and not just at the point of access control. A usable secure mechanism should ensure claims of identity can be corroborated with a degree of trust that corresponds to the risk rating of the transaction or system activity through continuous authentication (Gaehtgens et al. 2017; Liu et al. 2017). To ensure this, the system must be accountable by keeping logs about the nature of previous activities of an authorised entity, to instantly identify any divergence in an entity's transaction behaviour during a transaction (Lennartsson et al. 2021).

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *identify* as a factor for usable security include:

- The claim of identity should be verifiable during a transaction.

- Divergent activities by entities should be flagged based on risk level.
- Continuous authentication should be possible for certain levels of transaction.
- The user authentication mechanism should not increase the user's cognitive workload.

vi. Reliability

A reliable system provides timely and meaningful feedback. Lack of feedback or clarity of feedback messages are some of the challenges that lead to a lack of trust in security mechanisms. Reliability as a factor for usable security focuses on ensuring adequate, meaningful, and timely communication and feedback and the status of security actions. After verifying the identities of participants in a trust relationship, it is important to ensure exchange of information between them is effective and secure (Lennartsson et al. 2021). Furthermore, a user should not be left to guess the consequences of his security choices as the system should be able to communicate that to him. This communication should be in a clear and understandable manner. In the event something goes wrong, the mechanism should let the user know the effect of their action and how to go about making remedial or corrective choices (Eskandari et al. 2018; Reuter et al. 2022). Interaction between users and security mechanisms should be treated as an interaction between two entities in a trust relationship, where bidirectional feedback is required to maintain trust. Clear and timely feedback help boost user confidence and improve trust in security mechanism.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *reliability* as a factor for usable security include:

- Users should not be left guessing the consequence of their security actions; the system should make it clear to them.
- Feedback from security mechanisms must be presented in a clear and complete manner.
- Users should know what next to do when they get a feedback message after carrying out a wrong security action.
- Feedback and warning mechanisms should be considered for user mental models.
- Users must be comfortable with terminologies in feedback messages and alerts from security mechanisms.
- Error messages should provide the cause and severity of the problem encountered.

vii. User Support

Lack of user awareness is one impediment to usable security that was identified by several participants in the problem conceptualisation phase of this thesis. In the same vein, user support is the most cross-cutting usable security factor identified from the analysis of the identified literature. In addition to making helpful guides available to users promptly, this factor seeks to help users better understand security controls in such a way that it would help them apply these controls efficiently and effectively without adding more cognitive workload.

*Enablement* and *user support* are two phrases considered as code to describe this factor. However, *user support* was adopted because it is a more circumspect description of the factor.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *user support* as a factor for usable security include:

- The help function should have consideration for user time and cognitive capacity.
- Help documentation should be appropriate and specific.
- Help should be context-sensitive, only relevant sections should be available at any given time.
- Security mechanisms should have clear labels.
- Help documentation must be up-to-date.
- Security mechanisms should be understandable by a novice.
- Users should be comfortable navigating through security mechanisms with minimal need to seek help from documentation.
- Security mechanisms should help users minimise errors.

viii. Accessibility

Accessibility is a factor that focuses on the inclusivity of usable security. This function seeks to make security control work for the visually impaired. While other forms of accessibility concerns exist, the scope of this thesis only includes visual impairment.

The attribute underpinning this factor is based on the question below:

- Does the security mechanism have considerations for the visually impaired?

ix. Authenticity

This factor focuses on the preservation of trustworthiness and uniformity of the security mechanism its entire lifetime. It complements *identity* (Kumar et al. 2020). The factor seeks to ensure reasonable steps are taken to guarantee security mechanisms are up to date and functional at all times, and where there are downtimes, the system should inform the user. The problem of lack of trust or low trust in security mechanisms might not be unconnected to the fact that such solutions were more driven by what technology can achieve rather than user concerns and their perception of security (Naqvi and Seffah 2018).

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *authenticity* as a factor for usable security include:

- Users should be able to validate that security certificates are genuine and not corrupted.
- Users should be able to verify that the security mechanism is up to date.
- Users should easily understand and use digital signatures.
- Users should be able to tell if digital signatures are valid or not.
- The system should alert users of any non-trustworthy controls.

x. Compliance

Cybersecurity is a universal concern that standard-setting bodies and associations have worked towards addressing over the years at a global and national level. This factor seeks to ensure extant standards and guidelines are adhered to by developers of security mechanisms, and these standards are available in such a way that it does not add an extra burden to the solution providers. Some of these policies and guidelines include the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology (NIST) framework, the Open Web Application Security Project (OWASP), and other consumer protection, cybersecurity, and privacy guidelines at the global and national levels.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *compliance* as a factor for usable security include:

- Security mechanisms should comply with extant policies and guidelines.
- The standards and guidelines should be integrated into the development process in such a way that it should not add an additional burden on developers.

xi. Alignment

This thesis considers cybersecurity in MFS as a sociotechnical problem and has considerations for the ecosystem, ecosystem actors, and the environment in addressing usable security. This function focuses on consideration for mental models and the cognitive capacity of the users in such a way that it would facilitate good security behaviours. To ensure the consideration of mental models in system design, Mohamed et al. (2017) posited that, design features should be aligned with user requirement which is extracted from users' tacit knowledge. Furthermore, the authors proposed that the efficacy of usable security would depend on how well tacit knowledge is captured and translated into system design (Mohamed et al. 2017). The mental model of users affects their perception of how a system should work which might not be consistent with the conceptual model of the system. The major challenge this factor seeks to address is ensuring the security mechanism achieves the objective of protecting the user from unintended consequences of bad security choices and ensuring the control mechanism conforms to users' expectations in a way that would facilitate adoption and usage.

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *alignment* as a factor for usable security include:

- The requirement for security mechanisms should be user-focused.
- Security control should not add cognitive workload on users.

xii. Freedom

Users should not feel restricted by security controls. Security mechanisms should not restrict users from conducting their normal activity in a certain way if it does not break the system. Protecting the user from the harm of financial loss should not be a motivation for avoidable restrictions (Galanská 2017). Security controls should be non-intrusive as users do not want security in the way of their tasks. Understandably, there might be a need to activate certain security controls. In such instances the system should be flexible, provide for leveraging compensating controls, and only apply new controls where necessary. Similarly, complex security configuration tasks should be minimised and required only when necessary. The function ensures security controls are non-intrusive, non-restrictive, flexible, and activated only when necessary. Four models contributed to this theme as an important factor for usable security (Galanská 2017; Halunen et al. 2017; Kumar et al. 2020).

Based on the outcome of the analysis of the models presented, some of the attributes underpinning *freedom* as a factor for usable security include:

- Complex security configuration tasks by users should be required only when necessary.
- Security controls should be non-intrusive.
- Leverage compensating controls before thinking of applying a new one.
- Users should experience fewer and more critical security distractions.

## 7.4 SYNTHESISING AND CONSOLIDATING THE HEURISTICS

Based on the insight generated from the three iterations, the outcome of the iterations was synthesised to come up with the derived heuristics principles. Table 7.4 shows how functions from the 3 iterations relate to one another and how they were synthesised to come up with heuristics to address the requirements developed in Chapter Six of this thesis.

| # | Function | Source | Aligned to Iteration 3 Function | Justification |
|---|---|---|---|---|
| **1** | Complexity | Iteration 1 | Proportionality and Alignment | Complexity addresses user behaviour in the use of security mechanisms occasioned by the level of complexity of security control which arises due to their level of awareness (proportionality) or cognitive capacity (alignment) |
| **2** | Awareness | Iteration 1 | Empowerment and User Support | Awareness addresses factors that will enable the users to apply security controls more effectively. It aligns with the objectives of empowerment and alignment. |
| **3** | Environmental impact | Iteration 1 | Transparency and Reliability | Environmental impact from Iteration 1 addresses issues that affect reliability and trustworthiness in security controls as captured by transparency and reliability from Iteration 3 |
| **4** | Maintenance and updates | Iteration 1 | Integrity, Identity, and Authenticity | Function seeks to guarantee systems trustworthiness via updates during authentication and at the transaction level as |

| # | Function | Source | Aligned to Iteration 3 Function | Justification |
|---|---|---|---|---|
| | | | | addressed by integrity, identity, and authenticity from iteration 3 |
| **5** | Design | Iteration 2 | Alignment and Proportionality | Design function addresses inclusivity by design as addressed by alignment and proportionality from Iteration 3 |
| **6** | Communication and Reliability | Iteration 2 | Transparency, Reliability, and Integrity | Communication and reliability seek to improve trust by ensuring effective and timely feedback and system trustworthiness as proposed by transparency, reliability, and integrity from Iteration 3 |
| **7** | Quality | Iteration 2 | Compliance and Integrity | Quality seeks to ensure compliance with standards and ensure validation of trustworthiness as captured by compliance and integrity from Iteration 3 |
| **8** | Operations and Infrastructure | Iteration 2 | Integrity, Reliability, user Support, and Empowerment | The identified functions from Iteration 3 effectively addressed concerns raised by operations and infrastructure from Iteration 2 |

Table 7.4: Synthesis of Heuristics

To verify that the heuristics address the requirements for usable security based on the studies conducted and presented in Chapters Four and Five of this thesis, the heuristics were mapped and the functional requirements were identified in section 6.4.2 of this thesis. The exercise demonstrates that the developed heuristics can address the documented requirements for usable security.

## 7.5 HEURISTICS VALIDATION

A robust approach was adopted in developing the heuristics. This approach also factors in the process of validating the heuristics. To validate the heuristics, semi-structured interviews with experts with experience in cybersecurity and human factor space were conducted. Semi-structured interviews as a data collection tool in qualitative research was preferred to focus groups and workshops as it is easier to

access individual experts based on their schedule than to agree on a time and date that suits all experts at the same time. While finding such a time might not be impossible, due to the cross-sectional nature of this study, time constraints limited the choice of approach.

The interview instrument was made of sections that gauge the experience level of experts on mobile financial services, usable security, and heuristics evaluation. This assisted in the analysis of expert feedback vis-a-vis their experience level. Through the interview, feedback on the definition of derived heuristics was obtained on which should be dropped, merged, or refined with justification. Suggestion on prioritisation of heuristics was also captured as part of the interview questions. The semi-structured interview questionnaire for heuristics validation is attached in Appendix IV of this thesis.

After the development of the interview instrument, it was shared with some experts for feedback. These experts include a cybersecurity expert with fifteen (15) years of experience, a software engineer with seventeen years (17) years of experience, and two senior university academics with a research focus on human factors and cybersecurity. Their feedback was then used to revise the interview instrument. It should be noted that the experts who participated in the review of the interview instrument are different from the ones who participated in the heuristics validation exercise. After the final semi-structured interview instrument was approved, it was used to run three (3) pilot interviews after which the instrument was further refined and deployed for actual use.

Thirty (30) participants for the validation were identified via previous work and expert recommendations. They were all contacted via email and phone calls. However, fourteen participants participated in the final validation exercise. Table 7.5 shows the profile of the participants.

| # | Participant | Country | Years of Experience | Field | Domain |
|---|---|---|---|---|---|
| **1** | V1 | Lithuania | 2 | Cybersec/HCI | Freelance |
| **2** | V2 | USA | 10 | HCI | Info Tech |
| **3** | V3 | Nigeria | 4 | Cybersecurity | Payment |
| **4** | V4 | USA | 4 | Cybersecurity | Health |
| **5** | V5 | UK | 20 | Cybersecurity | Defense |
| **6** | V6 | USA | 1.5 | Cybersecurity | Health |
| **7** | V7 | USA | 10 | Cybersecurity | Financial Services |
| **8** | V8 | Italy | 12 | HCI | Academia |

| # | Participant | Country | Years of Experience | Field | Domain |
|---|---|---|---|---|---|
| **9** | V9 | UK | 4.5 | HCI | Financial Services |
| **10** | V10 | UK | 15 | Cybersecurity | Academia |
| **11** | V11 | UK | 25 | HCI | Financial Services |
| **12** | V12 | Nigeria | 8 | HCI | Academia |
| **13** | V13 | Nigeria | 11 | HCI | Financial Services |
| **14** | V14 | Nigeria | 12 | HCI | Financial Services |

Table 7.5: Participants Profile. V= Validator.

100% of the participants have between an intermediate and expert proficiency in usable security both in theory and practice. While 70% of the participants have high proficiency in mobile financial services, 54.5% have a good understanding of heuristics evaluations, 39% have participated in usable security evaluation in the past, and 33% have experience in conducting heuristics evaluation.

### 7.6.1 Heuristics Validation Results

As part of the overarching methodology for this thesis, a validation of the artefact developed and the process of developing the artefact was conducted. This section provides an overview of the feedback obtained from the validation exercise.

#### *7.6.1.1 Perspectives and Considerations for Usable Security*

As part of the validation process, participants shared their perspectives and considerations for usable security. While acknowledging the existence of many theoretical models for usable security, participants consider the actual implementation of the models problematic. A participant emphasised the importance of anchoring usable security implementation on the value it brings to users and not just a discussion on balancing system attributes. Further to that, another participant, in providing a similar perspective on value, mentioned that if there must be any balance, there should be a balance between value in terms of utility and assurance. Two participants highlighted two dimensions of inclusivity that should be considered in usable security. While one mentioned people with dementia and how it impacts learnability and memorability as usability attributes, the second mentioned consideration for people with a low degree of technology appreciation. Considerations for data privacy and the need to ensure clear responsibility for usable security were also highlighted.

#### *7.6.1.2 Feedback on Usable Security Elements*

Participants were asked to review the proposed heuristics and recommend any amendments to the definition and scope. They were requested to suggest if any

should be dropped, added, or merged. Also, they were asked to prioritise the heuristics with a focus on using them as a guide for development and for evaluating existing products.

One participant suggested "*integrity*" should be replaced with "*consistency*". Another suggested that regulation might impede empowerment. While further analysing *compliance*, it was suggested that the factor should be in three parts to focus on contractual agreement, legal requirement, and regulation, as this would make the recommendation more implementable. Similarly, while participants believe transparency and proportionality are important, they mentioned that layered implementation to meet all user segments might be a challenging task. To improve reliability, it was suggested that in-app feedback capability should be considered against the use of SMS. Also, it was suggested that reliability should be considered as a factor of design where the system would ensure that it does what it promises to do, and not feedback alone. Due to the criticality of app updates, it was suggested that a penalty for non-compliance should be introduced. Furthermore, it was suggested that instead of considering just mental models, *alignment* should focus on value and pain points to improve efficiency. It was suggested that *empowerment* should consider security and privacy empowerment. Suggested modifications to the factors are highlighted in Table 7.6.

| # | Factor | Suggested Addition |
|---|---|---|
| 1 | Proportionality | • Physical ability, entering pins are challenging for people with reduced finger dexterity<br>• Let go of security control if it is too complex and cannot be simplified to meet various end-user needs |
| 2 | Empowerment: | Users should know why data is collected and what it will be used for |
| 3 | Reliability | Backup systems should be considered in case of failure of the system to ensure that the service is continued |
| 4 | Accessibility | Does the system provide a variety of authentication mechanisms to suit different abilities e.g. biometrics? |
| 5 | Alignment | Security control does not add to the physical workload of the users |
| 6 | Transparency | Must have 3 of the elements in the definition as one or two of them only would not. (comprehensible, verifiable, and accessible) |
| 7 | User support | Capability to carry out a task where the need arises |

Table 7.6: Suggested Modifications

While all participants believed the factors were important to enable usable security during the development of MFS and for the evaluation of the existing solution, there was no agreement as to which one of the elements was more important than the other. However, an ANOVA test of statistical significance was carried out on the suitability of applying the factors for development and design. The result shows that there was no significant difference in the perception of the respondents, as shown in Table 7.7.

| | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| Evaluation | Between Groups | 48.68 | 3 | 16.23 | .74 | .565 |
| | Within Groups | 131.42 | 6 | 21.90 | | |
| | Total | 180.10 | 9 | | | |
| Design | Between Groups | 93.73 | 3 | 31.24 | .92 | .488 |
| | Within Groups | 204.67 | 6 | 34.11 | | |
| | Total | 298.40 | 9 | | | |

Table 7.7: ANOVA Test

## 7.7 USABLE SECURITY HEURISTICS

Table 7.8 shows the twelve derived heuristics after synthesis, alignment to requirements, and final validation.

| # | Heuristics Principle | Description | Underpinning Heuristics |
|---|---|---|---|
| 1 | Integrity | Put measures in place to protect transactions against unauthorised access or modification | ▪ Unauthorised parties should not have access to the transactions<br>▪ Transactions should be trustworthy at all times<br>▪ Effective measures for protecting transaction data should be put in place<br>▪ Measures to prevent unauthorised modification of transactions should be put in place<br>▪ Provide confidence that any change in a transaction is intended<br>▪ Transaction integrity check should commence at the point of authentication<br>▪ Access control and storage mechanisms should be considered<br>▪ Preserve trustworthiness by ensuring data reaches the intended recipient in an accountable way |

| # | Heuristics Principle | Description | Underpinning Heuristics |
|---|---|---|---|
| 2 | Proportionality | Ensure security mechanism caters to various types of stakeholders with different levels of technology appreciation, cognitive ability, knowledge of mobile financial services, and cybersecurity risks. | ▪ Usable security mechanisms should not discriminate against users' technical skill level<br>▪ Usable security mechanisms should have consideration for various levels of cognitive capacity<br>▪ The level of user expertise in cybersecurity should not limit the ability to identify and apply the right controls<br>▪ Usable security mechanism must work for non-experts<br>▪ Usable security should work well for urgent transactions as it would for normal transactions<br>▪ Usable security mechanisms should not put much burden on users<br>▪ Let go of security control if it is too complex and cannot be simplified to meet various end-user needs |
| 3 | Transparency | Ensure security controls are understandable, certifiable, and can be evaluated | ▪ Users should be aware of their transaction status<br>▪ Incorrect application of security control should lead to recognisable error<br>▪ The impact of any choice of security preference should be understood by users<br>▪ Security information should only be relevant to current activity<br>▪ Security information should be in clear and easy-to-understand language<br>▪ The user should be aware of their security state (secure or insecure) throughout a transaction session.<br>▪ Users should know where to find relevant security information<br>▪ Users should be aware when security control becomes inactive<br>▪ Users should be aware of the mandatory security actions required of them. |
| 4 | Empowerment | Enable users to have a perception of being in control | ▪ Users should have the freedom to customise their security preferences<br>▪ Users should be able to reverse certain levels of wrong security choices |

| # | Heuristics Principle | Description | Underpinning Heuristics |
|---|---|---|---|
| | | of their security decisions | ▪ Security choices should be in such a way users do not think someone else is responsible for their bad security choices.<br>▪ Users should be able to learn and use security control within a specified time limit<br>▪ Users should have confidence that the system behaviour will be as intended<br>▪ Users should be able to recover from non-critical errors<br>▪ Users should have a perception of having control over the security mechanism<br>▪ Users should feel empowered to make security decisions<br>▪ Security mechanisms must be centred on enabling users not restricting them<br>▪ Users should know why data is collected and what it will be used for. |
| 5 | Identity | Ensure that the verified identity of transacting entities remains the same, throughout the lifecycle of a transaction and not just at the point of access control | ▪ The claim of identity should be verifiable during a transaction<br>▪ Divergent activities by entities should be flagged based on risk level<br>▪ Continuous authentication should be possible for certain levels of transaction<br>▪ The authentication mechanism should not increase the user's cognitive workload. |
| 6 | Reliability | Ensure adequate, meaningful, and timely communication and feedback on critical security and traction activities | ▪ Users should not be left guessing the consequence of their security actions, the system should make it clear to them.<br>▪ Feedback from security mechanisms must be presented in a clear and complete manner.<br>▪ Users should know what next to do when they get a feedback message after carrying out a wrong security action.<br>▪ Feedback and warning mechanisms should be considered for user mental models. |

| # | Heuristics Principle | Description | Underpinning Heuristics |
|---|---|---|---|
| | | | ▪ Users must be comfortable with terminologies in feedback messages and alerts from security mechanisms.<br>▪ Error messages should provide the cause and severity of the problem encountered. |
| 7 | User Support | Assist users to better understand security controls to enable them use these controls efficiently and effectively without adding more cognitive workload | ▪ The help function should have consideration for user time and cognitive capacity<br>▪ Help documentation should be appropriate and specific<br>▪ Help should be context-sensitive, only relevant sections should be available at any given time<br>▪ Security mechanisms should have clear labels<br>▪ Help documentation must be up-to-date<br>▪ Security mechanisms should be understandable by a novice<br>▪ Users should be comfortable navigating through security mechanisms with minimal need to seek help from documentation<br>▪ Security mechanisms should help users minimise errors |
| 8 | Accessibility | Make security controls work for the visually impaired | ▪ Security mechanisms should have considerations for the visually impaired<br>▪ Systems provide a variety of authentication mechanisms to suit different abilities e.g. biometrics |
| 9 | Authenticity | Ensure reasonable steps are taken to guarantee security mechanisms are up to date and functional at all times, and where there are downtimes, the system should inform the user. | ▪ Users should be able to validate that security certificates are genuine and not corrupted.<br>▪ Users should be able to verify that the security mechanism is up to date.<br>▪ Users should easily understand and use digital signatures.<br>▪ Users should be able to tell if digital signatures are valid or not.<br>▪ The system should alert users of any non-trustworthy controls. |

| # | Heuristics Principle | Description | Underpinning Heuristics |
|---|---|---|---|
| 10 | Compliance | Ensure extant standards and guidelines are adhered to by developers of security mechanisms. | ▪ Security mechanisms should comply with extant policies and guidelines<br>▪ The standards and guidelines should be integrated into the development process in such a way that it should not add an additional burden on developers |
| 11 | Alignment | Ensure consideration for mental models and the cognitive capacity of the users in such a way that it would facilitate good security behaviours | ▪ The requirement for security mechanisms should be user-focused.<br>▪ Security control should not add cognitive workload on users.<br>▪ Security control does not add to the physical workload of the users. |
| 12 | Freedom | Ensures security controls are non-intrusive, non-restrictive, flexible, and activated only when necessary | ▪ Complex security configuration tasks by users should be required only when necessary<br>▪ Security controls should be non-intrusive<br>▪ Leverage compensating controls before thinking of applying a new one.<br>▪ Users should experience fewer and more critical security distractions. |

Table 7.8: Usable Security Heuristics

## 7.8 CHAPTER SUMMARY

This chapter presented the process undertaken and results obtained in the design and development of usable security heuristics for mobile financial services. Through an iterative approach, twelve usable security heuristics were derived. The chapter demonstrated that the heuristics address the requirements specified in Chapter Five of this thesis. The validated heuristics were presented. This chapter addresses objectives three and four of this thesis.

# CHAPTER EIGHT: EVALUATION THROUGH CASE STUDIES

This chapter presents the results and lessons from case studies conducted to implement the artefacts developed in this thesis. Through a critical analysis and contextualisation of the problem space, a requirement documentation for addressing usable security for mobile financial services was presented in Chapter Six of this thesis. Furthermore, twelve heuristics to address usable security requirements were developed and validated in Chapter Seven of this thesis, which addressed the five key objectives of this thesis discussed in Chapter One. Building upon the results from Chapters Six and Seven of this thesis, this chapter is focused on a demonstration of the application of the artefacts developed in Chapter Seven into developing usable security MFS solutions. The use of the artefacts to evaluate and identify usable security problems in existing MFS solutions is also demonstrated.

This chapter addresses objective five of this thesis: To exploit and disseminate the validated solution including recommendations.

## 8.1 CASE STUDY 1: HACKATHON

A major objective of documenting an approach to usable security for mobile financial services is to serve as a guide for MFS developers to implement usable security considerations as part of solutions design. This section describes the process and results from a hackathon conducted to apply the developed heuristics in the development of MFS solutions. The hackathon provides a test-and-learn approach to DevOps on how to integrate usable security to MFS development process.

To achieve the aim of the hackathon, this study adopted repeated measures as an experimental design approach, as it works better under time constraints than independent measures, which are more time-and-resource-consuming (McLeod 2023). Another approach that was considered was integrating existing heuristics to address usability in MFS and comparing them with the heuristics developed in this study. However, the shortcomings of existing heuristics have been stated in section 7.1 of this study. Future studies will examine the comparison with other heuristics in detail.

### 8.1.1 Considerations for the Approach Adopted

To implement the heuristics developed in Chapter Seven in developing usable secure solutions, two questions needed to be answered:

i. What is the most effective way to apply the developed heuristics to application development?

ii. How can the value of the developed heuristics be demonstrated?

To answer these questions, it was imperative to make the heuristics available to developers to use in the development of a live MFS system. In section 5.3 of this thesis, study findings showed that agile methodology is the most predominant development approach adopted by mobile financial services solution developers. It is therefore imperative to ensure that the proposed solution aligns with Agile and rapid development principles. Furthermore, hackathons have been applied in design research where they facilitated both solution design and learning (Flus and Hurst 2021). More so, hackathons require invention from participants making it a good approach to develop novel solutions (Rys 2023).

Hackathons are design sprints by technology entrepreneurs or developers collaborating to develop a working prototype to address a challenge within a very short period. The objective of the hackathon is to explore how usable security heuristics can be integrated into the MFS development process and how learning from it can be applied to improve security for users and DevOps of MFS. A hackathon can be completed within a short time frame. It enables one to get quick feedback from several developers via a working prototype. The drawback, however, is that participants would also develop a minimum viable product (MVP) to demonstrate the workability of the concept and not a full-blown product. Also, hackathons are expensive to conduct, and organisers will be expected to fund them. Some hackathons also enjoy large corporate sponsorship. Organising requires backroom organisers which would require time to recruit, train and deploy. This aim of this hackathon is to provide a test-and-learn approach on how usable security heuristics can be integrated into solution design.

The second challenge required the design and implementation of an experimental design where participants could be placed in an experimental group and a control group. In the case of the hackathon, it would require participants to develop their MVPs two times, first, without the heuristics, and second with the heuristics, or split into two groups and given two different challenges. Again, this approach comes with additional cost and time. To address this, the relevant literature on how such challenges are addressed most cost-effectively was reviewed.

There are several types of experimental design, each with its pros and cons. Table 8.0 shows an analysis of the type of experimental designs.

| # | Type | Description | Pros | Cons |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| 1 | Independent measure | Each condition of the experiment is carried out by a different group | Mitigates against order effect | ▪ Requires more participants<br>▪ Any lack of similarity between groups may affect the outcome |
| 2 | Repeated measure | The same participants carry out the conditions of the experiment | Requires fewer people and saves time | Performance might degrade in the second condition, for instance, due to fatigue when compared to the first condition |

Table 8.0: Types of Experimental Design

To mitigate against the identified risks, this project adopted the repeated measure approach and mitigated the risk of order effect through counterbalancing as participants were encouraged to apply the heuristics in random order (McLeod 2023).

### 8.1.2 Experiment Setup and Process Description

To conduct the hackathon, the researcher reached out to experts who have either conducted hackathons in the past or have responsibility for organising hackathons. One pointed to Kaggle and provided insight on how to run a successful hackathon. The second expert provided insight on how to approach the organisation of hackathons most cost-effectively. The third expert oversees an industry sandbox where various financial services application programming interfaces (APIs) are exposed to startups to develop products. They also organise hackathons. They have a community of over 4600 innovators. Given that her organisation already provides training, mentorship, and industry API access to innovators, partnering with them made the hackathon prize money more affordable compared to organising one from scratch. Recruitment time for participants was also a factor as the innovation hub already has a thriving community. After several meetings, the third experts agreed to partner with the researcher to conduct a hackathon to address the objective of this thesis. The organisation provided API, the environment, and technical resources to conduct the event. They were also responsible for recruiting participants. The researcher provided the content, prize money, and judges. Based on this understanding, the hackathon was conducted.

The hackathon was tagged “Cybersecurity Innovation Challenge” and was advertised amongst the community of over 4600 innovators and on fsi.ng website. Figure 8.0 shows a screen grab from the website advertising the event. The event is still listed on the website as a past event and can be accessed via https://fsi.ng/innovation-challenge/2/cybersecurity_innovation_challenge

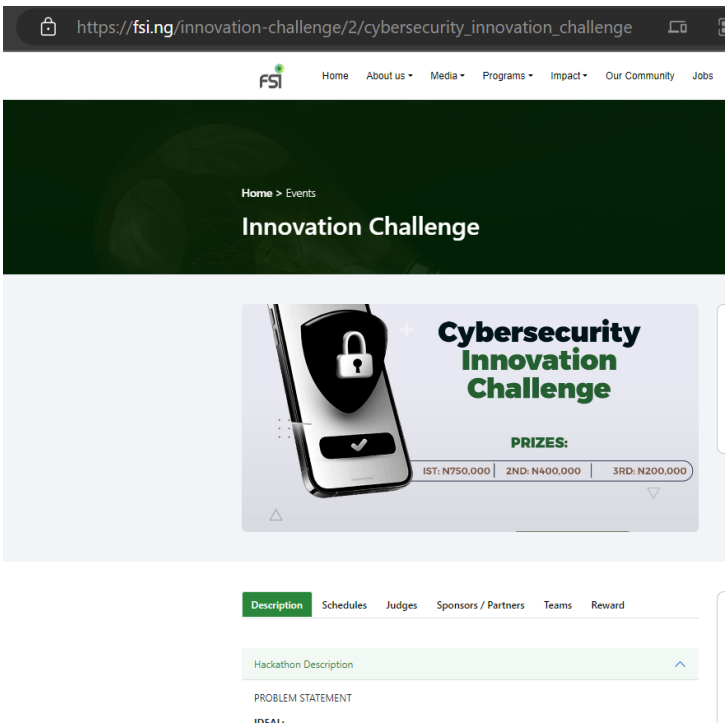



Figure 8.0: Hackathon Advert (FSI 2021)

As part of the plan for the event, a proposal was sent to the partner organisation to use as information for planning and recruitment. The sections of the proposal are shown in Table 8.1.

| # | Section | Description |
|---|---|---|
| 1 | Problem Statement | Provides insights into the real problem, the ideal problem, and the negative human condition it leads to, in terms of actual financial loss due to cybercrime.<br><br>The objective of the hackathon was also described in this section including the fact that insight from the study will feed into this PhD thesis. |
| 2 | Proposal | Describes how the heuristics would be applied in addressing the problem and what would be expected of participants. |
| 3 | Value | The contribution of the output of the study was described |
| 4 | Team Composition | Teams were requested to at minimum consist of a cybersecurity expert (1), UI expert (1), and mobile app developer (1) |
| 5 | Benefits | Benefits to the participants and partner organisation were described in this section |
| 6 | Scoring Criteria | Product design, innovativeness, scalability, and presentation |

Table 8.1: Hackathon Proposal Sections

Other elements of the proposal include scope, environment, presentation mode, and key date information.

Participants were asked to develop an innovative solution on how to apply any 3 of the twelve heuristics during the design and development of MFS solutions.

A team consists of 3 to 5 persons, and each team was requested to have at least one frontend, one backend, and one cybersecurity specialist and should select a team lead.

- All team members were directed to join FSI if they were yet to do so (https://fsi.ng/members/signup/student).
- The leaders of each team were asked to register the team, accept the terms and conditions, and invite team members to join.
- An email was sent to the team containing all the details.
- Teams were expected to use a minimum of 2 API endpoints provided by FSI during this challenge.

Participants were asked to build a mobile app minimum viable product (MVP) that the consumers could use to do any two of the following:

  - Save money,
  - Remit money,
  - Transfer money,
  - and/or purchase goods & services.

The prize for the top three finishers was communicated in advance. The winning prize was N750,000 while the runner-up prize was N500,000.

After 3 weeks of advertisement, 44 teams comprising 124 individuals applied to participate in the event. After the applications were closed, it took 17 days to conclude the entire process.

After the initial rounds, 10 teams successfully submitted mobile applications (APKs) and were moved to the second round. A workshop was organised for the teams to provide insight into the heuristics and what was expected of participants. Participants also sought clarifications from the researcher.

The finalists were expected to develop an MVP (mobile application) adopting a minimum of any 3 of the 12 heuristics principles in the 2nd round.

For the financial pitch, each participant was allocated 10 minutes to present their products and answer questions.

Finally, a live pitch session was organised at the end of the submission period and the finalists pitched to a panel of five judges. The top 3 winners were rewarded. Table 8.2 shows the profile of the judges. Judges were selected based on their experience in the human-computer interaction (HCI), cybersecurity, or DevOps domain.

| # | Alias | Expertise | Years of Experience | Sector |
|---|---|---|---|---|
| 1 | EA | Cybersecurity, machine learning, HCI | 20 years | Academia |
| 2 | IM | Cybersecurity, mobile app developer, API developer, software engineer, fintech | 11 years | Financial services |
| 3 | IO | IT quality assurance, IT business analyst, HCI, software engineering | 22 years | Technology Financial services |
| 4 | SA | HCI, cybersecurity, fintech | 21 years | Financial services |
| 5 | *IM2 | Cybersecurity | 17 years | Cybersecurity |

Table 8.2: Profile of Hackathon Judges

The scores recorded by Judge IM2 were not included in the final computation as he was not able to score more than 3 groups and it was decided by the coordinator that only the scores of the other judges who rated all participants would be considered. However, he was allowed to ask participants questions and provide feedback.

### 8.1.3 Hackathon Result

Results of judges' evaluation, product description, and feedback from all the teams are presented in this section.

#### 8.1.3.1 Hackathon Final Scores

The presentation by the teams was accessed based on the criteria presented in Table 8.2. The score was then aggregated to determine the winner. Table 8.3 shows the final scores. The names of the teams and judges were coded to protect their identity as agreed with them earlier in the process. A total achievable score of 30 was allocated each to product design, innovativeness, and scalability while a maximum score of 10 was allocated for presentation.

| # | Team | Score | Judge | Product Design | Innovativeness | Scalability | Presentation | Total |
|---|---|---|---|---|---|---|---|---|
| 1 | CB | 80.25 | EA | 28 | 28 | 28 | 8 | 92 |
| | | | IM | 30 | 30 | 25 | 10 | 95 |
| | | | IO | 25 | 25 | 20 | 8 | 78 |
| | | | SA | 17 | 17 | 15 | 7 | 56 |
| | | | | | | | | |
| 2 | TZ | 71.25 | EA | 22 | 20 | 24 | 7 | 73 |
| | | | IM | 25 | 15 | 25 | 10 | 75 |
| | | | IO | 28 | 28 | 25 | 9 | 90 |
| | | | SA | 14 | 15 | 12 | 6 | 47 |
| | | | | | | | | |
| 3 | HC | 58.75 | EA | 12 | 15 | 10 | 10 | 47 |
| | | | IM | 25 | 15 | 20 | 10 | 70 |
| | | | IO | 20 | 20 | 15 | 8 | 63 |
| | | | SA | 15 | 18 | 16 | 6 | 55 |
| | | | | | | | | |
| 4 | QS | 57.5 | EA | 18 | 14 | 20 | 7 | 59 |

| # | Team | Score | Judge | Product Design | Innovativeness | Scalability | Presentation | Total |
|---|---|---|---|---|---|---|---|---|
| | | | IM | 20 | 10 | 15 | 5 | 50 |
| | | | IO | 25 | 27 | 20 | 8 | 80 |
| | | | SA | 12 | 12 | 12 | 5 | 41 |
| | | | | | | | | |
| 5 | VP | 57 | EA | 21 | 20 | 24 | 7 | 72 |
| | | | IM | 20 | 15 | 20 | 10 | 65 |
| | | | IO | 15 | 5 | 16 | 7 | 43 |
| | | | SA | 15 | 15 | 12 | 6 | 48 |
| | | | | | | | | |
| 6 | ZZ | 55.33 | EA | 15 | 10 | 18 | 18 | 61 |
| | | | IM | 15 | 15 | 15 | 4 | 49 |
| | | | IO | 0 | 0 | 0 | 0 | 0 |
| | | | SA | 16 | 17 | 16 | 7 | 56 |
| | | | | | | | | |
| 7 | LK | 53 | EA | 22 | 22 | 21 | 6 | 71 |
| | | | IM | 5 | 5 | 5 | 2 | 17 |
| | | | IO | 20 | 24 | 25 | 6 | 75 |
| | | | SA | 13 | 17 | 14 | 5 | 49 |
| | | | | | | | | |
| 8 | KS | 46 | EA | 15 | 18 | 20 | 7 | 60 |
| | | | IM | 10 | 5 | 5 | 5 | 25 |
| | | | IO | 15 | 10 | 20 | 6 | 51 |
| | | | SA | 14 | 14 | 14 | 6 | 48 |
| | | | | | | | | |
| 9 | TI | 39.5 | EA | 15 | 10 | 10 | 5 | 40 |
| | | | IM | 5 | 5 | 5 | 2 | 17 |
| | | | IO | 20 | 25 | 24 | 8 | 77 |
| | | | SA | 7 | 7 | 7 | 3 | 24 |
| | | | | | | | | |
| 10 | RT | 0 | EA | 0 | 0 | 0 | 0 | 0 |
| | | | IM | 0 | 0 | 0 | 0 | 0 |
| | | | IO | 0 | 0 | 0 | 0 | 0 |
| | | | SA | 0 | 0 | 0 | 0 | 0 |

Table 8.3: Hackathon Final Score

Team 10 did not make a final presentation and was not rated.

### 8.1.3.2 Hackathon Pitch Result

As part of the directive for the competition, participants were asked to implement a minimum of three of the twelve heuristics. 89% of the participating teams implemented *integration.* 67% implemented *proportionality*, *identity,* and *integrity.* Only 11% of the teams applied *authenticity*. The team that used the highest number of heuristics in developing their MVP applied 67% of the heuristics while the one that applied the minimum used 25% of the heuristics. Table 8.4 provides details of how the teams applied the heuristics.

| # | Team | Heuristics Applied | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Integrity | Proportionality | Transparency | Empowerment | Identity | Reliability | User Support | Accessibility | Authenticity | Compliance | Alignment | Freedom |
| 1 | CB | | √ | √ | √ | √ | √ | √ | | | | √ | √ |
| 2 | TZ | √ | | | | | | | √ | √ | √ | √ | |
| 3 | HC | √ | | | | | | | √ | | | | √ |
| 4 | QS | √ | √ | | | √ | √ | √ | | | | | √ |
| 5 | VP | √ | | | | √ | √ | | | | | | |
| 6 | ZZ | √ | √ | | √ | √ | √ | √ | | | | | |
| 7 | LK | √ | √ | | | √ | √ | | | | | | √ |
| 8 | KS | √ | √ | | | | | √ | | | √ | √ | √ |
| 9 | TI | √ | √ | √ | | √ | √ | | | | √ | | |

Table 8.4: How Teams Applied Heuristics

Each participating team made a demo presentation of their MVP with a particular focus on how the heuristics were applied and the differences between the version of the product with the heuristics applied and the version without the heuristics. Extracts from the pitch of each team are described below.

i. Team 1 (CB)

The team built and presented an MVP called Escrow. Escrow is a solution that facilitates remittances and savings, and is also used as a payment gateway and marketplace targeted at low earners. The solution was built to be compatible with both basic and high-end smartphones. To develop the MVP, the team accessed APIs for payments and B2B transfers, customer wallets, and airtime purchases. These APIs were provided by the organising partners based on the needs and requirements from the lean canvas of the participants. Furthermore, the team described how it applied the heuristics to develop the MVP. In describing how they implemented *proportionality,* the team demonstrated how the system made users aware of every stage and step taken in a transaction flow with appropriate feedback. This they said was a result of their consideration for levels of user knowledge and sensitivity levels of transaction. To further buttress *proportionality*, the team demonstrated the use of the app with an illiterate market trader to show that anyone who can top up mobile phone credit would be comfortable using the system. For *identity*, the team demonstrated how the device fingerprint was mapped with the set access pattern lock

during first use and used to verify each transaction process “under the hood”, ensuring a user is uniquely identified and verified throughout a transaction lifecycle. Describing how *freedom* was implemented, the team demonstrated through various levels of funds transfer sensitivity, how the system allows users to choose the appropriate security levels. Also, this was implemented on the transaction level where the team demonstrated how users could choose between making a direct transfer to an account from their wallet balance and sending an e-cheque generated to a beneficiary to be cashed into the beneficiary’s wallet at a later date. With the introduction of easy-to-use e-cheques in the form of QR-codes generated from transactions, the team demonstrated how funds can be transferred via other digital formats like digital or printable pictures and only the intended beneficiary can successfully use it. The team believes this was done in a comprehensible, verifiable, and accessible way, satisfying the principle of *transparency*. In demonstrating the suitability of the solution for the visually impaired, the team demonstrated how in-app voice command was implemented. Similarly, the team also demonstrated how they applied all the heuristics they indicated.

Explaining the difference between the control and the system with the heuristics applied, the team demonstrated that the systems without the heuristics had basic consideration for authentication but had no consideration for usable security in the build and test of the solution.

The judges sought to understand the implication of the application of the heuristics on compute time and resources. In response, the team demonstrated that applying the heuristics added slightly more compute time and resources when compared to the control system. The team further noted that while it was possible to challenge for authentication at every transaction window, it had to ensure the security applied does not irritate users and become counterproductive. The judges advised the team to ensure that in subsequent builds, the actual measurement of time and resources for the application of the heuristics was noted to ensure a more effective and efficient application and use.

ii. Team 2 (TZ)

The team made a demo presentation of their MVP they tagged Avocado, a multipurpose mobile finance solution that helps users access and manage various bank accounts, wallets, and virtual accounts, from a single point. It enables users to send and receive payments and access value added services (VAS) at ease from a single point. In developing the MVP, five APIs were consumed. The APIs include wallet creation and management, bank account and one-time password (OTP)

creation, payment management and VAS, virtual account for other direct debits, and API for notifications and airtime. The team demonstrated how they deployed five usable security heuristics indicated in Table 8.4 in developing the MVP. The team demonstrated how it introduced the functionality of an application-level master PIN for dynamic authentication which is applied based on the sensitivity of a transaction. They also demonstrated how they integrated the application with a mobile OS-level accessibility tool for screen reading and voice. Furthermore, the team demonstrated how it applied the PCI DSS guideline to develop the solution and provided additional functionality for audit.

In describing how the authentication works in the use case for funds transfers and utility payments, the team demonstrated that their implementation ensures that a device-level authentication would be required for transfers and utility payments. They further demonstrated that at the back-end a cross-site cookie exists. The cookie fetches every form and hash with the user's IP address and location and sends it to the back end before the transaction is consummated. The process kept a copy of the transaction even when it failed. This they claim makes the system learn user patterns, based on which any change in transaction pattern would be flagged for reauthorisation. In summary, user transactions were hashed and compared with user behaviour (dynamic authentication). If location, for instance, changes, the system would challenge the user for reauthentication.

Comparing the MVP before and after the application of the heuristics, the team explained that the heuristics made the system more transparent to the user and had more consideration for simplifying security for users during design. The team mentioned that before the session on the need to apply the usable security heuristics, they had no defined way of ensuring they cater to usable security except to address any issue that arises from user or customer complaints. However, they noted that app and code size increased slightly with the application of the heuristics compared to when they were not applied.

iii. Team 3 (HC)

The team presented a solution they called Mubia, a financial technology platform that uses a secured hashing algorithm built and integrated with blockchain technology to facilitate offline end-to-end transactions without third-party access to user data. They noted that the solution was also suited for users who have only access to feature phones. The team demonstrated how transactions with the solution were secure, easy, and fast to use. In developing the solution, they consumed the APIs for

interbank, name inquiry, SMS, and USSD. The team used PHP and JAVASCRIPT for the bank end and Kotlin for the mobile app.

Concerns were raised by judges on the security weaknesses of USSD. The team was able to demonstrate that they have implemented encryption to help mitigate the concerns. In response to the question of how usable security was implemented before the heuristics were introduced, the team simply admitted they only focus on functionality and depend on any security made available for the device or any environmental implementation.

iv. Team 4 (QS)

This team had the largest membership with members comprising one UX researcher, an interactive designer, a visual designer, two front-end developers, three back-end developers, and four Android mobile developers. The MVP presented by the team provided a platform that allows buyers and sellers to transact safely. It provides an instant escrow pay link that ensures seamless trading without the fear of cybercrime and fraud. The team claims the solution is important as cybercrime slows down the adoption of fintech amongst the unbanked. The solution ensures that the buyers' funds are securely held until both parties are happy with the transaction by providing a transparent and accountable process. To develop the solution, the team used API for SMS and OTP, virtual account creation, and account name inquiry. They demonstrated how the heuristics identified in Table 8.4 were applied in their MVP.

The most important change brought about by the application of the heuristics was to make the team think more critically about usable security and provide an approach on how best to apply the heuristics practically. The panel provided feedback on the need to review the number of mandatory fields in the MVP so it does not become a disincentive to users. On the difference between the MVP with heuristics and the one without heuristics, the team demonstrated further that theirs was platform segment agnostic — it can be used for the banked and unbanked segment — and did not require much technical know-how to use.

v. Team 5 (VP)

The team presented an MVP they termed Tuper. Tuper is an online selling and payment transfer platform where buyers and sellers come together to get business done. Tuper makes use of two APIs from the financial services sector sandbox. These include an SMS API and a payment transfer API. The team demonstrated how Tuper makes use of secure encryption for data transmission between the buyer and the seller. When a customer places an order, it gets encrypted before being forwarded to

the seller. The decryption key is sent to the seller through SMS. The order can only be viewed by the seller if he/she has the decryption key. This is made so because a seller's account might get breached and his login information might be in the hands of an intruder. The team mentioned that even if the intruder gets into a seller's account, they would not be able to view details of a seller's transactions because the decryption key is only sent to the seller's registered phone number through SMS. For the app demonstration, the decryption code was generated and displayed on the platform for testing. They demonstrated that their implementation addresses concerns with unauthorised modification of transactions and privacy breaches. Also, they demonstrated how their implementation facilitates effective feedback throughout the phases of a transaction.

Furthermore, the team demonstrated that through incremental innovation, Tuper makes use of encryption to facilitate the secure transmission of transaction data between buyers and sellers. While encryption already exists, Tuper applies it for transaction facilitation. The key difference identified by the team between MVP without the heuristics and MVP with heuristics was that the former had no transaction ID to facilitate reliability. Like previous teams, they emphasised the fact that heuristics reminded them to implement existing security solutions in mind to address these heuristics.

vi. Team 6 (ZZ)

The team presented an MVP called Utopia. The team presented Utopia as an all-encompassing financial service application with integrated cybersecurity functionalities that leverage six security heuristics to deliver a highly secured payment solution. Its features include deposit/transfer, bill payment, savings, merchant payment, loan, etc. The solution can onboard both the banked and unbanked. API for SMS to send user messages and payments using a bank account was consumed. The team demonstrated how the system can also allow one account per device and how transaction tiers are used to address *proportionality and reliability.* The team also demonstrated options to opt out of sessions and hide account balances. They showed how users have the option to disable or enable 2FA for a specified duration and transaction type.

Panellists sought to understand what would happen to a customer's account in the event of a missing phone. This was in light of the fact that the solution recognises one device to one account. In response, the team demonstrated how the solution saves device information during onboarding and in the event of a missing device. A user

can log on to another device not on the database. Immediately the user logs on, the device ID will be updated. Therefore, the loss of the device does not equate to loss of account. The system generates a unique ID for each session not a unique device for ID.

vii. Team 7 (LK)

The team presented Virtual Pocket Money (VPM) a secured**,** quick, and simple transfer method that makes use of QR codes or unique IDs for all payments with very low service charges, the provision of a savings opportunity, and advancement in security methods taken to protect the customers. API for account creation was used. They further described some functionalities of the solution as follows:

i. Both SMS and email tokens are sent to the user when enabling a new device to use the app.
ii. The app has an embedded authenticator which has a password that is different from the normal app password.
iii. The embedded authenticator generates a 6-character token within the application that must be provided by the user before transferring funds or payment for any goods and services.
iv. The token lasts for only 45 seconds and users have only 3 trials to provide the right token for every transfer or purchase transaction after which the account will be suspended till it passes a security verification process.
v. The location of the device during every transaction is always recorded for cases of stolen devices or emergencies.
vi. Each account can only be signed in on one device at a time.

They demonstrated how the solution implemented the heuristics, by providing a functionality to check the progress of transactions, helping users to be aware of the status of their transaction at any time. They also provided thresholds for transaction limits and applied appropriate security based on the amount involved. The system also provides a unique transaction ID which enables the system to provide the correct status of all transactions to guide against falsification of receipts.

vii. Team 8 (KS)

The team presented an MVP called Quick Save which seeks to encourage a savings habit by automating the process. The solution enables users to save a fraction of their expenses as they make transfers. The customers' savings will be a minimum of 10 percent of every transfer made, At the end of a certain period, the customer can get access to his/her accumulated savings from transfers. The team mentioned that users

perform transactions every day sorting out various needs and wants. Quick Save ensures a saving habit is a norm while allowing people to do seamless transfers to one another on the app.

In demonstrating how the heuristics were applied, the team showed how settings are displayed and defaulted to users based on their account balance. The setting can be customised by users as they desire. Furthermore, they showed how the system prevents brute force attacks by ensuring backend API throttling to limit attackers from calling APIs multiple times trying random passwords or PINS. They also opined that the security settings designed for the system align with users' mental models. They claimed users are familiar and comfortable with the security features. They demonstrated how the system sends notification messages (SMS and/or email) for login and transactions performed, to keep the user informed of activity on their account on the app. They showed that it was configurable, as users are given the freedom they want to choose if they want notifications or not.

The team believes there was an interaction within the heuristics, and they can be addressed together as they have learned from their implementation experience. They noted that new locations and new devices are functionalities added because of heuristics that were not considered in the version before the use of heuristics. The team found out that by addressing security concerns using the heuristics, they were able to address usability as well. The team also mentioned that the application of the heuristics helped with better user engagement.

viii. Team 9 (TI)

The team's MVP was called Secured Save. The solution was created to help students save up for a long-term project. It leverages cloud computing and AI. The mobile-based transaction starts from the verification of credentials and it also shows the point of integration with cloud services. The API used include voice, SMS, authentication, Cloud Firestone, TensorFlow, and facial detection and recognition. To demonstrate how the heuristics were implemented in developing the solution, the team showed how the application adopted cloud authentication to authenticate a user each time the user wanted to use the application. It further applied facial recognition to authenticate the user in an advanced level of transaction. The use of icons and standout widgets made it easier to identify and use security mechanisms.

In response to the impact of the heuristics on their development practice, the team mentioned that the use of the heuristics further strengthens the integrity of the

transaction and provides a more robust authentication process. The team tried to link expert systems and the use of heuristics.

The process and the outcome of the hackathon addressed the objective of this study which included:

- To demonstrate how the usable security heuristics developed as part of this PhD can be implemented in the development of MFS
- To understand the differences in terms of usable security between developing an MFS solution without applying the heuristics vs. when the heuristics are applied
- To obtain feedback from participants in the hackathon as a process for continuous improvement of the heuristics.

## 8.2 CASE STUDY 2: BLACK-BOX EVALUATION

In Chapter Seven of this study, the researcher explained that the twelve usable security heuristics developed have two applications. Firstly, they is designed to be applied in the development of MFS and secondly, they can be applied to evaluate usable security compliance in existing MFS solutions. Section 8.1 has demonstrated how the heuristics can be applied in developing MFS solutions. This section is focused on how the heuristics can be applied to evaluate compliance with usable security principles.

The review of similar literature on using heuristics to evaluate an existing system and the need to address concerns from the conceptualisation phase of this study, necessitate the choice of the approach adopted for this case study. The heuristics evaluation method is a usability inspection method that is used to evaluate usability problems by applying heuristics. The model involves three to five experts working independently to identify usability problems, and using three measurement metrics, severity, frequency, and criticality, to rate a consolidated list of identified issues. The authors opined that the model is easy to apply and does not require much planning. However, they also noted that users are not involved, and the approach does not recommend how to address the problem. Furthermore, they noted that a lack of product knowledge by evaluators might hamper the outcome of the evaluation (Quiñones and Rusu 2017). Another model leveraged expert review with a focus on a targeted group of experts in alignment with the research question of their study. More so, they stated that user reviews and the collection of system feedback could also be used for the evaluation (Feth and Post 2019).

In Chapter Five of this thesis, it was demonstrated that various use behaviours and practices have an impact on usable security and both supply and demand side

stakeholders have a role to play in ensuring the implementation of a usable security mechanism in MFS. It is therefore imperative to adopt an approach that will help these stakeholders participate in the evaluation, even when they do not know the internal workings of the product. The approach should also be in alignment with standard development methodologies like Agile and Systems Development Lifecycle (SDLC) so that it can be conducted as part of the process and not as an additional task. Consequently, this thesis evaluated the product using heuristics as a part of the user acceptance testing (UAT) which is the final stage of typical software development before deployment (Elazar 2023). The adoption of black-box testing as against white-box testing also meant participants did not need to know the internal workings of the system to participate in the test. Adopting this methodology ensures that evaluation is conducted from the user's viewpoint, that non-technical participants can participate, and that participants are not expected to have systems development skills or any technical knowledge (Verma et al. 2017).

### 8.2.1 Experimental Approach and Setup

To conduct the evaluation, five key activities were carried out as follows:

i. Identify applications to evaluate

Eight candidate MFS solutions were identified for evaluation based on the following criteria:

- MFS services must have been offered for at least a year. This was to ensure all candidate MFS are stable applications that were not just introduced to the market
- All participants should have access to the product. This was to enable a seamless evaluation process
- The MFS should be available on Android and IOS. This was to examine the difference in behaviour on both mobile operating systems during the evaluation.

Four of the identified MFS were offered by conventional banks while the other four were fintech products.

ii. Develop evaluation tool

To conduct the evaluation, it was important to convert the heuristics to a language that would be understood by the testers. To that effect, a test script was developed to guide the process. The expected outcome from the test should be a pass (P), a

fail (F), or a partial pass (p). The detailed test script is attached in Appendix V of this thesis.

iii. Recruit participants

Four participants were recruited to participate in the evaluation. While all participants had at least an undergraduate degree, two of the participants were users who had no technical know-how, while the other two were experts in cybersecurity and quality assurance.

iv. Setup and conduct evaluation

The evaluation was conducted via Zoom to manage costs due to the geographical location of the participants and the cost and time implication of bringing them under one roof. The participants were briefed on the objective of the evaluation and what was expected of them. During the first session, the details of the twelve heuristics and the test script were explained to them. The researcher also provided answers to all the questions they raised. The evaluation was conducted over 3 sessions across one week. Each session lasted 30 minutes on average.

v. Document findings

The process and findings of the evaluation were then documented. An extract of this is presented in the next section of this thesis.

### 8.2.2 Results from Evaluation Exercise

In all, 75 cases were tested for two major mobile operating systems, iOS and Android, making it a total of 150 distinct test cases. Of the 150 test conditions, 46 tested functional requirements, 44 tested non-functional requirements, 38 tested technical requirements and 22 tested transitional requirements. In terms of priority, based on the MoSCoW methodology, 108 of the test cases were Must Have, 34 were Should Have and 8 were Could Have. Table 8.5 provides a summary of the UAT.

| | | Requirement | | Priority | | |
|---|---|---|---|---|---|---|
| # | Heuristic | Type | # Tested | MoSCoW | No. | Total Test |
| 1 | Integrity | Functional | 4 | Must Have | 10 | 14 |
| | | Non-Functional | 4 | Should have | 2 | |
| | | Technical | 6 | Could Have | 2 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 2 | Proportionality | Functional | 4 | Must Have | 10 | 20 |
| | | Non-Functional | 8 | Should have | 8 | |
| | | Technical | 8 | Could Have | 2 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 3 | Transparency | Functional | 4 | Must Have | 8 | 10 |

| # | Heuristic | Requirement | | Priority | | Total Test |
|---|---|---|---|---|---|---|
| | | Type | # Tested | MoSCoW | No. | |
| | | Non-Functional | 2 | Should have | 2 | |
| | | Technical | 4 | Could Have | 0 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 4 | Empowerment | Functional | 2 | Must Have | 6 | 14 |
| | | Non-Functional | 4 | Should have | 6 | |
| | | Technical | 2 | Could Have | 2 | |
| | | Transitional | 6 | Won't Have | 0 | |
| 5 | Identity | Functional | 4 | Must Have | 8 | 8 |
| | | Non-Functional | 2 | Should have | 0 | |
| | | Technical | 2 | Could Have | 0 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 6 | Reliability | Functional | 4 | Must Have | 12 | 16 |
| | | Non-Functional | 6 | Should have | 4 | |
| | | Technical | 2 | Could Have | 0 | |
| | | Transitional | 4 | Won't Have | 0 | |
| 7 | User Support | Functional | 4 | Must Have | 18 | 20 |
| | | Non-Functional | 4 | Should have | 2 | |
| | | Technical | 6 | Could Have | 0 | |
| | | Transitional | 6 | Won't Have | 0 | |
| 8 | Accessibility | Functional | 4 | Must Have | 4 | 4 |
| | | Non-Functional | 0 | Should have | 0 | |
| | | Technical | 0 | Could Have | 0 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 9 | Authenticity | Functional | 4 | Must Have | 6 | 6 |
| | | Non-Functional | 2 | Should have | 0 | |
| | | Technical | 0 | Could Have | 0 | |
| | | Transitional | 0 | Won't Have | 0 | |
| 10 | Compliance | Functional | 4 | Must Have | 8 | 10 |
| | | Non-Functional | 4 | Should have | 2 | |
| | | Technical | 0 | Could Have | 0 | |
| | | Transitional | 2 | Won't Have | 0 | |
| 11 | Alignment | Functional | 4 | Must Have | 10 | 16 |
| | | Non-Functional | 4 | Should have | 4 | |
| | | Technical | 4 | Could Have | 2 | |
| | | Transitional | 4 | Won't Have | 0 | |
| 12 | Freedom | Functional | 4 | Must Have | 8 | 12 |
| | | Non-Functional | 4 | Should have | 4 | |
| | | Technical | 4 | Could Have | 0 | |
| | | Transitional | 0 | Won't Have | 0 | |
| | Total | | | | | 150 |

Table 8.5: UAT Summary

Test results show that the compliance metric has the highest pass rate, with 100% on both platforms, indicating that the systems fully meet the set standards in this regard. However, participants noted that the basic compliance test was based on input

validation and user support. Compliance with coding principles would require access to the codes which should be incorporated into unit tests and system tests where the objective is a white-box testing of internal structure before exposure to the users.

*Freedom* has the highest failure rate on both platforms, with a 13% failure rate, which is considerably higher than other metrics. The pass rate for most metrics is quite high, mostly above 80%, indicating a generally good performance on both platforms. For reliability, Android (84%) and iOS (83%) have similar pass rates, but iOS has a higher partial pass rate (14%) compared to Android (11%). It was noted though, that some of the apps only show the history of successful transactions not failed transactions, while one of the fintech apps shows all. The bank apps only show when a transaction is reversed, not when it fails.

*User support* and *accessibility* have identical distributions of pass, partial pass, and fail percentages on both platforms. For user support, it was noted that two of the fintech-based apps have prompts that assist with walk-throughs and make onboarding more seamless and more interactive than conventional bank mobile apps. Furthermore, taking a screenshot from the two fintech apps can be enabled and disabled, but not all the apps have that capability. It was observed that no in-app capability was fully functional in any app. However, assistive tools available via OS could be used by the apps. For instance, Google Assistant can open the app, but cannot be used to perform further in-app tasks as there is a boundary of authority within device tools and apps. Participants agreed that in-app accessibility functions are required and a separate requirement for that should be developed to address that. It was also recommended that a backend integration of some OS assistive tools and the apps should be considered subject to the suitability of license requirements from the solution provider.

For transparency and identity, it was noted that iOS has a slightly better performance concerning the pass rate in these metrics compared to Android. However, participants believe the influence of the network carrier on the results should be examined to further validate this conclusion.

When testing for authenticity, it was noted that apps should always call the server for authorisation, and client-side checks should be discouraged. Session expiring time was used to check app compliance with server-side checks. Only one of the bank apps did not time out when examined. One app timed out after a minute and 20 seconds of inactivity, another timed out after 60 seconds of inactivity, one of the apps took 3 minutes to become inactive, and the status of others was not immediately

known until a new transaction was attempted, then the system challenged the user for login credentials.

What should be more secure and what should be more usable was a constant conversation throughout the test. For instance, as soon as the testers log on to some of the apps, the transaction history appears automatically. Some of the participants believe another level of access should be required for that, while others believe it is okay as it is.

Feedback from the app store revealed certain facts about customer frustration on the app. It was observed that the last updated version of MF2 was 8 months before the date this study was conducted.

A detailed analysis of the *freedom* metric is recommended to understand the reasons behind the high failure rate and to formulate strategies to improve in this area.

Participants noted that it might be beneficial to closely scrutinise and perhaps enhance the testing parameters for metrics such as *reliability* which show higher partial pass rates, to possibly push those towards a full pass.

Table 8.6 provides an extract of the UAT test script. The detailed text script is in Appendix V

| Req Type | Req ID | Req Description | Priority | Test Case ID | Pre conditions | Test Steps | Expected Results | Post conditions | MF1 Test Result | MF2 Test Result | MF3 Test Result | Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Functional | FR001 | The system shall implement mechanisms to ensure the integrity of user financial transactions. | Must-have | TC001 | User has initiated a financial transaction. | Execute the transaction in the system. Check logs/records for integrity mechanisms in place. | Transaction should be completed successfully with all integrity mechanisms in action (like no data tampering). | System returns to stable state, ready for the next transaction. | Pass | Pass | Pass | Minor delays observed in MF4, needs optimization. |
| Functional | FR002 | The system shall perform regular checks to validate the integrity of stored user data and transaction records. | Must have | TC002 | Regular checks are enabled in the system settings. | Trigger a manual/automatic integrity check in the system. | System should be able to validate the integrity of the stored data successfully; any discrepancies should be reported. | System returns to stable state, ready for the next operation. | Pass | Partial Pass | Pass | MF5 reported some discrepancies, further investigation needed. |
| Non-Functional | NFR005 | The system shall employ encryption mechanisms to protect user data during transmission and storage. | Must have | TC003 | System is set up with encryption mechanisms enabled. | Transmit and store data, then check if encryption is effectively applied during these processes. | Data should be encrypted during transmission and storage, complying with specified encryption standards. | System remains secure, ready for next operation. | Pass | Pass | Pass | Partial encryption failure noted in MF7, requires review. |

Table 8.6: Test Script Extracts Showing Some Output from Android Test for *Integrity*

## 8.4 CHAPTER SUMMARY

This chapter demonstrated how the artefact developed as part of this thesis was applied to real-life case studies. The first case study demonstrated how the heuristics can be integrated into the MFS application development process through a hackathon that saw the participation of 144 teams with 10 finalists and 9 minimum viable products demonstrated. Key lessons and learning from the process were highlighted and would serve to strengthen the process going forward. Furthermore, the second case study involved using heuristics to conduct black-box user acceptance testing by evaluating 150 test cases. Key findings and recommendations from the study were also highlighted.

This chapter addressed the last objective of the thesis; *Objective 5: To exploit and disseminate the validated solution including recommendations.*

# CHAPTER NINE: DISCUSSION

This thesis examined cybersecurity challenges in mobile financial services by conducting a state-of-play study on MFS security, conceptualising the problem space, developing a solution, and using the solution to solve a real-world problem.

In this chapter, a synthesis of the result presented in this thesis is analysed and presented along with a summary of the key findings from the studies conducted, and how it addresses the problem statement and research questions raised in Chapter One of this study. Furthermore, the chapter highlights the process followed during the studies and the lessons learned from the experience.

## 9.1 SUMMARY OF KEY FINDINGS

Eight studies were conducted as part of this PhD addressing various elements of the research questions and thesis objectives. Table 9.0 shows the summary of the studies conducted.

| # | Study | Description | Methodology | Sample Size | Outcome |
|---|---|---|---|---|---|
| 1 | Mobile Financial Services Sociotechnical System | Leveraged human factor approaches to understand cybersecurity issues and the objective of how to address them | Soft system methodology, interpretive structural model | 35 | Developed soft system model of MFS STS and identified about 269 cybersecurity problems in MFS STS |
| 2 | End-user Usable Security Behaviour | Examined how user behaviour impacts usable security in MFS | Survey, principal component analysis | 698 | Identified usable security behaviours of users and usable security factors |
| 3 | Usable Security Design and Development Practices | Examined usable security development practices and their impact on usable security | Semi-structured interview, thematic analysis | 37 | Identified usable security factors from a DevOps perspective |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Developing Usable Security Requirements For MFS | Developed and validated requirements based on data collected from previous studies | Requirement Analysis, MoSCoW | 5 | Validated requirements |
| 5 | Development of Usable Security Heuristics | Developed heuristics to address usable security issues in MFS | Literature review, semi-structured interview | 698 (iteration 1), 37 (iteration 2),14(validation) | Developed and validated 12 usable security heuristics |
| 6 | Hackathon Case Study | Implemented 12 usable security heuristics in developing MFS through a hackathon | Hackathon | 44 teams with 10 finalists | Feedback and recommendations on how to integrate usable security heuristics into MFS design and development |
| 7 | Black-box Testing Case Study | Used 12 heuristics to evaluate the usable security readiness of 5 MFS solutions | Black-box testing | 4 | Usable security problems and recommendations |
| 8 | Usable Security Consideration for the Visually Impaired | Developed requirements for the evaluation of MFS readiness for the Visually impaired | MoSCoW, Thematic Analysis | 5 | Results of evaluation of usable security readiness for 5 MFS solutions |

Table 9.0: Summary of Findings

The first study leveraged human factor approaches to examine the cybersecurity problem in mobile financial services sociotechnical systems from the viewpoint of stakeholders in the ecosystem. The second study leveraged a quantitative study to

analyse the usable security behaviour of 698 respondents to identify factors that can improve usable security. Similarly, the supply-side study of 37 participants comprising DevOps members and chief information technology officers was carried out to identify developer practices and their impact on the usable security of MFS. Through an iterative approach, 12 usable security heuristics together with recommendations on how to apply them were derived based on the studies conducted and a review of relevant literature. These heuristics were applied in a hackathon competition to demonstrate how they can be used in developing usable secure MFS and were then used to evaluate the usable security conditions of existing systems.

The rest of the chapter presents an analysis of the synthesis of these studies and how they address the research objectives.

## 9.2 MOBILE FINANCIAL SERVICES SOCIOTECHNICAL SYSTEM

The human element has been identified as the weakest link in cybersecurity. In a quantitative study of 462 participants, to investigate the nature of the weakest link based on participants' cybersecurity judgment on 16 scenarios, 23% of the participants had a correctness score of 50% or less and were termed the weakest of the weakest (Yan et al. 2018). Similarly, in a systematic literature review that was conducted, it was noted that unlike in the past when there was a more technology-based study on cybersecurity, there is increasing interest among computer science researchers in the human aspect of cybersecurity. The human factor study covers three key areas; user characteristics, cybersecurity system aspect, and usable systems. Furthermore, the multidimensional aspect of cybersecurity together with the need for a mix of sociotechnical features that protect users need to be put in place (Rahman et al. 2021). Similar to the findings from the literature, our study revealed that various strong technology countermeasures to improve cybersecurity in mobile financial services exist (Kunda and Chishimba 2018; Ibrahim et al. 2019). Despite the presence of these countermeasures, mobile financial services vulnerability leading to actual financial loss still exists Odueso (2022) and Khandelwal (2017), buttressing the consensus among cybersecurity professionals that security depends on people more than on technical controls and countermeasures (Benson et al.2019).

To understand the human element in MFS to strengthen cybersecurity in the system, an exploratory study of the MFS ecosystem was conducted to contextualise the nature of cybersecurity problems in mobile financial services, from the viewpoint of the human element in the ecosystem, leveraging human factor approaches. Human factor approaches guide the contextualisation of ill-defined complex sociotechnical problems like that of mobile financial services (Pollini et al. 2022). Through

stakeholder analysis, six stakeholder groups were identified in the MFS ecosystem. Leveraging soft systems methodology, interpretive structural model, and expert reviews, 269 issues together with objectives for addressing them were identified in the MFS ecosystem. Each of the participating teams grouped the identified issues based on their worldview. While one team grouped the issues into process-related, technology-related, people-related, and policy-related, another group identified issues into infrastructure-related, awareness-related, process-related, and cross-cutting issues. Also, while one of the participating teams prioritised the need to adopt an industry-wide approach to addressing cybersecurity issues in MFS, another team prioritised the need for awareness of social engineering.

A consolidated soft systems model provided insight into the nature of interaction in the ecosystem, revealing that cybersecurity in mobile financial services is a sociotechnical problem. To be effective in addressing vulnerabilities, cybersecurity countermeasures must consider interactions between entities in the MFS sociotechnical system, leveraging human activity systems to link system thinking to real-world problems. An expert review of the output of the soft systems study emphasised the importance of improving trust and addressing concerns related to unsecured third-party applications, irregular applications, OS updates, and compliance-related concerns. Furthermore, they believe actions to improve cybersecurity in the MFS ecosystem should prioritise improving trust by improving the usability of the MFS solution. While other studies demonstrated how to conduct a human or user-centric study of a cybersecurity ecosystem, which led to a focus on an approach than the actor of the ecosystem, our approach provided insight into the issue from the perspective of the users in the ecosystem, who are directly impacted with the problem (Feth and Polst 2019). Furthermore, in examining the human factor in cybersecurity, studies have shown that addressing it from the end-user perspective alone might not be sufficient in addressing the issue, as supply-side actors like developers are also affected by human weakness (Green and Smith, 2016). This study also has consideration for that as it focuses on both supply and demand side actors in the ecosystem.

## 9.3 USABLE SECURITY IN MFS

One key recommendation from the expert review of the study of the mobile financial services sociotechnical system was the need to improve through improving usable security in MFS. Usable security is a problematic area in the human factor study of cybersecurity and has received some attention over the years (Garfinkel and Lipford 2014). The trade-off between usability and security and the impact of usable security

mechanisms on users and developers are some key problematic areas in usable security as highlighted in Chapters Two and Five of this thesis.

Designing usable security solutions has focused on gathering and fusing usability and security requirements. To enable us to address usable security from a user viewpoint, it was imperative to understand the drivers for end-user's usable security decisions in the use of MFS. Similarly, key supply-side actors like MFS developers were examined to understand how their practices impact usable security in MFS.

An empirical study conducted on 698 MFS users reveals that user perception should be examined when it comes to making design decisions for MFS. When asked about the complexity of the system, only about 13% of the respondents perceived MFS as complex, but when an analysis was conducted on several variables that measured complexity, it turned out that about 88% of the respondents found the system complex. Similarly, respondents claimed to have an above-average understanding of privacy, but when their use behaviour was examined, the choices they made in the use of MFS showed a poor understanding of privacy and its implication on security. The impact of user perception as it affects its security, credibility, and behavioural control has been researched (Khasawneh et al. 2018). However, this study provides details on how perception affects usable security from the MFS user's perspective and how it can be used to improve usable security design in MFS.

Users create their MFS "single sign-on" by either using the same logon credential for their OS and their MFS or by saving their MFS credentials on their phones. Even though users are not averse to security controls in the use of MFS, they are devising unsafe means to make it easier for them to access services on their MFS. This typifies users' reaction to security mechanisms with poor usability consideration as highlighted in the literature (Hof 2015).

Users inherently exhibited good security behaviours. For instance, without understanding the implications of updating their MFS application, and phone OS, the majority of the respondents tend to upgrade their phone OS and MFS application regularly. The study revealed a correlation between observable user behaviours in the use of MFS with both usability and security. Though latent constructs exist that have a direct correlation between usability and security, not all latent components have a direct correlation with both usability and security. However, because all the observable constructs load on each other, a direct correlation between a latent construct and an observable construct might lead to an indirect correlation with usability and security.

Based on the result of this study, a one-size-fits-all solution for usable security might not be effective in addressing the usable security needs of all users, but consideration of various categories of users in designing security control for MFS might improve the chances of success. Furthermore, the study revealed that understanding user cognitive and behavioural dynamics in the use of MFS and considering them in the security design process for MFS will lead to an MFS solution that is highly secure yet highly usable for all categories of users.

Analysis of data obtained from the semi-structured interview conducted for 15 bank CIOs and 22 DevOps team members reveals that MFS developers would benefit from a documented approach on how to integrate usable security into MFS design. Moreover, participants believe usability and security should be implemented together to get the best results as implementing them separately would lead to an imbalance. Furthermore, the study revealed how usable security can improve trust which is a position supported by other literature (Khasawneh et al. 2018). The need to address roles and responsibilities for usable security in MFS was proposed in this study. This is to address the current situation where it is not well defined, leading to usability issues in security mechanisms. Analysis of feedback from participants also revealed that usable security requirements should not be restricted to knowledge of the development team or some selected customers but incorporate input from extensive user surveys. This was in line with the approach adopted for this study where the requirement for usable security was developed based on data collated from user surveys and interviews with solution providers, which led to robust requirement documentation for usable security in MFS.

In addition to revealing the impact of users' and solutions providers' behaviours and practices on usable security for MFS, these two studies provided the requirement for developing usable security for MFS, which informed the development of usable security heuristics for MFS as detailed in the next session.

## 9.4 USABLE SECURITY HEURISTICS

A major artefact developed in this thesis is the usable security heuristics to guide the design, development, and evaluation of usable security in MFS. The rigorous approach adopted enabled the development of these heuristics principles from requirements grounded in sociotechnical considerations of MFS from the perspective of ecosystem users. The approach adopted facilitates traceability from heuristics to requirements which is important to ensure the implemented approach addresses the requirement and ensures the usable security needs of end-users and experts.

The process of the development of the usable security heuristics in this thesis commenced with a rigorous requirement analysis approach that saw the development of requirements from issues identified by over 700 end-users of MFS and experts. Most requirements for usable security models proposed in the literature focus on identifying usability characteristics and security characteristics and then fusing them into a requirement for usable security in the domain of study (Feth and Polst 2019). Such requirements are not traceable to real user-related issues and might not guarantee the desired outcomes. This study, however, anchored the development of requirement documentation from issues raised by users during the three problem contextualisation studies carried out as part of this thesis as indicated in Table 9.1 in this chapter. The requirements documentation provides a clear and comprehensive set of requirements for developing usable security for MFS. The document aligns the requirements to the needs and expectations of stakeholders including end-users, developers, and testers, and ensures their perspectives and priorities are considered in a truly human-centred fashion. To the best of our knowledge, this thesis presents the most comprehensive requirement for the development of usable security heuristics for MFS.

The development of usable security heuristics in this thesis was a challenging endeavour for three reasons. First, no single approach exists in developing heuristics. While some heuristics are purely from literature reviews, some refine and categorise existing ones (Ambore et al. 2021a). This thesis adopted an approach that will address the objective of this study. Secondly, for the heuristics to have any benefit in practice, they must address the requirement developed in Chapter Six of this study. As part of the heuristics development process, this thesis ensured the traceability of the heuristics developed and the requirement it addressed as highlighted in Chapter Seven of this thesis. Lastly, the heuristics are meant to address the negative human condition; cybercrime affecting users of MFS. To address this issue, the developed heuristics must be implementable. Throughout the development process, the issue of how best to implement the heuristics was a major consideration.

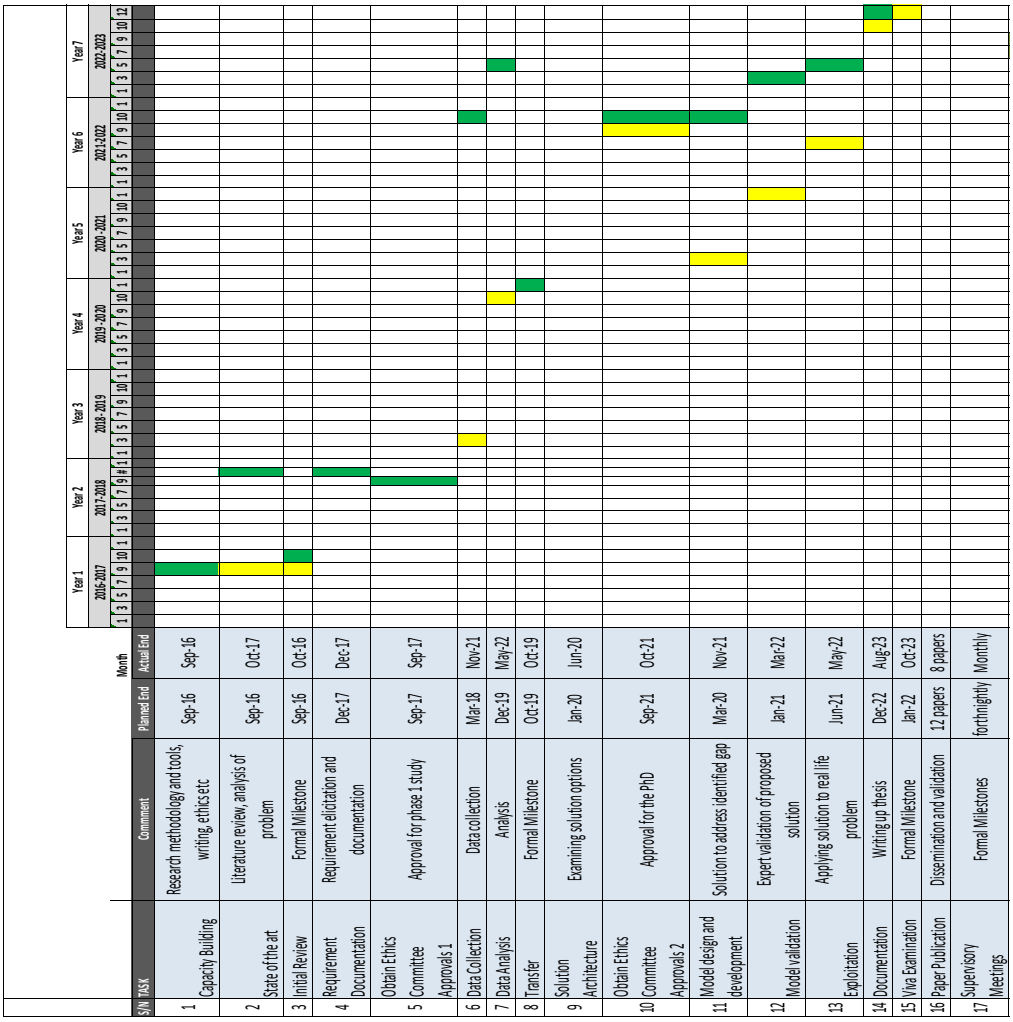
The diverse location and expertise of experts in validating the heuristics ensured various perspectives came into play and made the outcome even more robust. The insights from the experts on how to apply the heuristics for development and evaluation were instrumental in arriving at a final set of heuristics. Their persistent emphasis on the need to ensure implementability ensured the researcher analysed more critically how best to implement some of the heuristics in practice.

To implement the heuristics a case study for live MFS development would be required. This has implications on time and cost. Moreover, to ensure the heuristics work as expected several developments would be required. This thesis adopted an innovative approach to address this problem by leveraging hackathons to implement the heuristics. The process enabled the implementation of the heuristics across several MFS development projects within a time window better suited for the cross-sectional time duration of this thesis, in a way that outcomes and experiences could be easily compared. However, organising a hackathon comes with its challenges. Participants in hackathons normally expect a monetary reward which was a challenge as the researcher was self-funded. However, due to the value the outcome will contribute to knowledge and practice, the choice of running a hackathon was adopted. Partnership with the organising institution also ensured the cost burden was managed. Through the hackathon, the thesis proved that the heuristics can be applied in practice and that it would facilitate the consideration of usable security in the development of MFS. Feedback from hackathon participants also further enriched the heuristics. Furthermore, the black-box testing approach adopted in the second case study ensured that the evaluation of usable security for MFS can be integrated into the user acceptance testing of MFS where technical and non-technical stakeholders can participate.

While the developed guideline addressed a need raised during the problem conceptualisation study in Chapter Five of this thesis on the need for a guide on usable security for MFS developers, to the best of the knowledge of this researcher, no study has been conducted in the past that provided a guideline to integrate usable security for MFS development and evaluation, with an additional focus for the visually impaired user. Also, to the best of the knowledge of the researcher, this is the first time a hackathon will be deployed as a tool to validate the efficacy of a usable security guide. Similarly, this study is ground-breaking in how it ensured usable security evaluation is integrated into user acceptance tests and not treated as a separate effort outside system development.

## 9.5 LESSONS LEARNT

A major lesson learned during this PhD is managing time and disruptions. This PhD was planned to be completed within six years based on the university's guidelines for part-time PhD study. To ensure that the study was completed within this time window, the researcher developed a Gantt chart as shown in Table 9.1.



| S/N | TASK | Comment | Planned End | Actual End |
|---|---|---|---|---|
| 1 | Capacity Building | Research methodologyi and tools, writing, ethics etc | Sep-16 | Sep-16 |
| 2 | State of the art | Literature review, analysis of problem | Sep-16 | Oct-17 |
| 3 | Initial Review | Formal Milestone | Sep-16 | Oct-16 |
| 4 | Requirement Documentation | Requirement elicitation and documentation | Dec-17 | Dec-17 |
| 5 | Obtain Ethics Committee Approvals 1 | Approval for phase 1 study | Sep-17 | Sep-17 |
| 6 | Data Collection | Data collection | Mar-18 | Nov-21 |
| 7 | Data Analysis | Analysis | Dec-19 | May-22 |
| 8 | Transfer | Formal Milestone | Oct-19 | Oct-19 |
| 9 | Solution Architecture | Examining solution options | Jan-20 | Jun-20 |
| 10 | Obtain Ethics Committee Approvals 2 | Approval for the PhD | Sep-21 | Oct-21 |
| 11 | Model design and development | Solution to address identified gap | Mar-20 | Nov-21 |
| 12 | Model validation | Expert validation of proposed solution | Jan-21 | Mar-22 |
| 13 | Exploitation | Applying solution to real life problem | Jun-21 | May-22 |
| 14 | Documentation | Writing up thesis | Dec-22 | Aug-23 |
| 15 | Viva Examination | Formal Milestone | Jan-22 | Oct-23 |
| 16 | Paper Publication | Dissemination and validation | 12 papers | 8 papers |
| 17 | Supervisory Meetings | Formal Milestones | forthnightly | Monthly |

Table 9.1: PhD Gantt Chart

COVID-19 and the associated impact on movement and access to participants had a major impact on the thesis timeline. Moreover, due to the evolving nature of the research study, timelines were revised up to 3 times with the consent of the supervisory team. While better risk analysis would have reduced slippages, certain

variables were outside the control of the researcher. That said, the Gantt chart helped in monitoring progress against planned action.

This study involved all studies conducted as part of this thesis and required some level of expert review for validation. However, due to the restriction of movement by COVID-19, and the impact of assembling participants in a room on cost and time, semi-structured interviews were deployed in some instances as against a focus group. The flexibility in the choice of methodology in line with the reality on the ground was a very important factor in the process of this PhD

The early publication helped obtain feedback. The first conference paper published as part of this PhD was done six months after commencement. The experience was a practical way to improve writing and expose the work of this thesis for early feedback, which was very helpful to the process.

Obtaining information in the financial services space was particularly challenging. This might not be unconnected with the nature of the investigation conducted as part of this thesis. However, key financial services regulators helped open a lot of doors to some institutions. A clear communication of the benefit of the outcome of this thesis helped in obtaining the necessary cooperation, not just for the financial services sector but for other experts as well.

The cost of conducting this research was above what was anticipated by the PhD student. While the university has a provision for some funds to support this type of study, sending money across countries was a hindrance to accessing those funds. As such, the researcher had to seek funds elsewhere. Understanding this before the commencement of the studies would have helped in better planning.

While most of the lessons highlighted above were related to the process of the PhD, others affected data collection. There were several ground-breaking works in usability studies and heuristics evaluation between 1999 and 2012. However, due to the long reference time frame, most of them could not be referenced in this study. Despite this constraint, the rigorous nature of the literature review ensured that all relevant studies were analysed and they addressed the viewpoint of these important papers that did not meet the selection criteria. As such, their exclusion did not affect the findings of the study in any way.

In summary, several challenges were faced during this PhD study, and vital lessons were learned from them, some of which have been implemented.

## 9.6 CHAPTER SUMMARY

This chapter highlighted key findings from the eight studies conducted as part of this thesis. These findings were synthesised and analysed in the context of other studies, based on which the contribution of the study to the body of knowledge and impact in practice were highlighted. Furthermore, lessons learned and their impact on this study were also captured.

# CHAPTER TEN: CONCLUSION AND FUTURE WORK

This thesis addressed the aim of the PhD by designing and developing usable security heuristics to address cybersecurity problems identified through the eyes of key actors in the ecosystem. Leveraging human factor approaches, the nature of the problem in the ecosystems was highlighted and formed an input into developing the requirement for the solution. Insights from MFS user behaviour and its impact on cybersecurity in addition to MFS solution providers' practices also formed an input into the requirement for the development of usable security heuristics for MFS. Through innovative approaches, the artefacts developed as part of this thesis were deployed in addressing real-world problems. The case studies used demonstrated how usable security can be integrated into the MFS development and testing phase for the evaluation of usable security concerns. To the best of our knowledge, the work of this thesis is a novel contribution to addressing usable security problems in mobile financial services.

This chapter highlights how the thesis addresses the research question and objectives. It details the contribution of this thesis to knowledge and revisits the landscape of usable security for mobile financial services from the commencement of this PhD in January 2016 to date, intending to further evaluate the relevance of this PhD in light of recent happenings, so that it can inform areas of future studies. Furthermore, the thesis highlights the direction for future studies based on the findings of this PhD. The chapter is then summarised to emphasise the conclusion of this chapter.

## 10.1 ADDRESSING RESEARCH QUESTIONS AND OBJECTIVES

To address the aim and motivation of this study, six research questions were developed comprising one main question (RQM) and five supporting questions (RQ1, RQ2, RQ3, RQ4, and RQ5). “R” is an acronym for Research, “Q” stands for Question, “M” stands for Main, and the numbers indicate the exact number of each research question. Furthermore, the study was anchored on five main objectives and five supporting objectives. Three of the supporting objectives were linked to achieving objective two of this thesis, while two of the supporting objectives were linked to achieving objective three of this thesis. The research questions and objectives were addressed through eight studies conducted as informed by findings from the literature review. The details of the eight studies highlighting methodologies deployed, sample size, and key findings from the studies conducted were highlighted in section 9.1 of this thesis. As part of the studies conducted, various outcomes and artefacts that address the objectives of the thesis were identified. The thesis outcomes contribute

to addressing the problems identified by the thesis and also reveal further insight into the nature of the problem and the most cost-effective approach to implementing the findings of this study. Figure 10.1 shows how the research questions and objectives were addressed in this thesis.

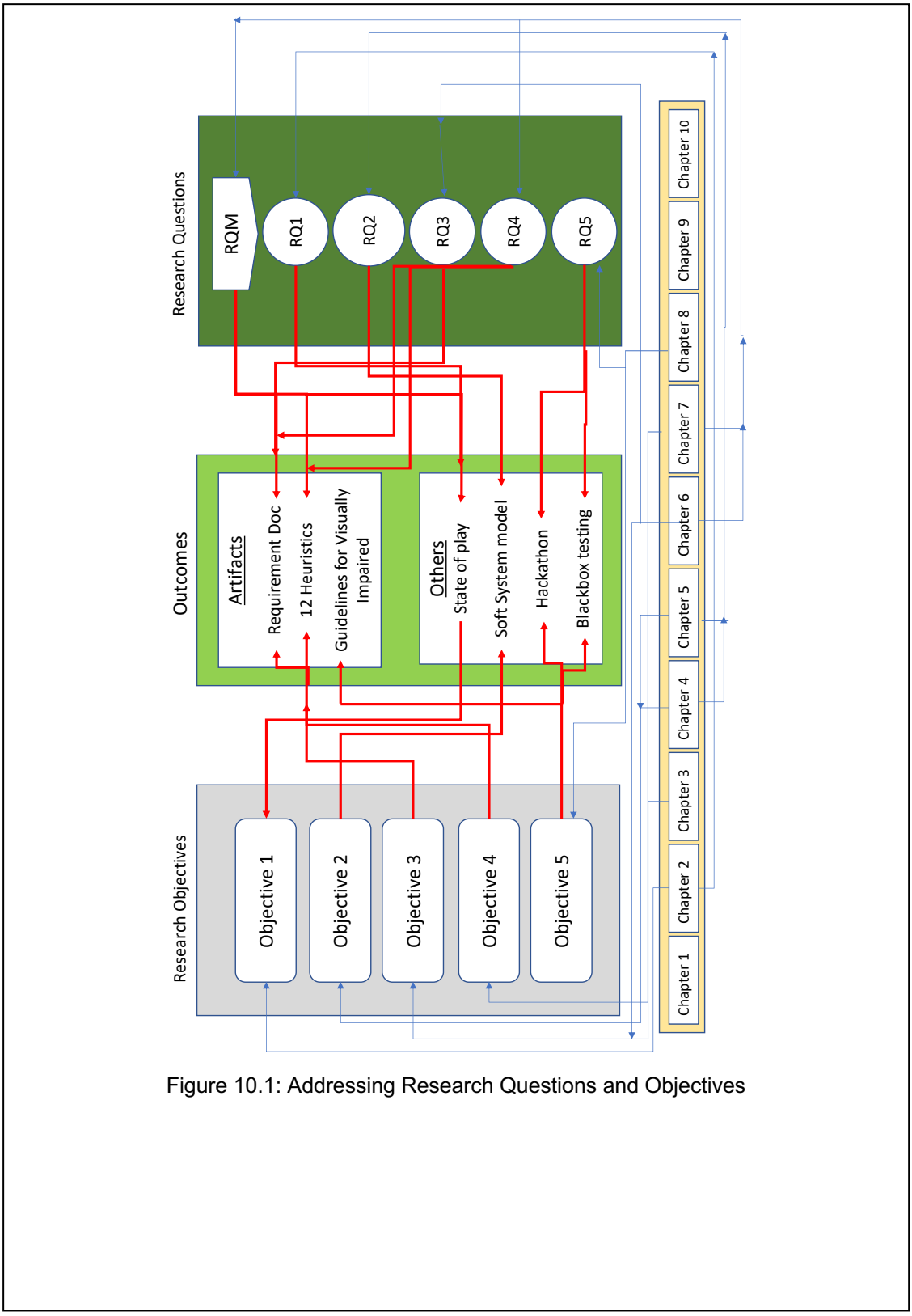



Figure 10.1: Addressing Research Questions and Objectives

Figure 10.1 highlights how the thesis has addressed the main research question of this thesis: *What design principles should inform the integration of usable security features in mobile financial services (MFS) to enhance cybersecurity?*

In addition to the main question, all other research questions and objectives for this thesis were duly addressed. Chapter Two of this study highlighted key findings of critical analysis of literature as it affects cybersecurity in MFS. The chapter addresses RQ1 and Research Objective 1 which were focused on understanding the state of play in cybersecurity for MFS. Also, a major work conducted as part of this thesis was the contextualisation of the problem space, to enable the understanding of cybersecurity in MFS from the perspective of the users in the ecosystem. The findings of the three studies conducted as part of this were published in Chapters Four and Five of this work which both addressed RQ2 and Research Objective 2 of this thesis. Similarly, RQ3 and 4 and Research Objectives 3 and 4 examined how to develop requirements for usable security heuristics, develop the heuristics, and validate the heuristics. Chapters Six and Seven of this thesis address questions raised by RQ3 and 4. It also addresses objectives 3 and 4 of this thesis. The requirement for the solution that addressed RQ3 was developed in Chapter Six based on input from preceding chapters. The development of the usable security heuristics in Chapter Seven addressed RQ4. Objectives 4 and 5 of this thesis were also addressed in Chapters Six and Seven of this thesis. RQ5 and the last research objective of this study were both addressed in Chapters Eight and Nine of this thesis. While Chapter Eight demonstrated how the developed solution can be applied in addressing a real-world problem through a hackathon and black-box testing activities, Chapter Nine provided an additional recommendation for all the artefacts. In addressing the research questions and objectives of this thesis, key outcomes in the form of artefacts and transitional outcomes were developed. The main artefact is the set of usable security heuristics that were developed. The requirement documentation in Chapter Six and the usable security requirements for the visually impaired in Chapter Eight of this thesis are the two other artefacts developed. The soft systems model in Chapter Four, and the hackathon and UAT in Chapter Eight, are part of the transitional outcomes from the thesis.

This section has highlighted how the thesis addressed all the research questions and objectives of this PhD study. The lessons learned from the process have been documented in Chapter Nine of this thesis.

## 10.2 REVIEWING CONTRIBUTION TO KNOWLEDGE

This study highlights key contributions to the body of knowledge, as highlighted in the abstract and section 1.5 of this thesis.

C1: **Provide an understanding of socio-technical factors in mobile financial services and their impact on usable security**

This study adopted a sociotechnical approach to explore usable security problems in the mobile financial services domain. It has been argued that usable security should have a consideration for how various stakeholders in the ecosystem engage with security features within a sociotechnical context rather than isolating user-related issues from technical issues (Abu-Salma et al. 2017). Moreover, it was opined that the importance of sociotechnical factors has often been neglected in usable security, making it difficult to implement a solution that will address stakeholder-related concerns (Krombholz et al. 2019). This thesis addressed this gap by ensuring usable security in MFS while considering the concerns of stakeholders in the ecosystem. By providing an understanding of each group's perspectives, this thesis adds depth to the literature, highlighting how MFS stakeholders' perspectives of usable security influence their behaviours and practices. Also, this PhD thesis addresses a critical gap by providing a strong foundation for future usable security research to adopt a sociotechnical approach in developing solutions that have consideration for diverse stakeholder worldviews. The details of this contribution have been discussed in Chapter Four of this PhD thesis. It has also been published in one journal and two conferences, highlighted in section 1.7 of this PhD thesis.

C2: **Provide empirical evidence of the impact of user behaviour and DevOps practices on usable security in MFS**:

This contribution focused on providing an understanding of user behaviours and supply-side practices that impact usable security in MFS. The complex relationship between user interaction with mobile security measures and the practices of DevOps players necessitates a thorough investigation to enhance usable security for MFS. Furthermore, this contribution addresses how end-users and DevOps players interact with security mechanisms in MFS, including their motivations, behaviours, challenges, and compliance tendencies.

The unique contribution lies in the combination of user behaviour analysis with DevOps practices, providing a comprehensive perspective on the ecosystem of MFS security, closing the gap on the need for a usable security measure that takes into cognisance user behaviour, as highlighted by (Lennartsson et al. 2021; Alturki and

Gay 2019). The study underscores the need to consider end-user perspectives and systems implementation (Lessa and Etoribussi 2023). Through this contribution, this study identifies usable security considerations for MFS from the standpoint of ecosystem players.

This contribution provides a holistic view that integrates both the user and supply-side perspectives of usable security in MFS. Addressing these aspects adds to a nuanced understanding that bridges gaps identified in other studies, such as those focusing solely on user behaviour or system design. This comprehensive approach makes this a valuable resource for developing MFS systems that are both secure and user-friendly, setting a precedent for future research and implementation in the field. The details of this contribution have been highlighted in Chapter Five of this PhD thesis and published in the proceedings of the British Human-Computer -Interaction (HCI) conference as highlighted in section 1.7 of this PhD thesis.

C3: **Develop and validate usable security heuristics for MFS**

This contribution centres on the development and validation of usable security heuristics specifically tailored for MFS. It addresses a significant need in the field of mobile finance and cybersecurity. This contribution addresses a gap in current research and practice that often struggles to address the trade-off between usability and security, as highlighted in section 2.6 of this study. The heuristics would facilitate evaluations that ensure security features are accessible and intuitive and do not overly burden the end-user. The validation of these heuristics was a crucial aspect of this work, lending empirical support and credibility to their applicability. This validation ensures that the heuristics are not only theoretically sound but also practical and effective in real-world scenarios, making them reliable input for designers and developers of MFS when compared to other purely theoretical models or models that treat usability and security in isolation (Feth and Polst 2019). Developers of MFS now have a validated set of heuristics to guide their work, ensuring that security is not compromised for usability and vice versa. This can lead to better-designed systems that reduce user error and enhance usable security in MFS.

The need for an approach that caters to both usability and security is well-documented in academic and industry circles, as highlighted in Chapter Two of this study. This contribution directly addresses this need in the context of MFS. It builds usable security requirements from literature and stakeholders in the ecosystem. By providing a set of heuristics that are validated and practical, this contribution supports better development practices that can improve usable security in MFS. The details of

this contribution have been highlighted in Chapters Six and Seven of this PhD thesis and have been published as highlighted in section 1.7 of this thesis.

C4: **Demonstrate real-world application of heuristics through hackathon and black-box testing**:

This study provides a structured way to incorporate previously developed usable security heuristics into the design process of MFS. It does this in a test-and-learn environment through a hackathon, exploring participants' creativity. This integration facilitates a cohesive method where designers and developers can apply these principles during the creation phase and also use them to evaluate existing systems for potential usability and security improvements. This study addresses the lack of an overarching approach to integrating usable security heuristics in MFS by unifying the developed heuristics into a comprehensive system applicable throughout the design process (Realpe-Muñoz et al. 2017). The uniqueness of this contribution lies in its ability to operationalise usable security heuristics within the context of MFS. As the mobile financial landscape continues to evolve. It addresses critical gaps in the current literature by providing a structured, validated approach that aligns with user-centric design principles and requirements grounded in literature and feedback from users and developers of MFS.

The tool developed embodies principles of usable security by providing features that guide users through secure practices without added complexity, help developers integrate these principles seamlessly into their design processes, and assist evaluators in assessing the usability-security balance in existing systems. This comprehensive approach ensures that all major stakeholders involved in MFS benefit from a structured and unified methodology. The tool addresses the challenge users may encounter with security mechanisms that could hinder their interaction with the system; it would also assist developers who might struggle to implement security features. While the need for such tools has been identified, none exist to address the need of MFS developers (Galanská 2017).

The significance of this contribution lies in its potential to tackle a usable security problem in MFS that affects multiple stakeholders. The details of this contribution have been highlighted in Chapter Eight of this study.

## 10.3 EVOLUTION OF RESEARCH AREA: 2016 TO 2024

This part-time PhD thesis commenced in 2016. As part of the effort of the researcher to ensure the research outcome remains relevant in light of the ever-evolving cybersecurity landscape for MFS, the researcher conducted a periodic review of the landscape. This section highlights changes in the landscape from the inception of this PhD study till date and its impact on the outcome of this thesis.

Between the years 2016 and 2018, there was a research focus on addressing cybersecurity concerns through addressing usable security for developers. For instance, while highlighting the gap between theoretical solutions for security and actual vulnerability, adopting a human factor approach was recommended for addressing usable security problems. The author proposed the development of an approach that would improve usable security for the developers (Acar et al. 2016). The need to leverage a human-centred approach to address usable security concerns for developers was an active research topic during this review period (Green and Smith 2016; Mindermann 2016; Smith 2016; Feth et al. 2017; Iacono and Gorski 2017; Realpe-Muñoz et al. 2017). Researchers still retain an active interest in addressing usable security concerns for developers to date as demonstrated by activity in the research landscape from 2019 to date, making it a very important research gap (Ambore et al. 2021a; Chowdhury et al. 2021; Gutfleisch et al. 2022; Nadeem et al. 2022; Gorski et al. 2022).

Various studies related to cybersecurity in mobile financial services were also conducted during the period under review. Some of the studies focused on addressing the problem from a country-based perspective. For instance, a survey of 414 MFS users in Thailand was conducted to understand the relationship between cybersecurity awareness and other variables that affect MFS security (Limna et al. 2023). Similarly, a study focused on addressing the MFS adoption barrier from a merchant viewpoint was conducted in Malaysia. While the exploratory study did not propose a solution to addressing cybersecurity issues, it nonetheless identified this as a key barrier to adoption (Moghavvemi et al. 2021). In the same vein, a study of 191 MFS users 55 years old and above highlights the impact of the perception of cybersecurity risks and the adoption of MFS amongst the elderly in the UK (Hanif and Lallie 2021).

In addition to the areas highlighted above, research on how to address cybersecurity in MFS has been examined during the time under review, seeking to address concerns related to human factors and technology-related concerns.

While the effort to address cybersecurity concerns in MFS has remained an active research interest, the problem still exists. The screenshot from Figure 10.2 below shows some issues from a current cybersecurity-related issue with some mobile applications which can be addressed by the application of the 12 usable security heuristics. The first two images show customer feedback arising due to issues related to the lack of implementation of *integrity,* one of the 12 usable security heuristics in Chapter Seven of this thesis. The third image shows issues that arise due to a lack of adherence to the principle of the *authenticity* usable security heuristics in Chapter Seven. Some part of the image has been greyed out to protect the identity of the financial institution and the user.

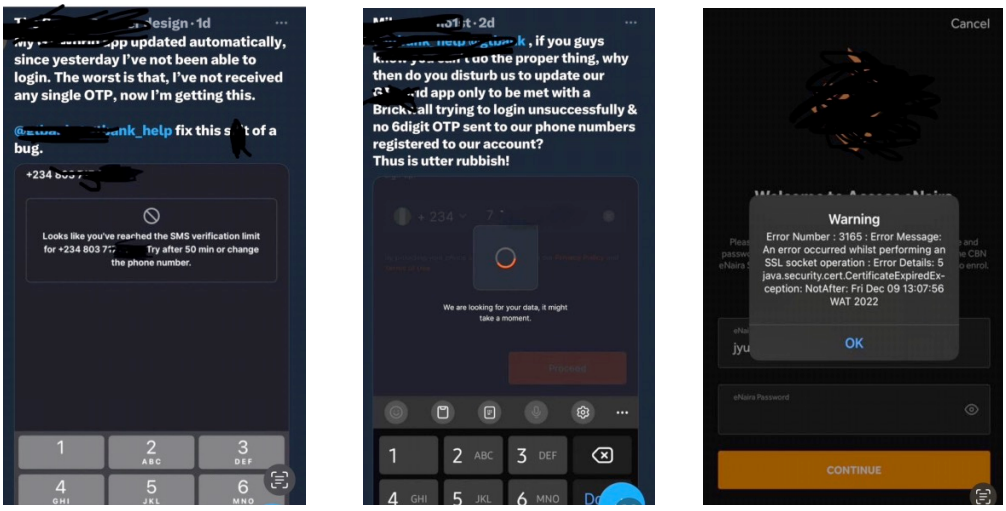



Figure 10.2: Usable Security Issues Still Exist in MFS

In the preceding paragraphs in this section, it has been demonstrated that despite the effort put in place by other researchers, the findings of this PhD study remain relevant in addressing usable security concerns in MFS in light of current realities.

## 10.4 ADDRESSING STUDY MOTIVATION

A major benefit of addressing the cybersecurity challenge in MFS is to improve trust and adoption in the way it will address a negative human condition where over 1.2 billion people globally cannot live up to their potential because they lack access to secure financial services. The work and outcome of this thesis have presented a tool for auditors to examine the suitability of MFS for use in terms of usable security. Furthermore, user involvement in the evaluation process will facilitate better conversations and agreement between the end-users and supply-side actors regarding the measurement of satisfaction rating on usable security readiness of MFS, further boosting trust. The integration of the heuristics in the application development process will enable developers to increase focus on cybersecurity

concerns that deter users from adopting the system. Based on feedback from developers during the hackathon exercise conducted and reported in Chapter Eight of this thesis, the heuristics also serve as a tool for cybersecurity awareness for solution developers.

The approach to address inclusivity in cybersecurity by considering user segments like the visually impaired and the focus on various types of users through the *proportional* heuristics principles also facilitates adoption and trust in MFS.

## 10.5 LIMITATION

This PhD thesis has contributed to the existing body of knowledge in theory and practice as enumerated in section 10.2. However, due to the time limit of the studies and other constraints, the study has some limitations that can be examined for possible future studies.

This PhD thesis draws its findings from the worldview of stakeholders within a specific geographic context. As such, it might be limited in scope and might not fully address usable security challenges in MFS in other jurisdictions. While the validation of heuristics and DevOps semi-structured interviews draw from experts from several countries, the end-user data may reflect country-specific user behaviours, practices, and environment-specific constraints.

Due to the cross-functional nature of this study and the methodology adopted, surveys were deployed for end-user data collection. While insight from the survey provided important insight into specific MFS usable security user behaviours, the self-reporting nature of surveys might lead to bias. Furthermore, users may not accurately report certain behaviours due to a limited understanding of security and usability terms. Also, supply-side actors like bank chief information officers (CIOs) who participated in the semi-structured interview might not be comfortable sharing information useful to the study due to the fear of unwittingly sharing company trade secrets or making the company's process or product look vulnerable.

While this PhD thesis adopted a robust theoretical approach in developing usable security heuristics that incorporated user perspectives based on findings from literature and end-user surveys, users were not involved in the validation of the heuristics, which was mostly expert-driven as the cost and time required are above the time limit and budget of this PhD. Also, the experimental design approach adopted enabled the demonstration of how usable security heuristics can be integrated into MFS development. While the thesis argued that existing heuristics were not suitable

for addressing usable security in the MFS context based on the reasons articulated in Chapter Seven of this study, this thesis did not compare the new heuristics side with the existing heuristics in a practical demonstration due to time constraints.

Usable security challenges from emerging areas like AI-generated phishing attacks and malware and the impact of emerging technologies like blockchain and decentralised financing on MFS development practice were not in-scope for this study. Similarly, a detailed study of the impact of privacy on usable security for MFS was also not in-scope for this study.

Furthermore, while conducting hackathons and black-box testing provided useful insight, this study did not explore practical observation of MFS by users over time to observe certain behaviours and practices, as it would require time and resources beyond this PhD limit.

The nature of this PhD involved some resource-intensive processes like conducting a hackathon, which led to huge additional expenses not planned for this study. Furthermore, COVID-19 affected data collection planning as semi-structured interviews, in some instances, replaced focus group meetings.

Addressing these limitations would strengthen the findings and recommendations of this PhD and provide additional insight into how it can be applied.

## 10.6 FUTURE WORK

This PhD thesis provides a robust foundation for understanding usable security problems in MFS and how to address them. However, the findings of the PhD study can be further strengthened through future studies examining certain limitations of this PhD.

A longitudinal study to evaluate the usable security heuristics in a real-world environment will provide an opportunity to leverage observational data collection approaches to complement survey data by providing new insight from participants, mitigating the risk of self-reporting data and biases from surveys and interviews. An observational data collection approach would enable real-time tracking of user behaviour under various experimental conditions. It will also facilitate the comparison of the new heuristics with existing ones in a real-world scenario. Also, future efforts would benefit from conducting end-user studies across various countries to test the generalisabilty of the findings of this PhD study. This might reveal how cultural biases, country-level regulations, social norms, and practices affect usable security in MFS. The findings of such a study would make the heuristics more globally applicable.

Furthermore, future studies should consider end-user involvement in the heuristic validation process, which can further serve as a validation of MFS usable security end-user behaviour.

Heuristics developed were applied in a hackathon, which largely leveraged Agile software development methodology, the predominant methodology for MFS development. Future studies will seek to apply the heuristics in a waterfall development methodology. Chapter Two of this thesis examined zero trust, which encourages the continuous verification of trust entities. Future studies would benefit from the cognitive workload of this model on usable security in MFS.

In addressing usable security challenges for developers, it was important to ensure that the heuristics provided do not add to developers' workload, introducing a secondary usability problem. Future studies would examine the impact of adding usable security heuristics for MFS development on the cognitive workload of developers. The startup ecosystem would benefit from applying the usable security heuristics to facilitate the development of secure solutions in the fintech space, and future work could explore integrating the process into an industry and a regulatory sandbox environment. Furthermore, Central Bank Digital Currencies (CBDC) are gaining prominence, with live implementations in countries like Nigeria. One of the characteristics of CBDC that facilitates financial inclusion is smart contracts to programmable money. Future studies would seek to leverage the heuristics to evaluate usable security in smart contracts. User acceptance testing (UAT) is the last test conducted before deployment. The black-box test conducted as part of this thesis was user acceptance testing. Future studies would investigate how the heuristics can be deployed in white-box testing for unit and system tests. This would enable the developers to fix any gap and reduce the effort, time, and cost needed in conducting UAT. Other areas of future research focus are the extension of the heuristics to address the need for hearing impairment and how to develop capacity-building programmes on usable security for MFS developers.

## 10.7 CHAPTER SUMMARY

This chapter highlighted how the thesis addressed all the objectives and research questions of this study. Taking a chapter-by-chapter approach, the chapter showed how each chapter contributes to addressing the research objectives and major outcomes of this thesis. Furthermore, the chapter highlighted the contribution of the thesis to the body of knowledge and practice. Similarly, the chapter demonstrated how the research addressed the motivation for this PhD. Examining the research

landscape since the commencement of the PhD study, the relevance of the findings of this study in light of current realities was established. Also, the chapter presented the limitations of the thesis and the process undertaken to conduct the work of the thesis. The chapter concluded by providing a direction for future work.

# REFERENCE


Abdinoor, A. and Mbamba, U.O., 2017. Factors influencing consumers' adoption of mobile financial services in Tanzania. *Cogent Business & Management*, 4(1), p.1392273.

Abu-Salma, R., Sasse, M.A., Bonneau, J., Danilova, A., Naiakshina, A. and Smith, M., 2017, May. Obstacles to the adoption of secure communication tools. In 2017 *IEEE Symposium on Security and Privacy* (SP) (pp. 137-153). IEEE.

Acar, Y., Backes, M., Fahl, S., Garfinkel, S., Kim, D., Mazurek, M. L., and Stransky, C., 2017, May. Comparing the usability of cryptographic APIs. In 2017 *IEEE Symposium on Security and Privacy* (SP) (pp. 154-171). IEEE.

Acar, Y., Fahl, S. and Mazurek, M.L., 2016. You are not your developer, either: A research agenda for usable security and privacy research beyond end-users. 2016 *IEEE Cybersecurity Development* (SecDev), pp.3-8.

Agarwal, S. and Zhang, J., 2020. FinTech, lending and payment innovation: A review. *Asia-Pacific Journal of Financial Studies*, 49(3), pp.353-367.

Agur, I., Peria, S. M., & Rochon, C., 2020. Digital financial services and the pandemic: Opportunities and risks for emerging and developing economies. *International Monetary Fund Special Series on COVID-19*, Transactions, 1, 2-1.

Agrawal, A., Alenezi, M., Khan, S.A., Kumar, R., and Khan, R.A., 2022. Multi-level fuzzy system for usable-security assessment. *Journal of King Saud University-Computer and Information Sciences*, 34(3), pp.657-665.

Ahmad, A. H., Green, C., & Jiang, F., 2020. Mobile money, financial inclusion, and development: A review with reference to African experience. *Journal of Economic Surveys*, 34(4), 753-792.

Ahmed, N., Kulsum, U., Azad, I.B., Momtaz, A.Z., Haque, M.E. and Rahman, M.S., 2017, December. Cybersecurity awareness survey: An analysis from Bangladesh perspective. *In 2017 IEEE Region 10 Humanitarian Technology Conference* (R10-HTC) (pp. 788-791). IEEE.

Ajibola, A.S. and Goosen, L., 2017. Development of heuristics for usability evaluation of m-commerce applications. *In Proceedings of the South African Institute of Computer Scientists and Information Technologists* (pp. 1-10).

Alderman, J., 2021. Auditor Litigation Risk: A Review of Past Perspectives, Recent Developments, and Emerging Issues. *Journal of Forensic and Investigative Accounting*, 13(1).

Al-Dmour, R., Dawood, E. A. H., Al-Dmour, H., & Masa'deh, R. E., 2020. The effect of customer lifestyle patterns on the use of mobile banking applications in Jordan. *International Journal of Electronic Marketing and Retailing*, 11(3), 239-258.

Alarifi, A., Alsaleh, M., & Alomar, N., 2017. A model for evaluating the security and usability of e-banking platforms. *Computing*, *99*, 519-535.

Algarni, A., Xu, Y. and Chan, T., 2017. An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. *European Journal of Information Systems*, 26(6), pp.661-687.

Alt, F. and von Zezschwitz, E., 2019. Emerging trends in usable security and privacy. *i-com*, 18(3), pp.189-195.

Alturki, R. and Gay, V., 2019. Usability attributes for mobile applications: a systematic review. *Recent trends and advances in wireless and IoT-enabled networks*, pp.53-62.

Ambore, S., Dogan, H. and Apeh, E.T., 2021a. Development of Usable Security Heuristics for Fintech. *In 34th British HCI Conference* 34 (pp. 121-132)

Ambore, S., Breban, A., Apeh, E., & Dogan, H. 2021b. Evaluating Security and Accessibility Trade-off for Visually Impaired Mobile Financial Services Users. *In 34th British HCI Workshop and Doctoral Consortium* (pp. 1-5). BCS Learning & Development.

Ambore, S., Richardson, C., Dogan, H., Apeh, E. and Osselton, D., 2017. A resilient cybersecurity framework for Mobile Financial Services (MFS). *Journal of Cyber Security Technology*, 1(3-4), pp.202-224.

Android, 2023a. Design for Safety | App quality | *Android Developers*. [Online]. Available from: https://developer.android.com/quality/privacy-and-security [Accessed 07 Jul 2023]

Android, 2023b. Advanced and proactive Android device security | *Android*. [Online]. Available from: https://www.android.com/safety/security/ [Accessed 07 Jul 2023]

Apple, 2023. Security Overview - *Apple Developer*. [Online] Available from: https://developer.apple.com/security/ [Accessed 07 Jul 2023]

Asatryan, D. June 2017, Security and Lack of Trust Stall Mobile Payment Adoption. *Bank innovation* [Online]. Available from : https://bankinnovation.net/2017/06/security-and-lack-of-trust-stall-mobilepayment-adoption/ [Accessed 05 May 2018]

Balamurugan, K., Sudalaimuthu.T, Sherlin Solomi.V , 2023, February. An Analysis of Various Cyber Threat Modeling. *In 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)* (pp. 426-429). IEEE.

Banks, A.P., Gamblin, D.M. and Hutchinson, H., 2020. Training fast and frugal heuristics in military decision-making. *Applied Cognitive Psychology*, *34*(3), pp.699-709.

Barclays, 2018, what is Paym? *Barclays bank* [online]. Available from: https://www.barclays.co.uk/ways-tobank/mobile-banking-services/what-is-paym/ [Accessed 23 May 2018]

Bashir, M.S. and Farooq, A., 2019. EUHSA: Extending usability heuristics for smartphone application. *IEEE Access*, *7*, pp.100838-100859.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A. and Rossi, M., 2018. Design science research contributions: Finding a balance between artefact and theory. *Journal of the Association for Information Systems*, 19(5), p.3.

Beck, T., 2020. Fintech and financial inclusion: Opportunities and pitfalls (No. 1165). *ADBI Working Paper Series*.

Benson, V., McAlaney, J. and Frumkin, L.A., 2019. Emerging threats for the human element and countermeasures in the current cyber security landscape. *In Cyberlaw, privacy, and security: Concepts, methodologies, tools, and applications* (pp. 1264-1269). IGI Global.

BIS, 2023, Project Polaris, *A handbook for offline payment with CBDC, Bank of International Settlement (BIS) Innovation hub* pp. 30-32.

Bradford, T., 2020. Neobanks: Banks by any other name. *Federal Reserve Bank of Kansas City, Payments System Research Briefing*, August, 12, pp.1-6.

Braun, V. and Clarke, V., 2019. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise, and health*, 11(4), pp.589-597.

Braun, V. and Clarke, V., 2021. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, *18*(3), pp.328-352.

Chatterjee, S., Chaudhuri, R., Vrontis, D. and Hussain, Z., 2023. Usage of smartphone for financial transactions: from the consumer privacy perspective. *Journal of Consumer Marketing*, 40(2), pp.193-208.

Checkland, P. and Poulter, J., 2020. Soft systems methodology. *Systems approaches to making change: A practical guide*, The Open University, pp.191-242. Springer International Publishing

Chen, S., Fan, L., Meng, G., Su, T., Xue, M., Xue, Y., Liu, Y. and Xu, L., 2020, October. An empirical assessment of security risks of global android banking apps. In *2020 IEEE/ACM 42nd International Conference on Software Engineering (ICSE)* (pp. 1310-1322). IEEE.

Choi, H., Park, J., Kim, J., & Jung, Y., 2020. Consumer preferences of attributes of mobile payment services in South Korea. *Telematics and Informatics*, 51, 101397.

Chowdhury, P.D., Hallett, J., Patnaik, N., Tahaei, M. and Rashid, A., 2021, October. Developers are neither enemies nor users: they are collaborators. *In 2021 IEEE Secure Development Conference (SecDev)* (pp. 47-55). IEEE.

Cornish, F., Breton, N., Moreno-Tabarez, U., Delgado, J., Rua, M., de-Graft Aikins, A. and Hodgetts, D., 2023. Participatory action research. *Nature Reviews Methods Primers*, *3*(1), p.34.

David-West, O., Iheanachor, N., & Umukoro, I., 2020. Sustainable business models for the creation of mobile financial services in Nigeria. *Journal of Innovation & Knowledge*, 5(2), 105-116.

Das, S., Dingman, A., & Camp, L. J., 2018. Why Johnny doesn't use two-factor a two-phase usability study of the FIDO U2F security key. In Financial Cryptography and Data Security: *22nd International Conference, FC 2018, Nieuwpoort, Curaçao,*

*February 26–March 2, 2018, Revised Selected Paper*s 22 (pp. 160-179). Springer Berlin Heidelberg.

Das, S., Russo, G., Dingman, A.C., Dev, J., Kenny, O. and Camp, L.J., 2018, December. A qualitative study on usability and acceptability of Yubico security key. In *Proceedings of the 7th workshop on socio-technical aspects in security and trust* (pp. 28-39).

Deery M. 2021, What is a Hackathon? *A 3-Step Beginner's Guide*. [Online]. Available from:https://careerfoundry.com/en/blog/web-development/what-is-a-hackathon/ [Accessed 02 Jan 2023]

Demirgüç-Kunt, A., Klapper, L., Singer, D. and Ansar, S., 2022. Financial inclusion, digital payments, and resilience in the age of COVID-19. *The Global Findex Database 2021*. World Bank Publications.

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F., 2021. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, 54(8), pp.1-35.

Dzidzah, E., Kwateng, K. O., and Asante, B. K., 2020. Security behaviour of mobile financial service users. *Information & Computer Security*.

EdmonRamin, 2017, Apple iOS 10.3 beta gets pushy with iCloud two-factor. *Bank innovation* [Online]. Available From: https://bankinnovation.net/2017/06/security-and-lack-of-trust-stall-mobile-paymentadoption/ [Accessed 05 May 2017]

Elazar, 2023, What is User Acceptance Testing (UAT)? | Full Process Explained, *Panaya*, Available From: https://www.panaya.com/blog/testing/what-is-uat-testing/ [Accessed 02 Jul 2023]

Erich, F.M., Amrit, C. and Daneva, M., 2017. A qualitative study of DevOps usage in practice. *Journal of software: Evolution and Process*, *29*(6), p.e1885.

Eskandari, S., Clark, J., Barrera, D., &Stobert, E., 2018. A first look at the usability of bitcoin key management. *arXiv preprint arXiv:*1802.04351.

Evered, D. and Roger, I.S., 2022. An assessment of the scientific merits of action research. *An assessment of the scientific merits of action research*, pp.135-161.

Fanelle, V., Karimi, S., Shah, A., Subramanian, B., & Das, S., 2020. Blind and human: Exploring more usable audio {CAPTCHA} designs. *In Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 111-125).

Fernandes, C., Borges, M. R., & Caiado, J., 2021. The contribution of digital financial services to financial inclusion in Mozambique: an ARDL model approach. Applied Economics, 53(3), 400-409.

Fassl, M., Gröber, L.T. and Krombholz, K., 2021, May. Exploring user-centred security design for usable authentication ceremonies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

Ferrag, M.A., Maglaras, L., Derhab, A. and Janicke, H., 2020. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, *73*, pp.317-348.

Feth, D., Maier, A. and Polst, S., 2017. A user-centred model for usable security and privacy. In Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of *HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings* 5 (pp. 74-89). Springer International Publishing.

Feth, D., & Polst, S. 2019. Heuristics and models for evaluating the usability of security measures. In *Proceedings of Mensch und Computer 2019* (pp. 275-285).

FLPFI, 2019, The logic behind branchless banking, *Fletcher, Leadership Program for Financial Inclusion lecture materia*l. Fletcher Business School Tuft University, MA.

Focardi, R., Luccio, F.L. and Wahsheh, H.A., 2019. Usable security for QR code. *Journal of Information Security and Applications*, 48, p.102369.

FSI, 2021, Hackathon Advert. *Cybersecurity Innovation Challenge* [Online]. Available From: https://fsi.ng/innovation-challenge/2/cybersecurity_innovation_challenge [Assessed 30 Nov 2021]

FSB, 2018, Bank Branch Closures. *Finance and the economy* [Online]. Available From: https://www.fsb.org.uk/standing-upfor-you/policy-issues/finance-and-the-economy/bank-branch-closures. [Assessed 17 Feb 2018]

Flus, M. and Hurst, A., 2021. Design at hackathons: new opportunities for design research. *Design Science*, *7*, p.e4.

Gaehtgens, F., Allan ,A., Zlotogorski, M., Buytendijk,F., 2017, Definition: Digital Trust. *Gartner research*, Published: 24 May 2017 ID: G00329409.

Galli, T., Chiclana, F. and Siewe, F., 2020. Software product quality models, developments, trends, and evaluation. *SN Computer Science*, 1, pp.1-24.

Galanská, K., 2017. Usability of Usable Security Guidelines from IT Professional Point of View. *Excel@FIT 2021*, Faculty of Information Technology, Brno University of Technology

Garcia-Retamero, R. and Cokely, E.T., 2017. Designing visual aids that promote risk literacy: A systematic review of health research and evidence-based design heuristics. *Human factors*, *59*(4), pp.582-627.

Gbongli, K., 2022. Understanding Mobile Financial Services Adoption through a Systematic Review of the Technology Acceptance Model. *Open Journal of Business and Management, 10*(5), pp.2389-2404.

Ghelani, D., Hua, T.K. and Koduru, S.K.R., 2022. Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints*.

Grobler, M., Gaire, R. and Nepal, S., 2021. User, usage and usability: Redefining human centric cyber security. *Frontiers in big Data*, *4*, p.583723.

Gobov, D., and Huchenko, I., 2020, September. Requirement elicitation techniques for software projects in Ukrainian it: an exploratory study. *In 2020 15th Conference on Computer Science and Information Systems (FedCSIS)* (pp. 673-681). IEEE.

Gomez, M.A. and Villar, E.B., 2018. Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance*, *6*(2), pp.61-72.

Gong, X., Zhang, K. Z., Chen, C., Cheung, C. M., & Lee, M. K., 2020. What drives trust transfer from web to mobile payment services? The dual effects of perceived entitativity. *Information & Management, 57*(7), 103250.

Gonzalez-Holland, E., Whitmer, D., Moralez, L. and Mouloua, M., 2017, September. Examination of the use of Nielsen's 10 usability heuristics & outlooks for the future. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 61, No. 1, pp. 1472-1475). Sage CA: Los Angeles, CA: SAGE Publications.

Gorod, A., Nguyen, T. and Hallo, L., 2017, April. Systems engineering decision-making: Optimizing and/or satisficing? *In 2017 Annual IEEE International Systems Conference (SysCon)* (pp. 1-6). IEEE.

Gordieiev, O., Kharchenko, V. and Leontiiev, K., 2019. Usability, security and safety interaction: profile and metrics based analysis. In *Contemporary Complex Systems and Their Dependability: Proceedings of the Thirteenth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, July 2-6, 2018, Brunów, Poland 13* (pp. 238-247). Springer International Publishing.

Gorski, P.L., Iacono, L.L. and Smith, M., 2022. Eight Lightweight Usable Security Principles for Developers. *IEEE Security & Privacy, 21*(1), pp.20-26.

Green, M., & Smith, M., 2016. Developers are not the enemy: The need for usable security APIs. *IEEE Security & Privacy, 14*(5), 40-46.

Guild, J., 2017. Fintech and the Future of Finance. *Asian Journal of Public Affairs*, pp.17-20.

Gupta, S. and Dhingra, S., 2022. Modeling the key factors influencing the adoption of mobile financial services: An interpretive structural modeling approach. *Journal of Financial Services Marketing, 27*(2), pp.96-110.

Gupta, S. and Dhingra, S., 2022. Past, present and future of mobile financial services: A critique, review and future agenda. *International Journal of Consumer Studies*, *46*(6), pp.2104-2127.

Gutfleisch, M., Klemmer, J.H., Busch, N., Acar, Y., Sasse, M.A. and Fahl, S., 2022, May. How does usable security (not) end up in software products? results from a qualitative interview study. *In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 893-910)*. IEEE.

Hadlington, L., 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7).

Halunen, K., Häikiö, J., &Vallivaara, V., 2017. Evaluation of user authentication methods in the gadget-free world. *Pervasive and Mobile Computing, 40*, 220-241.

Hanif, Y. and Lallie, H.S., 2021. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using

modified UTAUT and MTAM-with perceived cyber security, risk, and trust. *Technology in Society*, 67, p.101693

He, Y., Huang, D., Chen, L., Ni, Y. and Ma, X., 2022. A survey on zero trust architecture: Challenges and future trends. *Wireless Communications and Mobile Computing*, *2022*(1), p.6476274.

Himel, M.T.A., Ashraf, S., Bappy, T.A., Abir, M.T., Morshed, M.K. and Hossain, M.N., 2021. Users' attitude and intention to use mobile financial services in Bangladesh: an empirical study. *South Asian Journal of Marketing*, 2(1), pp.72-96.

Ho, J. C., Wu, C. G., Lee, C. S., & Pham, T. T. T., 2020. Factors affecting the behavioural intention to adopt mobile banking: *An international comparison. Technology in Society*, 63, 101360.

Hof, H. J.,2015. User-centric IT security-how to design usable security mechanisms*. arXiv preprint arXiv*:1506.07167.

Humbani, M., & Wiese, M., 2018. A cashless society for all: Determining consumers' readiness to adopt mobile payment services. *Journal of African Business*, 19(3), 409-429.

Iacono, L.L. and Gorski, P.L., 2017. I do and i understand. not yet true for security apis. so sad. *In European Workshop on Usable Security* (Vol. 4).

Ibrahim, T.M., Alarood, A.A., Chiroma, H., Al-garadi, M.A., Rana, N., Muhammad, A.N., Abubakar, A., Haruna, K. and Gabralla, L.A., 2019. Recent advances in mobile touch screen security authentication methods: A systematic literature review*. Computers & Security, 85*, pp.1-24.

I2i, 2017. Banking on trust: Building trust to drive usage of financial services. *Insight to Impact (I2i),* [online]. Available from: https://i2ifacility.org/insights/blog/banking-on-trust-building-trust-to-drive-usage-of-financial-services/. [Accessed 01 Jan 2023].

Jacobs, D., & McDaniel, T., 2022, June. A survey of user experience in usable security and privacy research. *In International Conference on Human-Computer Interaction* (pp. 154-172). Cham: Springer International Publishing.

Jain, M., Diwakar, N. and Swaminathan, M., 2021, May. Smartphone usage by expert blind users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-15).

Janssens, G., van Moorst, L., Kusters, R. and Martin, H., 2018. An expert-based taxonomy of ERP implementation activities. *Journal of Computer Information Systems*.

Johnson, V.L., Kiser, A., Washington, R. and Torres, R., 2018. Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behaviour, 79*, pp.111-122.

Joo, J. and Han, Y., 2021. An evidence of distributed trust in blockchain-based sustainable food supply chain. *Sustainability, 13*(19), p.10980.

Kadena, E. and Gupi, M., 2021. Human Factors in Cybersecurity: Risks and Impacts. *Security science journal, 2*(2), pp.51-64.

Kang, J., 2018. Mobile payment in Fintech environment: trends, security challenges, and services. *Human-centric Computing and Information Sciences, 8*(1)

Karjaluoto, H., Shaikh, A.A., Saarijärvi, H. and Saraniemi, S., 2019. How perceived value drives the use of mobile financial services apps. *International Journal of Information Management, 47*, pp.252-261.

Kaur, A., Dani, D., & Agrawal, G., 2017, January. Evaluating the accessibility, usability, and security of Hospitals websites: An exploratory study. *In 2017 7th international conference on cloud computing, data science & engineering-confluence* (pp. 674-680). IEEE.

Khalid, F., Daud, M.Y., Rahman, M.J.A. and Nasir, M.K.M., 2018. An investigation of university students' awareness on cyber security. *International Journal of Engineering & Technology*, *7*(421), pp.11-14.

Khan, R., McLaughlin, K., Laverty, D. and Sezer, S., 2017, September. STRIDE-based threat modeling for cyber-physical systems. *In 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)* (pp. 1-6). IEEE.

Khandelwal, S., 2017a. New Ransomware Not Just Encrypts Your Android But Also Changes PIN Lock. *The hacker news*. [online]. Available From: https://thehackernews.com/2017/10/android-ransomware-pin.html [Accessed, 23 Feb 2018]

Khandelwal, S., 2017b. "Cyber Crime Gang Arrested for Infecting Over 1 Million Phones with Banking Trojan". *The hacker news*. [Online]. Available From: https://thehackernews.com/2017/05/cronmobile-banking-malware.html [Accessed 08 Apr 2018]

Khasawneh, M.H.A., Hujran, O. and Abdrabbo, T., 2018. A quantitative examination of the factors that influence users' perceptions of trust towards using mobile banking services. *International Journal of Internet Marketing and Advertising, 12*(2), pp.181-207.

Kishnani, U., Noah, N., Das, S. and Dewri, R., 2022, November. Privacy and Security Evaluation of Mobile Payment Applications Through User-Generated Reviews. *In Proceedings of the 21st Workshop on Privacy in the Electronic Society* (pp. 159-173).

Kohn, S.C., de Visser, E.J., Wiese, E., Lee, Y.C. and Shaw, T.H., 2021. Measurement of trust in automation: A narrative review and reference guide. *Frontiers in psychology, 12*, p.604977.

Kravchenko, T., Bogdanova, T., &Shevgunov, T., 2022. Ranking requirements using MoSCoW methodology in practice. *In Computer Science On-line Conference* (pp. 188-199). Cham: Springer International Publishing.

Krombholz, K., Busse, K., Pfeffer, K., Smith, M. and Von Zezschwitz, E., 2019, May. " If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS. *In 2019 IEEE Symposium on Security and Privacy (SP)* (pp. 246-263). IEEE.

Kumar, R., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., & Khan, R. A., 2020. An integrated approach of fuzzy logic, AHP, and TOPSIS for estimating usable-security of web applications. *IEEE Access, 8*, 50944-50957.

Kumar, V., & Mittal, S., 2020. Mobile marketing campaigns: practices, challenges, and opportunities. *International Journal of Business Innovation and Research*, 21(4), 523-539.

Kumari, S., Chaudhry, S.A., Wu, F., Li, X., Farash, M.S. and Khan, M.K., 2017. An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Applications*, *10*, pp.92-105.

Kunda, D. and Chishimba, M., 2018. A survey of Android mobile phone authentication schemes. *Mobile Networks and Applications*, pp.1-9.

Lai, K. P., 2020. FinTech: The dis/re-intermediation of finance?. *In The Routledge handbook of financial geography* (pp. 440-457). Routledge.

Lakshmanan R., 2023. Alert: 330,000 FortiGate Firewalls Still Unpatched to CVE-2023-27997 RCE Flaw, *The Hacker news*. [Online] Available From: https://thehackernews.com/2023/07/alert-330000-fortigate-firewalls-still.html [Accessed 04 Apr 2023]

Lakshmanan R., 2023. Hackers Exploiting Unpatched WordPress Plugin Flaw to Create Secret Admin Accounts. *The hacker news*. [Online] Available from: https://thehackernews.com/2023/07/unpatched-wordpress-plugin-flaw-could.html. [Accessed 20 Jul 2023]

Lal, N., 2020. Business Analysis and Planning Process in requirements phase for ERP projects. *SSRN 3673426*.

Lamoyero, Z. and Fajana, O., 2023. July. Exposed: Critical Vulnerabilities in USSD Banking Authentication Protocols. *In 2023 IEEE International Conference on Cyber Security and Resilience (CSR)* (pp. 275-280). IEEE.

Larson, H.J., Clarke, R.M., Jarrett, C., Eckersberger, E., Levine, Z., Schulz, W.S. and Paterson, P., 2018. Measuring trust in vaccination: A systematic review. *Human vaccines & immunotherapeutics, 14*(7), pp.1599-1609.

Lead, V.T.T., 2020. Usable security & privacy methods and recommendations. Cyber Security for Europe. *CyberSec4Europe D3.5*

Leguesse, Y., Colombo, C., Vella, M. and Hernandez-Castro, J., 2021. PoPL: Proof-of-Presence and Locality, or How to Secure Financial Transactions on Your Smartphone. *IEEE Access, 9*, pp.168600-168612.

Lema, A., 2017. Factors influencing the adoption of mobile financial services in the unbanked population. Inkanyiso: *Journal of Humanities and Social Sciences*, 9(1), pp.37-51.

Lennartsson, M., Kävrestad, J., & Nohlberg, M., 2021. Exploring the meaning of usable security–a literature review. *Information & Computer Security, 29*(4), 647-663.

Lessa, L. and Etoribussi, A.G., 2023. Usability of Security Mechanisms of E-Health Applications: Cases From Ethiopia. In *Fraud Prevention, Confidentiality, and Data Security for Modern Businesses* (pp. 37-56). IGI Global.

Lewis, J.R., 2018. The system usability scale: past, present, and future. *International Journal of Human–Computer Interaction, 34*(7), pp.577-590.

Li, W., Xia, Y., Lu, L., Chen, H. and Zang, B., 2019, April. TEEv: Virtualizing trusted execution environments on mobile platforms. *In Proceedings of the 15th ACM SIGPLAN/SIGOPS international conference on virtual execution environments* (pp. 2-16).

Lian, J. W., & Li, J., 2021. The dimensions of trust: An investigation of mobile payment services in Taiwan. *Technology in Society*, 67, 101753.

Limna, P., Kraiwanit, T., Siripipattanakul, S., Limna, P., Kraiwanit, T. and Siripipattanakul, S., 2023. The relationship between cyber security knowledge, awareness, and behavioural choice protection among mobile banking users in Thailand. *International Journal of Computing Sciences Research*, *7*, pp.1133-1151.

Liu, C., Clark, G. D., & Lindqvist, J., 2017, May. Where usability and security go hand-in-hand: Robust gesture-based authentication for mobile systems. *In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 374-386).

Lokanan, M. E., & Sharma, K., 2022. Fraud prediction using machine learning: The case of investment advisors in Canada. *Machine Learning with Applications*, 8, 100269.

Lu, L., 2017. Financial technology and challenger banks in the uk: Gap fillers or real challengers?. *Journal of International Banking Law and Regulation* (2017), 32(7), pp.273-282.

Luan, S., Reb, J. and Gigerenzer, G., 2019. Ecological rationality: Fast-and-frugal heuristics for managerial decision making under uncertainty. *Academy of Management Journal*, *62*(6), pp.1735-1759.

Marous, J. 2018, Banking Providers Fail to Sell Benefits of Mobile Banking and Payments. *Mobile banking payment trends*. [Online]. Available from: https://thefinancialbrand.com/69892/mobile-banking-payments trends/. [Accessed 05 May 2018]

Marsh, H.W., Morin, A.J., Parker, P.D. and Kaur, G., 2014. Exploratory structural equation modeling: An integration of the best features of exploratory and confirmatory factor analysis. *Annual review of clinical psychology*, *10*, pp.85-110.

McLeod S., 2023. Experimental Design: Types, Examples & Methods. *simply psychology*. [online] Available from: https://www.simplypsychology.org/experimental-designs.html [Accessed 29 Jun 2023]

Medina Angarita, M.A. and Nolte, A., 2020. What do we know about hackathon outcomes and how to support them?–A systematic literature review. In Collaboration Technologies and Social Computing: *26th International Conference, CollabTech 2020, Tartu, Estonia, September 8–11, 2020, Proceedings 26* (pp. 50-64). Springer International Publishing.

Melnikovas, A., 2018. Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of futures Studies, 23*(2).

Meredith, P., Summons, P., Park, M., & Cheek, B., 2019. What do Employers expect from Business Analysts and is it captured by the Business Analysis Body of Knowledge (BABOK)?. *ACIS 2019 Proceedings.* AIS Electronic Library (AISeL).

Mindermann, K., & Wagner, S. 2018, Usability and security effects of code examples on crypto apis. *In 2018 16th Annual Conference on Privacy, Security and Trust (PST)* (pp. 1-2). IEEE.

Miranda, E., 2022, June. Moscow rules: A quantitative exposé. In *International Conference on Agile Software Development* (pp. 19-34). Cham: Springer International Publishing.

Morgan, G., and Moyer, K.R 2017, How to Win in World without Trust; *Gartner research, Published 27, September, 2017*. ID: G00341586.

Mpofu, F. Y., & Mhlanga, D., 2022. Digital Financial Inclusion, Digital Financial Services Tax and Financial Inclusion in the Fourth Industrial Revolution Era in Africa. *Economies, 10*(8), 184.

Moghavvemi, S., Mei, T.X., Phoong, S.W. and Phoong, S.Y., 2021. Drivers and barriers of mobile payment adoption: Malaysian merchants' perspective. Journal of Retailing and Consumer Services, 59, p.102364.

Mohamed, H., 2019. Effect of Mobile Banking On the Financial Performance of Commercial Banks in Kenya. *Doctoral dissertation, United States International University-Africa*, *2019*.

Mobile Payment Market., 2022. Mobile Payment Market Size, Share & Trends Analysis Report by Technology (Near Field Communication, Direct Mobile Billing), by Payment Type (B2B, B2C, B2G), by Location, by End Use, by Region, and Segment Forecasts, 2022-2030. *Research and markets* [Online]. Available from: https://www.researchandmarkets.com/reports/5390561/mobile-payment-market-size-share-and-trends?utm_source=CI&utm_medium=PressRelease&utm_code=d7fstf&utm_campaign=1749981+-+Global+Mobile+Payments+Market+Report+2022%3a+A+%24587.5+Billion+Market+by+2030+-+Growth+of+mCommerce+Industry+%26+Growing+Shift+Toward+Contactless+Payments&utm_exec=chdo54prd. [Accessed 02 Jan 2023]

Mohamed, M. A., Chakraborty, J., &Dehlinger, J., 2017. Trading off usability and security in user interface design through mental models. *Behaviour & Information Technology, 36*(5), 493-516.

Mohamed, M., Gao, S., Sachdeva, N., Saxena, N., Zhang, C., Kumaraguru, P., & Van Oorschot, P. C. (2017). On the security and usability of dynamic cognitive game CAPTCHAs. *Journal of Computer Security, 25*(3), 205-230.

Mueller, R.O. and Hancock, G.R., 2018. Structural equation modeling. In *The reviewer's guide to quantitative methods in the social sciences* (pp. 445-456). Routledge.

Muniandy, L., Muniandy, B. and Samsudin, Z., 2017. Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity*, *800299*.

Murinde, V., Rizopoulos, E. and Zachariadis, M., 2022. The impact of the FinTech revolution on the future of banking: Opportunities and risks. *International Review of Financial Analysis,* 81, p.102103.

Myers, M.D., 2019. Qualitative research in business and management. *Qualitative research in business and management*, pp.1-364.

Nadeem, M., Al-Amri, J.F., Subahi, A.F., Seh, A.H., Khan, S.A., Agrawal, A. and Khan, R.A., 2022. Multi-level hesitant fuzzy based model for usable-security assessment. *Intell. Autom. Soft Compute, 31*(1), p.103304.

Naiakshina, A., Danilova, A., Tiefenau, C., Herzog, M., Dechand, S., & Smith, M. (2017, October). Why do developers get password storage wrong? A qualitative usability study. *In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 311-328).

Nambiro, A., Wabwoba, F. and Wasike, J., 2020. Cyber security challenges to mobile banking in SACCOs in Kenya. *International Journal of Computer*. ISSN 2307-4523

Naqvi, B., &Seffah, A., 2018, May. A methodology for aligning usability and security in systems and services. In 2018 3rd *International Conference on Information Systems Engineering (ICISE)* (pp. 61-66). IEEE.

Ndibwile, J.D., Luhanga, E.T., Fall, D. and Kadobayashi, Y., 2019. A demographic perspective of smartphone security and its redesigned notifications. *Journal of Information Processing*, *27*, pp.773-786.

Nguyen, G., Nguyen, B.M., Tran, D. and Hluchy, L., 2018. A heuristics approach to mine behavioural data logs in mobile malware detection system. *Data & Knowledge Engineering*, *115*, pp.129-151.

NIBSS., 2018. NIBSS, Banks, Telcos Deepen Financial Inclusion with mCASH. *mCash Press release*. [Online]. Available from: https://www.nibss-plc.com.ng/images/api/mCASH_Press_Release.pdf. [Accessed 23 May 2018]

NIST., 2023 Cybersecurity Framework. *NIST*. [Online] Available From: https://www.nist.gov/cyberframework. [Accesed 01 Jul 2023]

Nolte, A., Chounta, I.A. and Herbsleb, J.D., 2020. What happens to all these hackathon projects? Identifying factors to promote hackathon project continuation. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), pp.1-26.

Obaid, M., Bayram, Z., & Saleh, M., 2019. Instant secure mobile payment scheme. *IEEE Access*, 7, 55669-55678

Oliveira, D.S., Lin, T., Rahman, M.S., Akefirad, R., Ellis, D., Perez, E., Bobhate, R., DeLong, L.A., Cappos, J. and Brun, Y., 2018. {API} blindspots: Why experienced developers write vulnerable code. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 315-328).

Odueso T, 2022. MTN accuses 18 Nigerian banks of $53 million mobile money fraud, *TechCabal.* [Online]. Available from: https://techcabal.com/2022/06/27/mtn-accuses-18-nigerian-banks-of-53-million-mobile-money-fraud/. [Accessed 30 Dec 2022]

Ouma, S.A., Odongo, T.M. and Were, M., 2017. Mobile financial services and financial inclusion: Is it a boon for savings mobilization?. *Review of development finance, 7*(1), pp.29-35

OWASP, 2023 OWASP Foundation, the Open Source Foundation for Application Security | *OWASP Foundation*. [Online]. Available From:https://owasp.org/. [Accessed 01 Jul 2023]

Owusu, G. M. Y., Bekoe, R. A., Addo-Yobo, A. A., & Otieku, J., 2021. Mobile banking adoption among the Ghanaian youth. *Journal of African Business*, 22(3), 339-360.

Parizi, R. M., Amritraj, and Dehghantanha, A., 2018. Smart contract programming languages on blockchains: An empirical evaluation of usability and security. In Blockchain–ICBC 2018: First International Conference, Held as Part of the Services Conference Federation, *SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 1* (pp. 75-91). Springer International Publishing.

PCI DSS., 2023. Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security, and Credit Card Security Standards. *PCI Security Standards.* [online]. Available from: https://www.pcisecuritystandards.org/. [Accessed 02 Jul 2023]

Pearman, S., Zhang, S.A., Bauer, L., Christin, N. and Cranor, L.F., 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 319-338).

Perlman, L., 2017, Technology Inequality, Opportunities and Challenges for Mobile Financial Services, Centre for Financial Inclusion, Accion. *Columbia Business School Research Paper, 201.*

Pinto, S., Gomes, T., Pereira, J., Cabral, J. and Tavares, A., 2017. IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices. *IEEE Internet Computing, 21*(1), pp.40-47.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D., 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, *Technology and Work, 24*(2), 371-390.

Quiñones, D., &Rusu, C. (2017). How to develop usability heuristics: A systematic literature review. *Computer standards and interfaces*, *53*, 89-122.

Rahman, T., Rohan, R., Pal, D. and Kanthamanon, P., 2021, June. Human factors in cybersecurity: a scoping review. *In The 12th International Conference on Advances in Information Technology* (pp. 1-11).

Realpe-Muñoz, P., Collazos, C.A., Granollers, T., Muñoz-Arteaga, J. and Fernandez, E.B., 2017, September. Design process for usable security and authentication using a user-centred approach. *In Proceedings of the XVIII International Conference on Human Computer Interaction* (pp. 1-8).

Realpe, P. C., Collazos, C. A., Hurtado, J., & Granollers, A., 2016. A set of heuristics for usable security and user authentication. *In Proceedings of the XVII International Conference on Human Computer Interaction* (pp. 1-8).

Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J. and Seamons, K., 2019. A usability study of five {two-factor} authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)* (pp. 357-370).

Reuter, C., Iacono, L. L., &Benlian, A., 2022. A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead. *Behaviour and Information Technology, 41*(10), 2035-2048.

Reuters, 2020. UK to raise contactless card payment limit to 45 pounds in April. *Britain payments limit*. [online]. Available from: https://www.reuters.com/article/britain-payments-limit/uk-to-raise-contactless-card-payment-limit-to-45-pounds-in-april-idUSL4N2BG518. [Accessed 12 Dec 2020]

Rizzo, M., 2018. CYBERSECURITY FOR MOBILE FINANCIAL SERVICES-FAQs for regulators, supervisory authorities and digital financial. *CGAP research report*.

Rocha, L.C., Andrade, R.M., Sampaio, A.L. and Lelli, V., 2017. Heuristics to evaluate the usability of ubiquitous systems. In *Distributed, Ambient and Pervasive Interactions: 5th International Conference, DAPI 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9–14, 2017, Proceedings 5* (pp. 120-141). Springer International Publishing.

Rohan, R., Funilkul, S., Pal, D. and Chutimaskul, W., 2021a, December. Understanding of human factors in cybersecurity: A systematic literature review. *In 2021 International Conference on Computational Performance Evaluation (ComPE)* (pp. 133-140). IEEE.

Rossi I, 2023. Securing Your WiFi Network: Risks, Vulnerabilities, and Best Practices. *Pulse*. [online]. Available from: https://www.linkedin.com/pulse/securing-your-wifi-network-risks-vulnerabilities-best-isabella-rossi. [Accessed 10 May 2023]

Ruan, Y., Zhang, P., Alfantoukh, L. and Durresi, A., 2017. Measurement theory-based trust management framework for online social communities. *ACM Transactions on Internet Technology (TOIT), 17*(2), pp.1-24.

Russo, D. and Van Roy, B., 2018. Satisficing in time-sensitive bandit learning. *arXiv preprint arXiv:*1803.02855.

Rys, M., 2023. Invention development. the hackathon method. *Knowledge Management Research and Practice, 21*(3), pp.499-511.

Salam, A. 2020. Internet of things for sustainable community development: introduction and overview. *In Internet of Things for Sustainable Community Development* (pp. 1-31). Springer, Cham.

Schiller, K. and Adamsky, F., 2021, October. Work in Progress: Can Johnny Encrypt E-Mails on Smartphones?. In *International Workshop on Socio-Technical Aspects in Security* (pp. 182-193). Cham: Springer International Publishing.

Seo, J.H. and Park, E.M., 2018. A study on financing security for smartphones using text mining. *Wireless Personal Communications*, 98, pp.3109-3127.

Shareef, M.A., Baabdullah, A., Dutta, S., Kumar, V. and Dwivedi, Y.K., 2018. Consumer adoption of mobile banking services: An empirical examination of factors according to adoption stages. *Journal of Retailing and Consumer Services*, 43, pp.54-67.

Sharma, S. K., and Al-Muharrami, S., 2018. Mobile banking adoption: Key challenges and opportunities and implications for a developing country. Emerging Markets from a Multidisciplinary Perspective. *Advances in Theory and Practice of Emerging Markets (ATPEM)* (pp. 75-86). Springer International Publishing

Sheridan, T.B., 2019. Individual differences in attributes of trust in automation: measurement and application to system design. *Frontiers in Psychology*, 10, p.1117.

Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P. and Woody, C., 2018. Threat modeling: a summary of available methods. *Carnegie Mellon University Software Engineering Institute Pittsburgh United States*.

Shilling C., 2021. New contactless payment limit – what do small businesses need to know?. *Simply business*. [Online]. Available from: https://www.simplybusiness.co.uk/knowledge/articles/2021/10/contactless-payment-limit-increased/. [Accessed 2 Jul 2023]

Shrestha, N., 2021. Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics*, *9*(1), pp.4-11.

Snehal M, Onkar S, 2020, Mobile Banking Market by transaction (consumer-to-consumer and consumer-to -business), Platform (Android, IOS, and others): Global opportunity analysis and industry forecast, 2019-2026). *Mobile Banking Market*. [Online]. Available from: https://www.alliedmarketresearch.com/mobile-banking-market. [Accessed 30 Dec 2020]

Sommerhalder, M., 2023. Trusted Execution Environment. *Trends in Data Protection and Encryption Technologies* (pp.95-101). Springer International Publishing

STA, 2018, Secure Technology Alliance, Trusted Execution Environment (TEE) 101: A primer. Version 1.0. *A Secure Technology Alliance Mobile Council White Paper*

Stone, C.M., Chothia, T. and Garcia, F.D., 2017 Spinner: “Semi-automatic detection of pinning without hostname verification”. December, 2017. *In Proceedings of the 33rd Annual Computer Security Applications Conference (pp. 176-188).* ACM.

Subashini, N., Udayanga, L., De Silva, L. H. N., Edirisinghe, J. C., & Nafla, M. N. 2022. Undergraduate perceptions on transitioning into E-learning for continuation of higher education during the COVID pandemic in a developing country: a cross-sectional study from Sri Lanka. *BMC Medical Education, 22*(1), 1-12.

Takeda, A. and Ito, Y., 2021. A review of FinTech research. *International Journal of Technology Management, 86*(1), pp.67-88.

Temelkov, Z., 2020. Differences between traditional bank model and fintech based digital bank and neobanks models. SocioBrains, *International scientific refereed online journal with impact factor*, (74), pp.8-15.

Thakor, A.V., 2020. Fintech and banking: What do we know? *Journal of Financial Intermediation*, 41, p.100833.

Theofanos, M., 2020. Is usable security an oxymoron?. *Computer*, *53*(2), pp.71-74

TOGAF, 2023, The Open Group Architecture Framework *(TOGAF)® Standard, Version 9.2.* [Online]. Available From: https://pubs.opengroup.org/architecture/togaf9-doc/arch/. [Accessed 10 May 2023]

Tun, P.M., 2020. An investigation of factors influencing intention to use mobile wallets of mobile financial services providers in Myanmar. *The Asian Journal of Technology Management, 13*(2), pp.129-144.

Van Niekerk, C.M., 2022. Usable Security Heuristics for Instant Messaging Application Development. *Masters of Information Technology thesis*. Mandela University

Van Schaik, P., Renaud, K., Wilson, C., Jansen, J. and Onibokun, J., 2020. Risk as affect: The affect heuristic in cybersecurity. *Computers & Security*, *90*, p.101651.

Verizon, 2018, Data Breach Investigation report. *Verizon reports*. [Online]. Available from: https://www.verizon.com/business/resources/T422/reports/DBIR_2018_Report.pdf. [Accessed 04 Sep 2019]

Verma, A., Khatana, A. and Chaudhary, S., 2017. A comparative study of black box testing and white box testing. *International Journal of Computer Sciences and Engineering, 5*(12), pp.301-304.

Vimala, B., & Alamelu, K., 2021. Forcible Displacement, Financial Inclusion and Consequences. *International Journal of Advance and Innovative Research, 8*(4), 9-17.

VomBrocke, J., Hevner, A. and Maedche, A., 2020. Introduction to design science research. *Design science research. Cases*, pp.1-13.

Wang, T., Zhang, G., Bhuiyan, M. Z. A., Liu, A., Jia, W., & Xie, M. (2020). A novel trust mechanism based on fog computing in sensor–cloud system. *Future Generation Computer Systems,* 109, 573-582.

Wang, Y., Rawal, B., Duan, Q., & Zhang, P., 2017, February. Usability and security go together: A case study on database. *In 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)* (pp. 49-54). IEEE.

Wang, Y., Liu, X., Mao, W. and Wang, W., 2019, May. Dcdroid: Automated detection of ssl/tls certificate verification vulnerabilities in android apps. *In Proceedings of the ACM Turing Celebration Conference-China* (pp. 1-9).

Wang, Y., Luan, S. and Gigerenzer, G., 2022. Modeling fast-and-frugal heuristics. *PsyCh Journal*, *11*(4), pp.600-611.

Ward, J., Dogan, H., Apeh, E., Mylonas, A. and Katos, V., 2017. Using human factor approaches to an organisation's Bring Your Own Device scheme. *In Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017,*

*Held as Part of HCI International 2017, Vancouver, BC, Canada, July 9-14, 2017, Proceedings 5* (pp. 396-413). Springer International Publishing.

Wazid, M., Zeadally, S. and Das, A.K., 2019. Mobile banking: evolution and threats: malware threats and security solutions. *IEEE Consumer Electronics Magazine*, *8*(2), pp.56-60.

Weber, S., Coblenz, M., Myers, B., Aldrich, J., & Sunshine, J., 2017. Empirical studies on the security and usability impact of immutability. 2017 IEEE Cybersecurity Development (SecDev), 50-53.

Weese, S. and Wagner, T., 2017. *CBAP/CCBA certified business analysis study guide*. John Wiley & Sons.

White, A., and Oestreich, T.W, 2017, Reset Your Information Governance Approach by Moving From Truth to Trust, Published: 8 May 2017 *ID: G00319696*

Wiefling, S., Dürmuth, M. and Lo Iacono, L., 2020, December. More than just good passwords? A study on usability and security perceptions of risk-based authentication. In *Proceedings of the 36th Annual Computer Security Applications Conference* (pp. 203-218).

Wijayarathna, C., &Arachchilage, N. A. G., 2019. Why Johnny can't develop a secure application? A usability analysis of Java Secure Socket Extension API. *Computers and Security*, 80, 54-73.

Wodo, W., Blaskiewicz, P., Stygar, D. and Kuzma, N., 2021. Evaluating the security of electronic and mobile banking. *Computer Fraud & Security, 2021*(10), pp.8-14.

XIE, X., 2019. Principal component analysis. Wiley interdisciplinary reviews.

Yaacoub A. 2019, Counterfeit Mobile Devices  More Than Just a Security Risk. *Two birds*. [online]. Available from: https://www.twobirds.com/en/insights/2019/uae/counterfeit-mobile-devices-more-than-just-a-security-risk#:~:text=Counterfeit%20Mobile%20Devices%20%E2%80%93%20More%20Than%20Just%20a,Cost%20of%20IPR%20Infringement%20in%20the%20Smartphones%20Sector%22%29. [Accessed 10 Mar 2023].

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E., 2018. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behaviour*, 84, pp.375-382.

Yan, C., Siddik, A.B., Akter, N. and Dong, Q., 2021. Factors influencing the adoption intention of using mobile financial service during the COVID-19 pandemic: The role of FinTech. *Environmental Science and Pollution Research*, pp.1-19.

Yıldırım, M. and Mackie, I., 2019. Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, pp.741-759.

Zhang, M. Y., & Williamson, P., 2021. The emergence of multiplatform ecosystems: insights from China's mobile payments system in overcoming bottlenecks to reach the mass market. *Technological Forecasting and Social Change*, 173, 121128.

Zhou, L., Bao, J., Watzlaf, V. and Parmanto, B., 2019. Barriers to and facilitators of the use of mobile health apps from a security perspective: mixed-methods study. *JMIR mHealth and uHealth*, *7*(4), p.e11223.

Zhu, Q., Lyu, Z., Long, Y., & Wachenheim, C. J., 2022. Adoption of mobile banking in rural China: Impact of information dissemination channel. *Socio-Economic Planning Sciences*, 83, 101011.

# Appendix I: MFS Sociotechnical Study

**Financial Services Regulator**

Participant profile

- 1 Payment System Expert
- 1 Mobile Financial Services expert
- 1 Banking Compliance and Surveillance Expert
- 1 Official of ePayment Security Committee
- 1 Financial Inclusion representative

Soft Systems Approach Output:

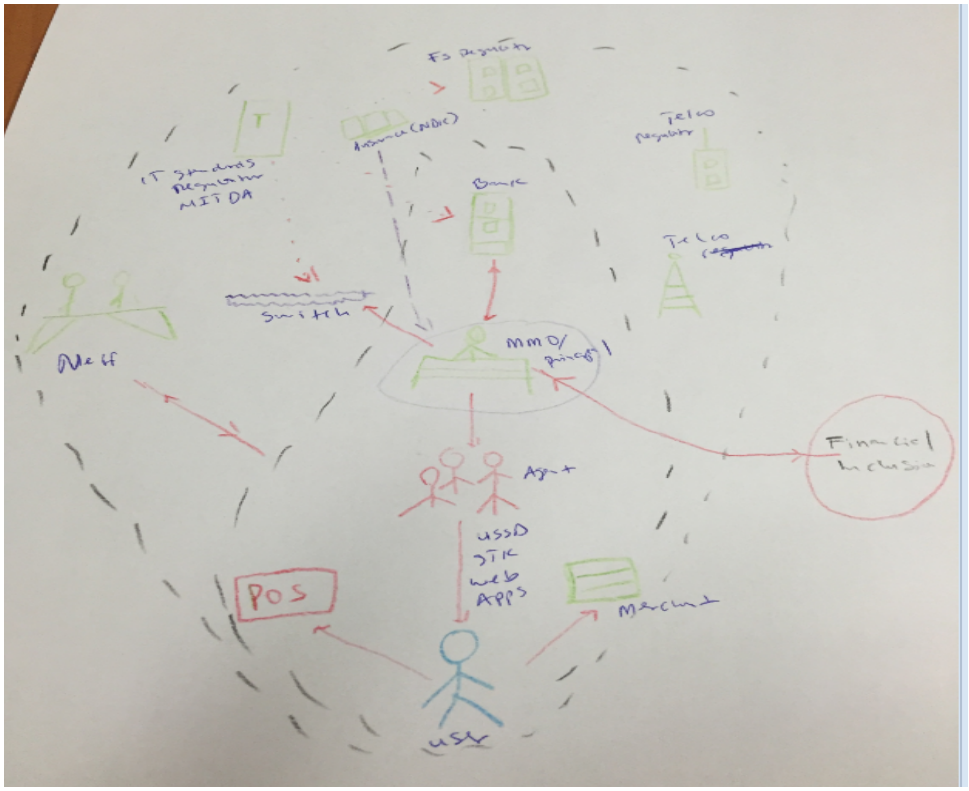



Figure A1: Photograph of Rich Picture by FS Regulator Group Focus Group (personal collection 2017)

Root Definition:

An industry-wide information security operations centre that will facilitate information sharing on cybersecurity incidences by participants (all stakeholders in financial services) in order to minimise the risk of cybercrime and boost end-user confidence in the financial sector

C: End-User

A: Central Bank, Banks, Technology Service Providers, Cybersecurity Experts, Law enforcement, Judiciary

T: Information Security Operations Centre

W: Information security operations centre will facilitate collaboration in combatting cybercrime

O: Bankers Committee

E: Financial Services Sector

The final task for the soft system approach was for the group to come up with a conceptual model based on the root definition. Figure below shows the model.

Conceptual Model (CM):

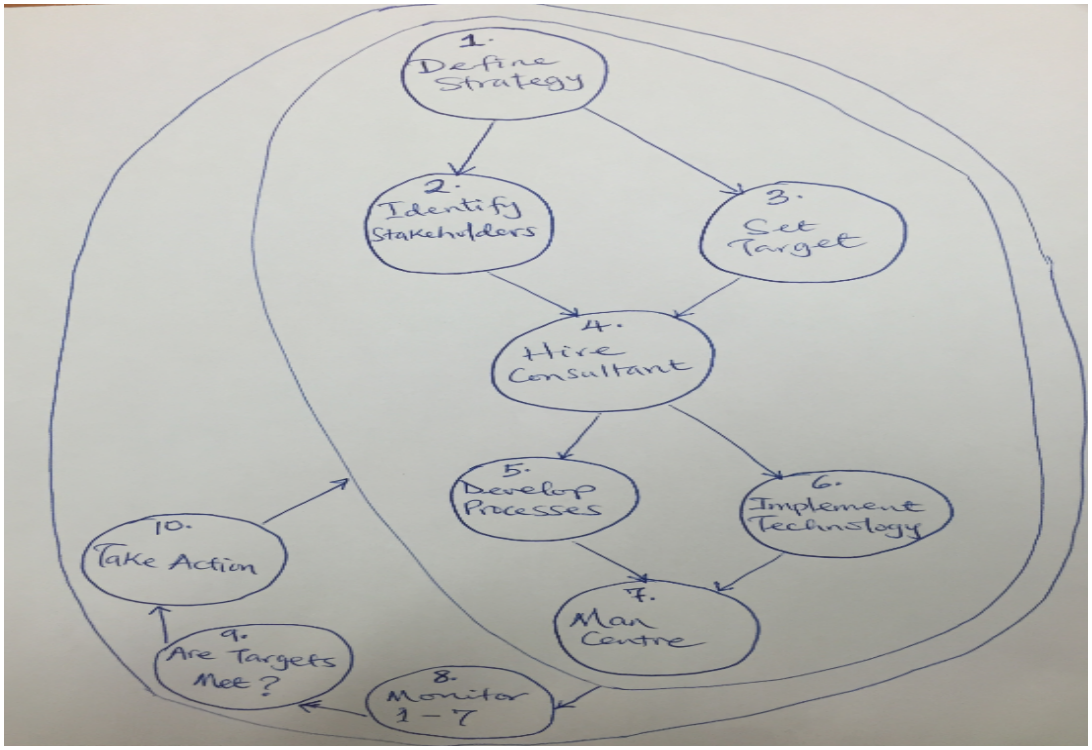



Figure A2: Photograph of CM by FS Regulatory Focus Group (personal collection 2017)

IW Output by FS Group

P1: FI

1. Lack of sufficient user awareness
2. Telecommunication infrastructure challenges

3. Regulatory gaps due to unaligned regulatory perspectives between the monetary authority and telco regulator
4. Lack of stringent KYC requests to accommodate the unbanked
5. Lapses in SIM registration process
6. International Monetary transfer might be used for money laundry or terrorism financing
7. Cross border nature of funds transfer might cause regulatory gaps that might lead to cyber crime

P2: SS

1. Vulnerability introduced in the system due to weaknesses in USSD technology
2. Data privacy concerns hindering investigation
3. Implementation model might impact monetary policy
4. Regulatory gap (no regulation for internal payment wallet)
5. Low capitalization by MMO
6. Insufficient cybersecurity awareness campaign by banks for Mobile banking users

P3: BSD

1. Poor cyber risk management and oversight from board of directors down to middle management
2. Top management focus more and business strategy and profitability and give little or no consideration for effective enterprise-wide cybersecurity programme
3. Lack policies and procedures for establishing appropriate accountability and oversight
4. Poor cybersecurity controls by banks
5. Lack of trainings and sensitization to address the practices and processes the banks uses to protect assets, infrastructure, and information

6. Lack of process for continuous, automated protection and monitoring by banks
7. Lack of capability for threat detection
8. Lack of sufficient threat Intelligence and Collaboration by financial services sector
9. Lack of external dependency management of technology assets and information
10. Lack of cyber-Incident management process
11. Lack of rigorous emphasis on cyber resilience in technology dependent process implementation
12. Lack of capability to ensure compliance to technology standards

P4: Payment System

1. Security of mobile wallet not circumspect
2. Least KYC approach (Phone number, name and address only) might encourage fraudsters
3. Deviation from guidelines during implementation might open up to process to fraud
4. The anonymity of mobile phone-based transactions might be an incentive for money laundry
5. Lack of skills by regulators to enforce compliance

P5: BPS

1. Vulnerability in USSD might be exploited
2. Drop sessions due to restrictions from telcos might be exploited to perpetuate fraud. For instance, a USSD session in Nigeria last only 120 seconds
3. Clone apps for mobile banking exist in some app's stores. Unsuspecting users might fall prey and be defrauded
4. Services outage by telcos might cause a vulnerability in the system

5. Service downtime with Mobile Money Operators might cause a vulnerability in the system
6. Lack of an end-to-end BCP for the ecosystem might lead to a vulnerability
7. Lack of proper reconciliation by Mobile Money Operators (MMO) might lead to cyber crime
8. Delay in reconciliation between e-float and actual bank balance by MMO might lead to cyber crime
9. Unsuspecting users can be defrauded via sperm SMS or call

Grouping of Issues

| **Process** | **People** |
|---|---|
| Lack of stringent KYC request to accommodate the unbanked<br><br>Insufficient cybersecurity awareness campaign by banks for Mobile banking users<br><br>Poor cyber risk management and oversight from board of directors down to middle management<br><br>Top management focus more and business strategy and profitability and give little or no consideration for effective enterprise-wide cybersecurity programme<br><br>Lack policies and procedures for establishing appropriate accountability and oversight<br><br>Poor cybersecurity controls by banks<br><br>Lack of trainings and sensitization to address the practices and processes the banks uses to protect assets, infrastructure, and information<br><br>Lack of process for continuous, automated protection and monitoring by banks | Lack of sufficient user awareness<br><br>Lack of stringent KYC request to accommodate the unbanked<br><br>Lapses in SIM registration process<br><br>Lack of capability for threat detection<br><br>Lack of capability to ensure compliance to technology standards<br><br>Lack of skills by regulators to enforce compliance<br><br>Unsuspecting users can be defrauded via sperm SMS or call |

| | |
|---|---|
| Lack of capability for threat detection<br><br>Lack of sufficient threat Intelligence and Collaboration by financial services sector<br><br>Lack of external dependency management of technology assets and information<br><br>Lack of cyber-incident management process<br><br>Lack of rigorous emphasis on cyber resilience in technology dependent process implementation<br><br>The anonymity of mobile phone-based transactions might be an incentive for money laundry<br><br>Lack of an end-to-end BCP for the ecosystem might lead to a vulnerability<br><br>Lack of proper reconciliation by Mobile Money Operators (MMO) might lead to cyber crime<br><br>Delay in reconciliation between e-float and actual bank balance by Mobile Money Operators might lead to cyber crime | |
| **Technology** | **Regulation** |
| Telecommunication Infrastructure Challenges<br><br>Vulnerability introduced in the system due to weaknesses in USSD technology<br><br>Lack of capability for threat detection<br><br>Vulnerability in USSD might be exploited<br><br>Drop sessions due to restrictions from telcos might be exploited to perpetuate fraud. For instance, a USSD session in Nigeria last only 120 seconds | Regulatory gaps due to unaligned regulatory perspectives between Monetary authority and Telco regulator<br><br>International Monetary transfer might be used for money laundry or terrorism financing<br><br>Cross border nature of funds transfer might cause regulatory gaps that might lead to cyber crime<br><br>Data privacy concerns hindering investigation |

| | |
|---|---|
| Clone apps for mobile banking exist in some app's stores. Unsuspecting users might fall prey and be defrauded<br><br>Services outage by telcos might cause a vulnerability in the system<br><br>Service downtime with Mobile Money Operators might cause a vulnerability in the system | Implementation model might impact monetary policy<br><br>Regulatory gap (no regulation for internal payment wallet)<br><br>Low capitalization by MMO<br><br>Lack of sufficient threat Intelligence and Collaboration by financial services sector<br><br>Security of mobile wallet not circumspect<br><br>Least KYC approach (Phone number, name and address only) might encourage fraudsters<br><br>Deviation from guidelines during implementation might open up to process to fraud |

Table A1: Grouping of Issues 1

Nominal Group Technique Output

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Ensure compliance to standards | 4 | 1 | 2 | 4 | 2 | 13 |
| 2 | Setup an industry wide cybersecurity operations centre | 3 | - | 4 | 5 | 5 | 17 |
| 3 | Ensure Deposit Money Banks implement necessary oversight for cybersecurity | 5 | 2 | 3 | 3 | 1 | 14 |
| 4 | Mitigate risk associated with poor infrastructure (e.g. power, internet, technology) | - | 4 | 5 | 1 | 4 | 14 |
| 5 | Improve user awareness on mobile banking security and general technology security | 1 | 5 | 1 | 2 | - | 9 |
| 6 | Develop strategy for external dependence management | 2 | 3 | - | - | 3 | 8 |

Table A2: Nominal Group Technique Output

## Banks

### Participant Profile

All stakeholders were from ebusiness unit of their Banks. The unit has direct responsibility for Mobile related Banking Business

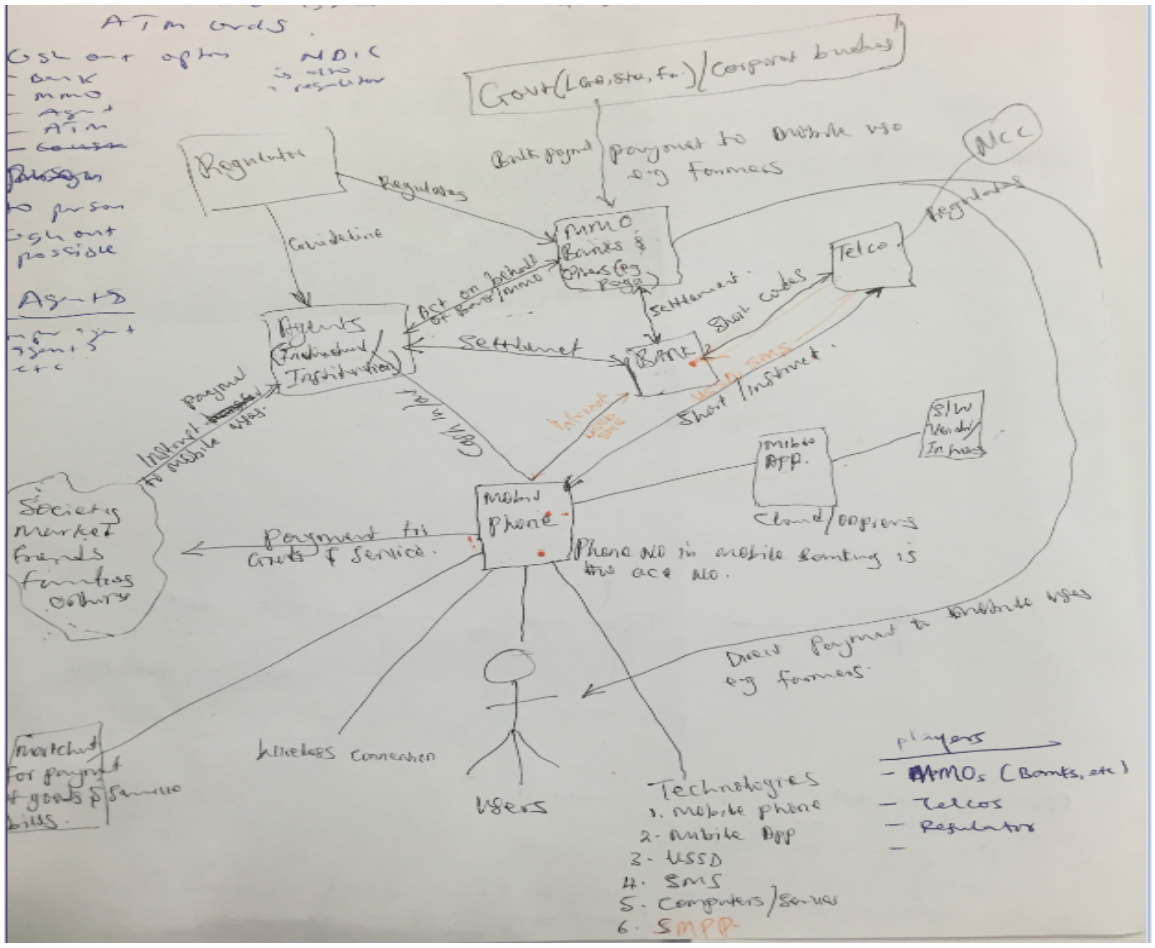



Figure A3: Photograph Rich Picture by Banking Focus Group (personal collection 2017)

Based on the rich picture and one of the obvious problems in the ecosystem, the group was requested to come up with a root definition, below was the root definition of the group.

**Root Definition:**

A robust user awareness programme that will ensure end-user data security by providing regular user education that will keep users abreast of new cyber security threat and safe use of mobile banking, delivered by banks

C: End-user

A: Banks, Agents and Mobile Money Operator

T: Implementing a user security awareness programme

W: Regularly educating users on cybersecurity threat will mitigate end-user related security breaches

O: Banks

E: Mobile Financial Services environment

The final task for the soft system approach was for the group to come up with a conceptual model based on the root definition. Figure below shows the model.

**Conceptual Model (CM):**

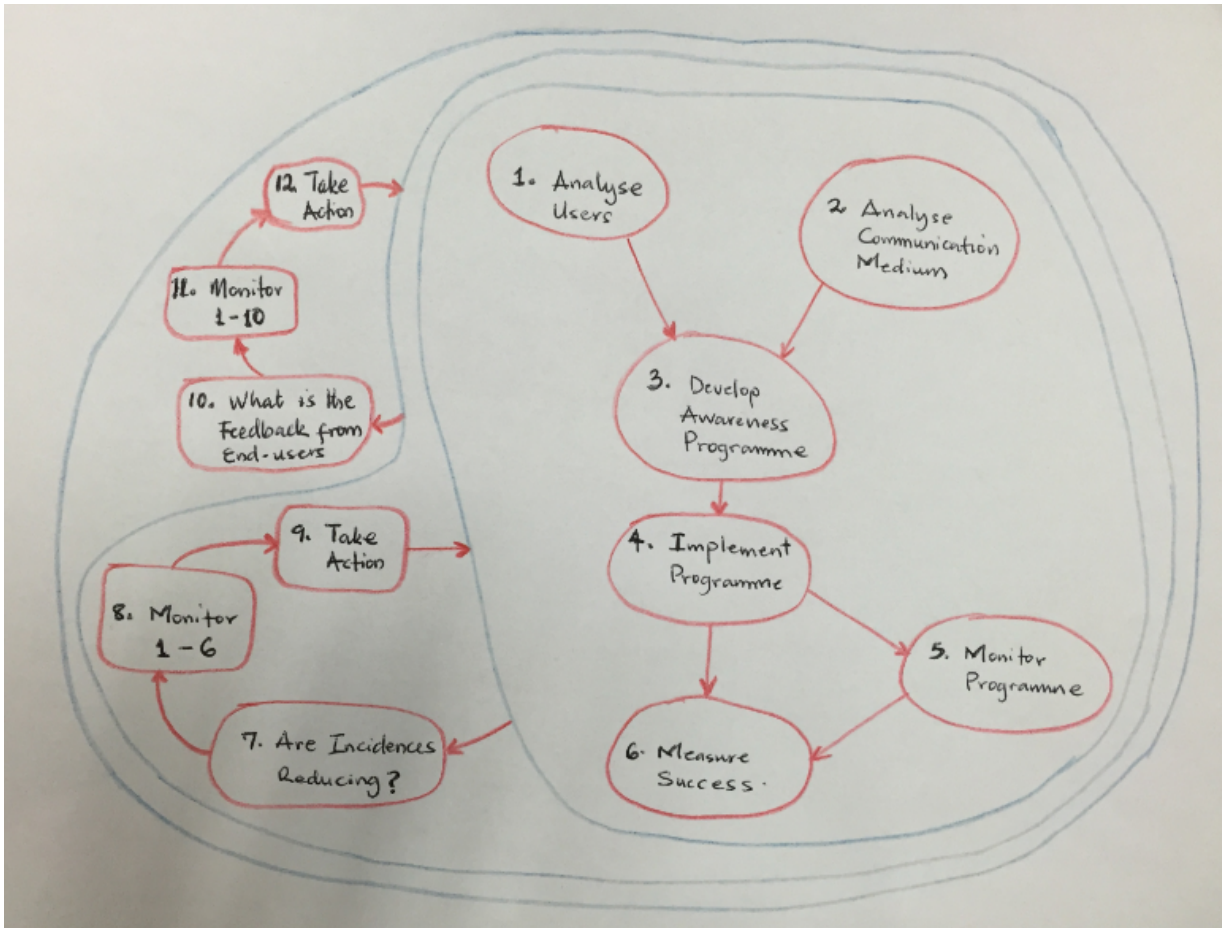



Figure A4: Photograph of CM by Banking Focus Group (personal collection 2017)

IW Output

P1:

1. Risk of losing phone and credentials might lead to cyber crime
2. Poor Telco service might create gaps for cyber crime
3. Lack of proper reconciliation by Mobile Money Operators between pool funds and e-float might lead to cybercrime
4. Rise in mobile malware which can be used to compromise a phone and access mobile banking application

5. Lack of awareness on malware by mobile banking users
6. Phishing and collecting data from users via social engineering
7. Infrastructure challenges – connectivity and power issues
8. Lack of system redundancy
9. Skill gaps in mobile banking system management by banks
10. Design issues- poor design of mobile banking platform
11. Banks driven by profitability and trading important security control for speed to market
12. Interface issues between the mobile banking and payment apps and core banking application

P2:

1. Lack of skills/knowledge by user on how to protect password/passcode, PIN etc
2. The risk of ignorant users sharing confidential details with agents based on trust
3. Cash build up by agent and their ability to manage volume
4. Reconciliation problem which can be exploited
5. Application security loopholes that can be taken advantage of
6. Apathy towards internet/mobile transaction due to unresolved issues that have arisen from past banking transaction

P3:

1. Insecurity of the phone being accessible by family members and friends
2. Unreliability of mobile operator
3. Lack of It skills by phone owners/users
4. Phone OS upgrade might not be compatible with application
5. Application accessibility from rural and remote areas

P4:

1. Interception by hacker/imposter between user and partner (vendor, bank, merchant etc.)
2. Collusion between players (e.g. staff of Agent and staff of bank) to exploit weaknesses in the system
3. Inoperative/non-existing controls resulting in vulnerabilities
4. Possibility of user's phone been stolen leading to phone security being breached by the thieves
5. Insider abuse
6. Mobile Money and Mobile Payment platform do not offer token and can be spoofed
7. Mobile Money security depends on the channel between mobile application and service provider. This can be compromised
8. Mobile wallet is unregulated and can lead to fraud

P5:

1. Misplacement of mobile phones
2. Dubious agents deliberately refusing to remit transactions
3. Double or multiple transactions. Users mistakenly making multiple transactions unknowingly
4. Application congruence with operating system and the mobile phone
5. Human Ignorance of system use
6. Drive for better user experience on devices to the detriment of security
7. Trade-off between user experience and security on mobile banking apps

Ideas Grouping

| **Awareness** | **Infrastructure** |
|---|---|
| Lack of awareness on malware by mobile banking users<br><br>Phishing and collecting data from users via social engineering | Poor Telco service might create gaps for cyber crime<br><br>Infrastructure challenges – connectivity and power issues<br><br>Lack of system redundancy |

| | |
|---|---|
| Skill gaps in mobile banking system management by banks<br><br>Lack of skills/knowledge by user on how to protect password/passcode, PIN etc<br><br>The risk of ignorant users sharing confidential details with agents based on trust<br><br>Insecurity of the phone being accessible by family members and friends<br><br>Lack of It skills by phone owners/users<br><br>Human Ignorance of system use | Interface issues between the mobile banking and payment apps and core banking application<br><br>Application security loopholes that can be taken advantage of<br><br>Unreliability of mobile operator<br><br>Phone OS upgrade might not be compatible with application<br><br>Interception by hacker/imposter between user and partner (vendor, bank, merchant etc.)<br><br>Mobile Money and Mobile Payment platform do not offer token and can be spoofed<br><br>Application congruence with operating system and the mobile phone |
| **Process** | **Others** |
| Lack of proper reconciliation by Mobile Money Operators between pool funds and e-float might lead to cybercrime<br><br>Inoperative/non-existing controls resulting in vulnerabilities<br><br>Insider abuse<br><br>Mobile Money security depends on the channel between mobile application and service provider. This can be compromised<br><br>Mobile wallet is unregulated and can lead to fraud<br><br>Double or multiple transactions. Users mistakenly making multiple transactions unknowingly | Risk of losing phone and credentials might lead to cyber crime<br><br>Rise in mobile malware which can be used to compromise a phone and access mobile banking application<br><br>Design issues- poor design of mobile banking platform<br><br>Banks driven by profitability and trading important security control for speed to market<br><br>Cash build up by agent and their ability to manage volume<br><br>Reconciliation problem which can be exploited<br><br>Apathy towards internet/mobile transaction due to unresolved issues that have arisen from past banking transaction<br><br>Application accessibility from rural and remote areas<br><br>Collusion between players (e.g. staff of Agent and staff of bank) to exploit weaknesses in the system<br><br>Possibility of user's phone been stolen leading to phone security being breached by the thieves<br><br>Dubious agents deliberately refusing to remit transactions<br><br>Misplacement of mobile phones<br><br>Trade-off between user experience and security on mobile banking apps |

Table A3: Grouping of Issues 2

Nominal Group Technique Output

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Enforce segregation of duty in Banks to minimise possibility of insider abuse | | 4 | 4 | 4 | 5 | 17 |
| 2 | Provide redundancy for infrastructure to mitigate against service downtime | 5 | 3 | 5 | 1 | 3 | 17 |
| 3 | Eliminate reconciliation issues between Mobile Money Operators and their agents | 4 | 1 | 1 | | 1 | 7 |
| 4 | Implement robust awareness programme on social engineering for users | 3 | 5 | 3 | 5 | 4 | 20 |
| 5 | Set up cybersecurity response units in banks | 2 | 2 | 2 | 2 | 2 | 10 |
| 6 | Ensure regular system upgrade and patching by banks | 1 | | | 3 | | 4 |

Table A4: Nominal Group Technique Output 2

**Unbanked or No Mobile Banking/Mobile Money Account**

**Participant Profile**

1. 1 Medical Doctor
2. 1 Civil Servant
3. 2 Students
4. 1 Unemployed

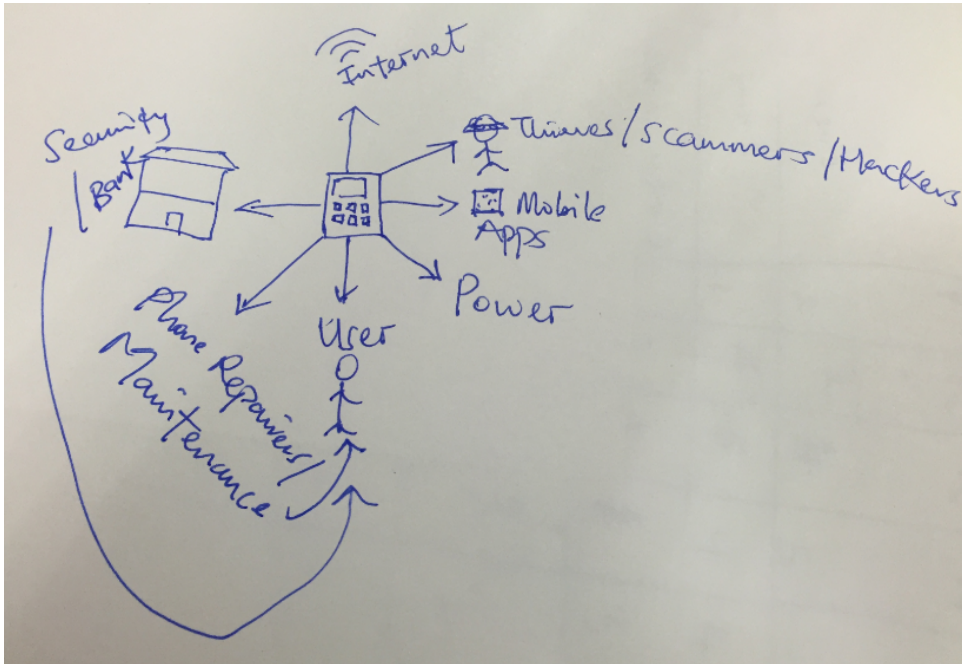



Figure A5: Photograph of Rich Picture by the Unbanked Focus Group (personal collection 2017)

**Root Definition:**

Provide information that will help customer understand how to manage phone security and to escalate any security breach in order to improve confidence in the system

C: Customer

A: Banks, Agents

T: Information sharing

W: The more customers understand the system the more their confidence in the system will improve

O: Banks

E: Mobile Banking and Payment

The final task for the soft system approach was for the group to come up with a conceptual model based on the root definition. Figure below shows the model.

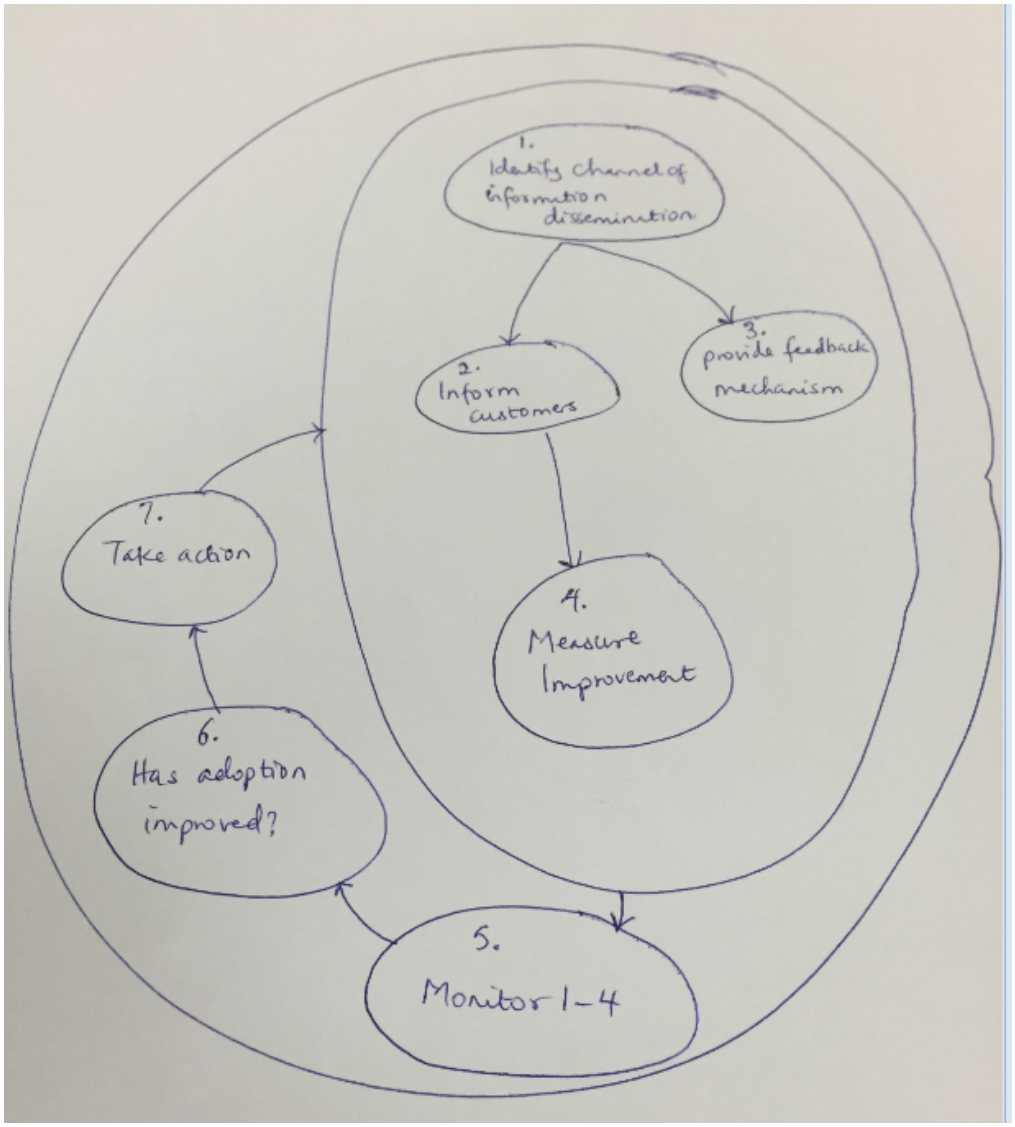



Figure A6: Photograph of CM by the Unbanked Group (personal collection 2017)

IW Output

P1:

1. Lack knowledge of security skills by financial officers in banks
2. Inadequate security measures taken by users
3. Mobile Hacking and theft
4. Poor maintenance measures by users i.e leaving viruses into the device
5. Poor security measure taken by bank
6. Lack of IT skills by phone users
7. Inadequate security measures by banks

P2:

1. Lack of security consciousness by users
2. Proximity to banking halls as soon as security breaches occur especially in satellite towns that habit a larger population
3. Carelessness of the part of users
4. Intelligent thieves who are smarter in IT than the average population
5. Poor maintenance of bank appliance which lead to problems in money transfer
6. Carelessness on the part of the bankers

P3:

1. Lack of proper understanding of users' ability by mobile banking providers
2. Lack of proper mobilization and orientation of the public
3. Lack of knowledge on the part of security agents in cases of mobile banking scams
4. Lack of proper check on the customer service
5. lack of proper advice on internet banking security
6. poor access to internet service and power

P4:

1. Inadequate information on mobile banking
2. Lack of adequate power supply
3. Wrong usage of the service
4. Lack of maintenance on part of the users
5. Poor internet services
6. Lack of sufficient information on the service
7. Proximity to banking hall in event of a need to physically report breach

P5:

1. Lack of proper security checks by banks

2. Porosity of internet leading to hacking by thieves
3. Lack of sufficient IT knowledge by bank support staff
4. Poor power supply
5. Lack of IT knowledge by users
6. Carelessness by users
7. Fear of uncertainty by users
8. Poor internet access
9. Carelessness on the part of the customer service

Idea Grouping

| **Banks** | **Users** |
|---|---|
| Lack of proper mobilization and orientation of the public<br>Lack of proper understanding of users' ability by mobile banking providers<br>Proximity to banking halls as soon as security breaches occur<br>Poor security measure taken by bank<br>Lack knowledge of security skills by financial officers in banks<br>Lack of sufficient IT knowledge by bank support staff<br>Carelessness on the part of the customer service<br>lack of proper advice on internet banking security | Poor maintenance measures by users<br>Inadequate security measures taken by users<br>Lack of IT knowledge by users<br>Carelessness by users<br>Fear of uncertainty by users<br>Lack of security consciousness by users |
| **Service Providers** | **Hackers** |
| Poor maintenance of bank appliance<br>Porosity of internet leading to hacking by thieves<br>Poor power supply<br>Poor internet access<br>Lack of knowledge on the part of security agents in cases of mobile banking scams | Mobile Hacking and theft<br>Intelligent thieves who are smarter in IT than the average population |

Table A5: Idea Grouping

Nominal Group Technique Output

| SN | Objective | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Improve awareness on technology and information security | 2 | 2 | 4 | 5 | 5 | 18 |
| 2 | Understand familiar phone hackers' mode of operation | 1 | 4 | 5 | 4 | 4 | 18 |
| 3 | Understand consumer compliant process | 4 | 1 | 1 | 1 | 3 | 10 |
| 4 | Take responsibility for basic level phone security | 3 | 5 | 3 | 3 | 2 | 16 |
| 5 | Capacity building of mobile money operation staff | 5 | 3 | 2 | 2 | 2 | 13 |

Table A6: Nominal Group Technique Output

**Banked: Mobile Banking/Payment Account Holders**

**Participant Profile**

All participants had functional bank account in addition:

2 were Mobile Banking use, 3 were both Mobile Banking and Mobile Payment users

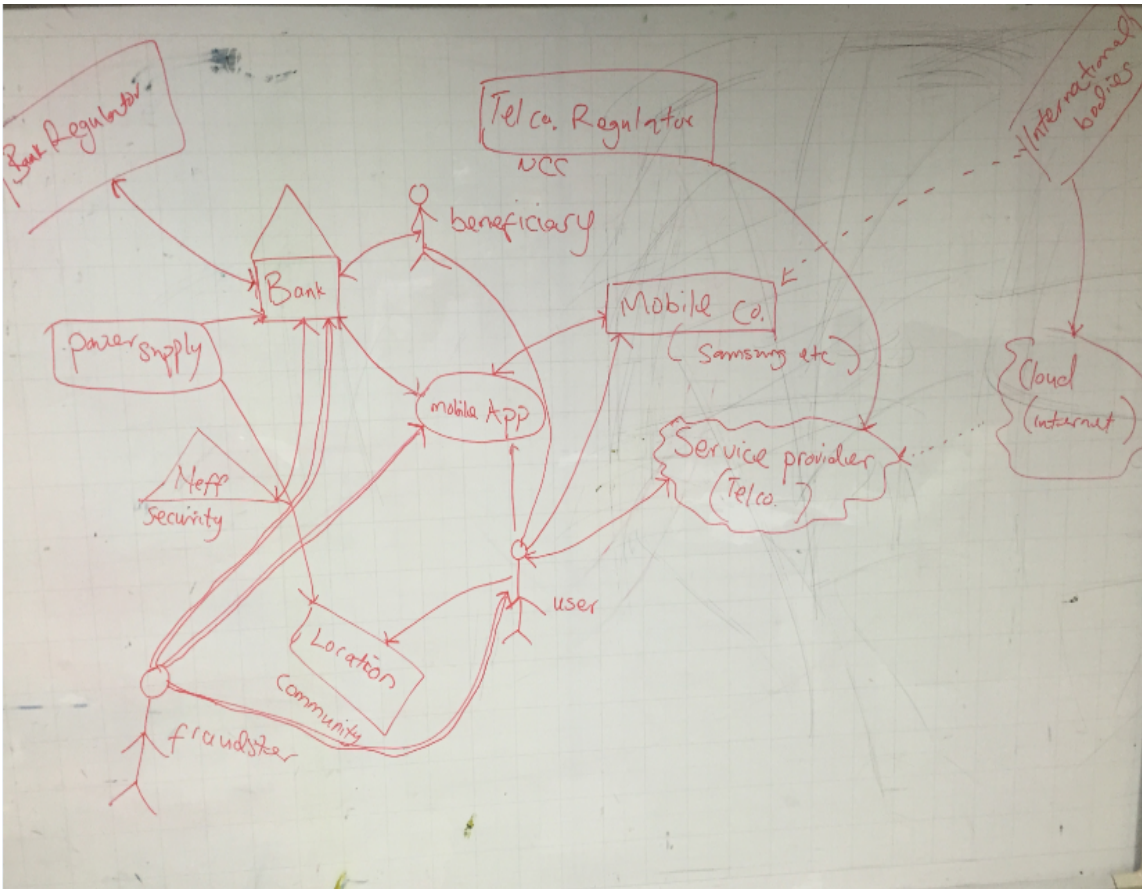



Figure A7: Rich Picture “Banked” group

**Root Definition:**

An effective alternative banking channel that will not add additional demand of the customer or expose customer to threat of financial loss

C: Customer

A: Banks, Agents

T: Additional Banking channel

W: Mobile Banking/Payment is an additional payment channel

O: Banks

E: Mobile Banking and Payment

The final task for the soft system approach was for the group to come up with a conceptual model based on the root definition. Figure below shows the model.

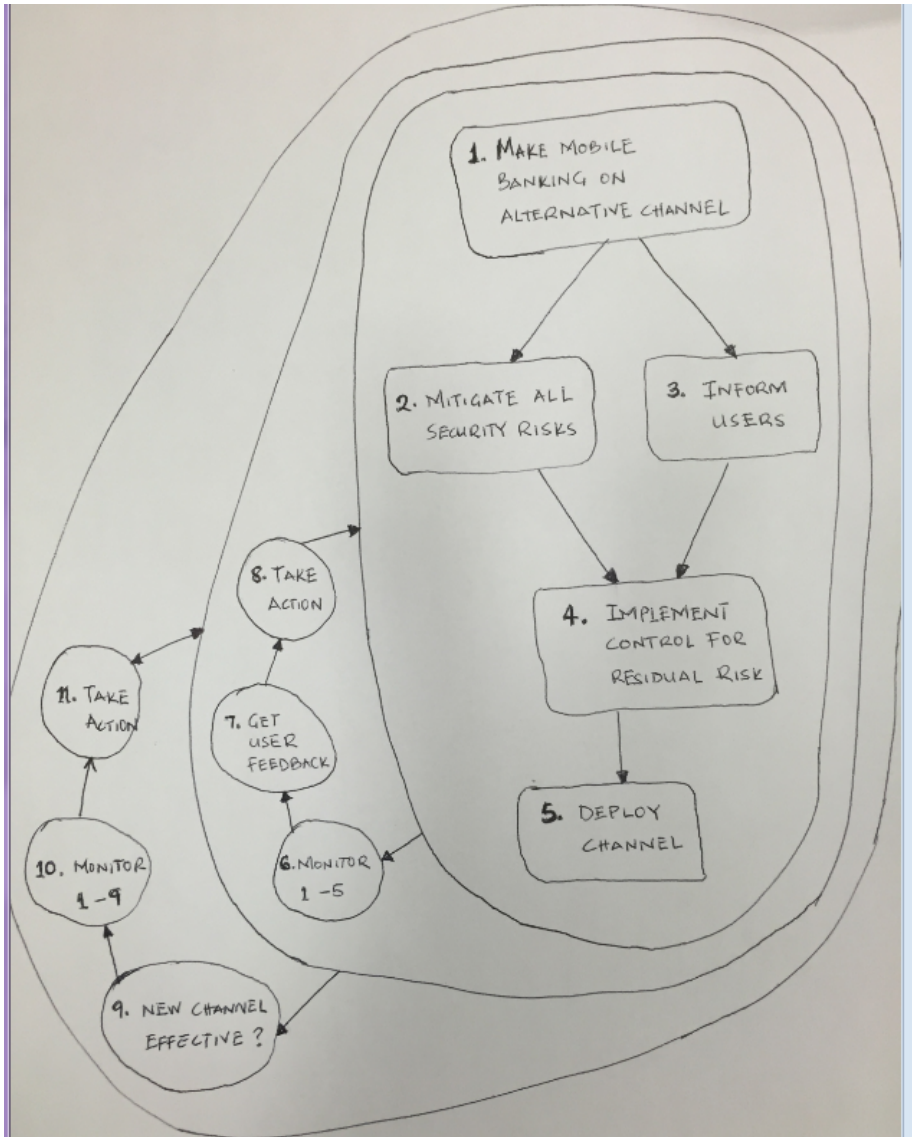



Figure A8: Conceptual Model “Banked” holder

IW Output

P1:

1. Negligence by users
2. Lack of knowledge of technology

3. Using weak passwords and other login credentials
4. Unwillingness/resistance to change
5. Poor feedback from Banks and service provider on fraud related concerns
6. Lack of trust on technology
7. Lack of understanding of mobile banking
8. Fear of the unknown as the value chain of who and who us really involved in mobile payment and mobile banking is not clear

P2:

1. Lack of knowledge of mobile banking by users
2. Lack of sufficient knowledge on mobile banking by bank support staff
3. Lack of security awareness by users
4. Poor infrastructure power/internet
5. Malicious intent from hackers
6. Poor quality of internet service
7. Lack of seamless integration with other services
8. Lack of frequent update of system infrastructure; apps, OS etc
9. System unavailability concerns
10. Lack of seamless integration within system might open loopholes for fraudsters
11. Little or not sufficient campaign by Banks of Mobile Banking
12. Lack of trust on banking on mobile phone
13. Need to share phone with others might compromise security

P3:

1. Lack of awareness on password protection
2. Lack of awareness on how to create strong passwords
3. Lack of awareness on password management

4. Poor network connectivity
5. Lack of user-friendly mobile apps
6. Lack of awareness on mobile banking security by banks
7. Funds sent by users not reaching recipient because of service failure, eroding confidence in the system
8. Resistance to change by users
9. Poor management of phones by users
10. Unsolicited messages to phones make users to be doubtful of real communications from agents
11. Unexplained charges by banks causing fear of more charges if one uses mobile channel

P4:

1. Lack of user education on password protection policies
2. Lack of appropriate security measures by service providers
3. Too many service providers
4. Lack of detailed investigation in existing fraud situation
5. Power supply downtime leading to cyber threat
6. Lack of trust in mobile banking app
7. Need to remember USSD codes for payment
8. Lack of secure platform by service providers
9. Lack of technical know-how by service providers
10. Lack of support from government in providing enable legislation to protect users
11. Poverty making most people in the rural areas not able to afford smart phone, using feature phone and living with the risk

P5:

1. Loss of phones while not locked

2. Lack of tokens for mobile payment
3. Privacy worries by users
4. Poor network
5. Lack of readiness for uptake of new technology product by users
6. Increased banking demand on users and need to learn new technology at the same time
7. Resistance to change by users
8. Lack of adequate security measures by bank to assure users of safety of transaction
9. Inadequate security measures by service providers
10. Lack of technical know-how by bank customer services
11. Lack security awareness by banks and users

Idea Grouping

| **Customer** | **Bank/Regulator** |
|---|---|
| Negligence by users<br>Lack of knowledge of technology<br>Using weak passwords and other login credentials<br>Unwillingness/resistance to change<br>Lack of trust on technology<br>Lack of understanding of mobile banking<br>Fear of the unknown<br>Need to share phone with others might compromise security<br>Resistance to change by users<br>Poor management of phones by users<br>Loss of phones while not locked | Poor feedback from Banks and service provider on fraud related concerns<br>Lack of sufficient knowledge on mobile banking by bank support staff<br>Lack of seamless integration within system might open loopholes for fraudsters<br>Poor infrastructure<br>Malicious intent from hackers<br>Unexplained charges by banks causing fear of more charges if one uses mobile channel<br>Too many service providers<br>Lack of support from government<br>Privacy worries by users |
| **Mobile Money Operator** | **Mobile Network Operator** |
| System unavailability concerns<br>Lack of security awareness by users<br>Lack of user-friendly mobile apps<br>Lack of secure platform by service providers | Poor quality of internet service<br>Unsolicited messages to phones |

| | |
|---|---|
| | |

Table A8: Idea Grouping

Nominal Group Technique Output

| SN | Issues | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Improve Lack of users education on password management | 4 | 3 | 1 | 4 | 2 | 14 |
| 2 | Banks to provide assurance of adequacy of security measure | 5 | 4 | 2 | 2 | 3 | 16 |
| 3 | Understand Security put in place for Mobile Banking to improve trust in the process | 3 | 5 | 3 | 5 | 4 | 20 |
| 4 | Be open to change | 2 | 2 | 5 | 3 | 5 | 17 |
| 5 | Improve awareness on technology | 1 | 1 | 4 | 1 | 1 | 8 |

Table A9: Nominal Group Technique Output

**CERT/Incidence Management**

**Participant Profile**

5. 1 CERT Member
6. 1 FS CERT Member
7. 1 Judiciary –Legal Expert
8. 1 IT Security Expert
9. 1 Consumer Protection Expert

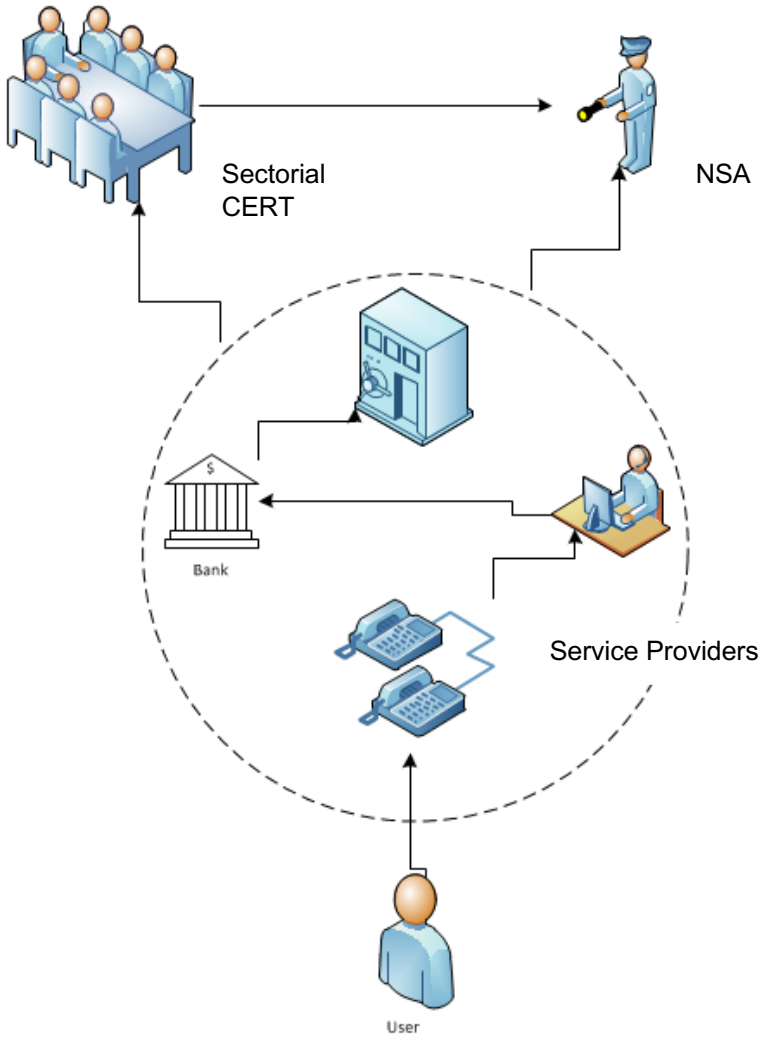



Figure A10: Rich Picture CERT

**Root Definition:**

An industry wide user awareness programme, delivered by the industry, in other to ensure support personnel and end-users have basic awareness of cybersecurity concerns in mobile financial services and how they can help to mitigate it.

C: Entire Financial Services industry and end-users

A: Banks, Financial Services regulators, Mobile Money Operators

T: Identify skill gap and deliver appropriate awareness programme

W: Education support staff and end-users on cybersecurity threat will mitigate cyber security risks in mobile banking

O: CERT

E: Financial Services sector

**Conceptual Model:**

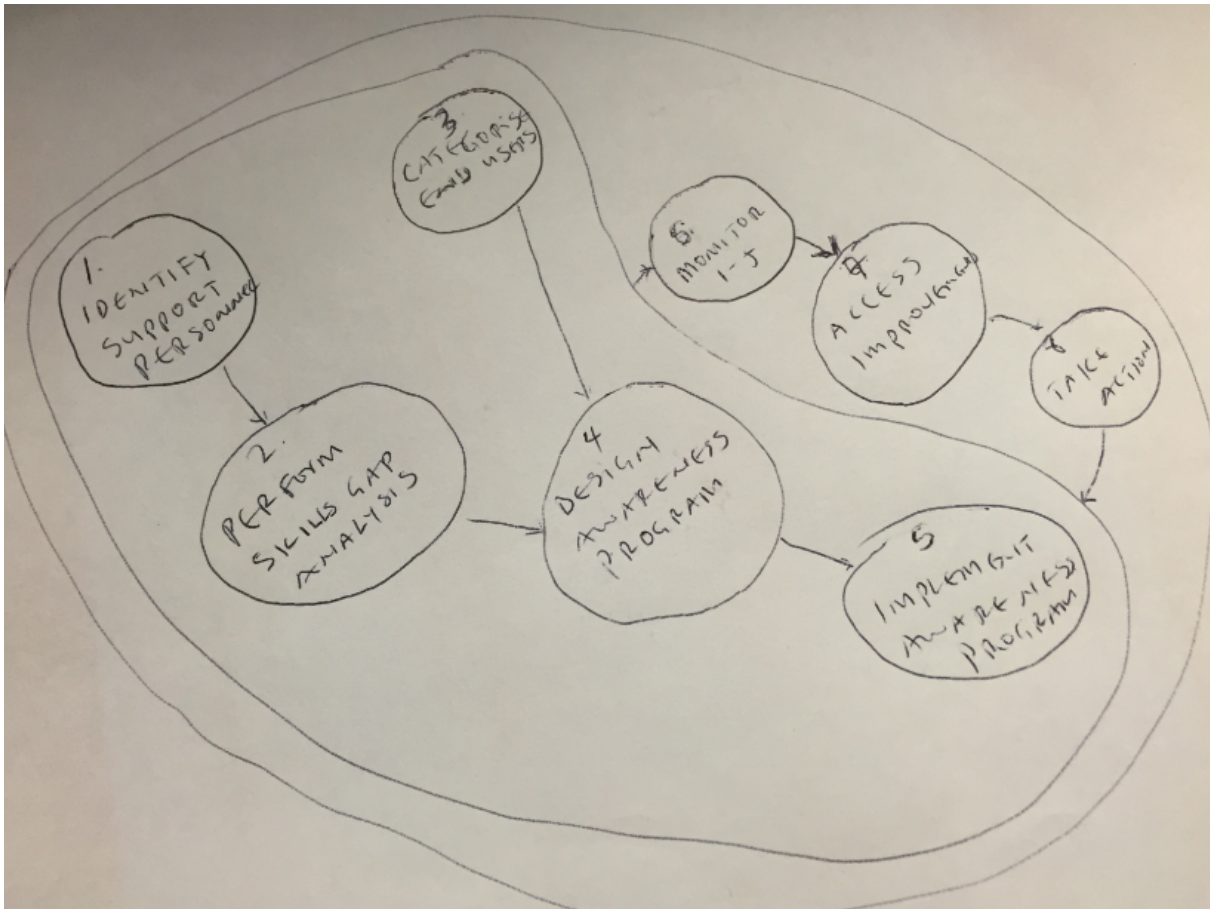



Figure A11: CM by CERT Group

IW Output by CERT Group

P1 FS CERT

1. Gaps in the existing cybersecurity Act
2. Lack of good pedigree of conviction or apprehension of cybercriminals
3. Frustrating legal process for trails of cybercrime suspected
4. Lack of knowledge of existence of industry fraud desks
5. Lack of industry fraud desks in some industries
6. Lack of effective centralization of incident management
7. Lack of expertise on incident management

8. Insufficient incidence management skills
9. Lack of functional fraud reporting platform

P2 (Judiciary)

1. Intangible nature of electronic evidences
2. Lack of durability of some printed evidences
3. Lack of sufficient storage capacity of mobile phones  make investigation into data of past years difficult
4. Difficulty in managing chain of custody in  mobile
5. Challenges with cross border laws in Information Technology
6. Lack of sufficient skills for Mobile based fraud by lawyers
7. Skill gaps in judges
8. Gaps in cybersecurity strategy

P3 Tech CERT

1. Duplication of effort within agencies in managing cybersecurity incidences
2. Disparate reporting framework for managing cybersecurity incidences
3. Lack of skilled human resources in managing cyber incidences
4. Lack of cybersecurity helpdesk by most telcos
5. Customer care staff not satisfactorily handling reported cybersecurity incidences
6. Lack of sectorial CERT for telco and banking
7. Current cybersecurity act too centralised
8. Lack of enforcement of existing polices
9. Lack of awareness
10. Lack of proper coordination of cyber incidence management
11. Lack of cybersecurity skills by IT personnel

P4 (Security)

1. Lack of interoperability between payment schemes
2. Lack of end-to-end payment process
3. Some scheme operators obtaining license before perfecting process
4. Low product adoption due to lack of trust
5. Lack of interoperability at merchants points of sale
6. Lack of awareness of who to escalate a cybercrime incidence to
7. Infrastructure instability causing time lag between reporting incidence and response from responsible parties
8. Lack of fit for purpose awareness programme
9. Legal limitations

P5 (CP)

1. Lack of awareness of consumer rights
2. Lack of reporting of incidences by consumers
3. Lack of resolution of cyber incidences issues logged
4. Time lag between logging and resolving incidences
5. Lack of understanding of the role of stakeholders in consumer protection and management
6. Fraudulent incident reporting
7. False alarms

Grouping of Issues

| **Process** | **People** |
|---|---|
| Gaps in the existing cybersecurity Act<br>Lack of good pedigree of conviction or apprehension of cybercriminals<br>Frustrating legal process for trails of cybercrime suspected | Lack of expertise on incident management<br>Insufficient incidence management skills<br>Lack of sufficient skills for Mobile based fraud by lawyers<br>Skill gaps in judges |

| | |
|---|---|
| Lack of knowledge of existence of industry fraud desks<br>Lack of industry fraud desks in some industries<br>Lack of effective centralization of incident management<br>Gaps in cybersecurity strategy<br>Duplication of effort within agencies in managing cybersecurity incidences<br>Disparate reporting framework for managing cybersecurity<br>Lack of cybersecurity helpdesk by most telcos<br>Lack of sectorial CERT for telco and banking<br>Current cybersecurity act too centralised<br>Lack of enforcement of existing polices<br>Lack of proper coordination of cyber incidence management<br>Lack of end-to-end payment process<br>Some scheme operators obtaining license before perfecting<br>Lack of fit for purpose awareness programme<br>Legal limitations<br>Lack of reporting of incidences by consumers<br>Lack of resolution of cyber incidences issues logged<br>Time lag between logging and resolving incidences | Lack of skilled human resources in managing cyber incidences<br>Customer care staff not satisfactorily handling reported cybersecurity<br>Lack of awareness<br>Lack of cybersecurity skills by IT personnel<br>Low product adoption due to lack of trust<br>Lack of awareness of who to escalate a cybercrime incidence<br>Lack of awareness of consumer rights<br>Lack of understanding of the role of stakeholders in consumer protection and management<br>Fraudulent incident reporting<br>False alarms |
| **Technology** | |
| Lack of functional fraud reporting platform<br>Intangible nature of electronic evidences<br>Lack of durability of some printed evidences<br>Lack of sufficient storage capacity of mobile phones make investigation into data of past years difficult<br>Difficulty in managing chain of custody in mobile phones<br>Challenges with cross border laws in Information Technology | |

| | |
|---|---|
| Lack of interoperability between payment schemes<br><br>Infrastructure instability causing time lag between reporting incidence and response from responsible parties | |

Table A10: Grouping of Issues

Nominal Group Technique Output

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Develop and implement a fit for purpose user awareness programme | 1 | 3 | 5 | 1 | 5 | 15 |
| 2 | Revise current cybersecurity act with input from all key stakeholders | 3 | 4 | 4 | 4 | 1 | 16 |
| 3 | Setup sectorial CERTS | 2 | 1 | 2 | - | - | 5 |
| 4 | Setup cybercrime help desks in all Banks and telco | - | - | 1 | 3 | 4 | 8 |
| 5 | Develop capacity building programme on cybersecurity for all key players | 4 | 5 | 3 | 2 | 2 | 16 |
| 6 | Setup a Risk and Incidence Response Centre | 5 | 2 | - | 5 | 3 | 15 |

Table A11: Nominal Group Technique Output

**Service Provider Group**

**Participant Profile**

1. 1 Telco Regulator
2. 1 Mobile Money Operator
3. 1 Broadband Service Provider
4. 1 Network Service provider
5. 1 Telco Head of IT

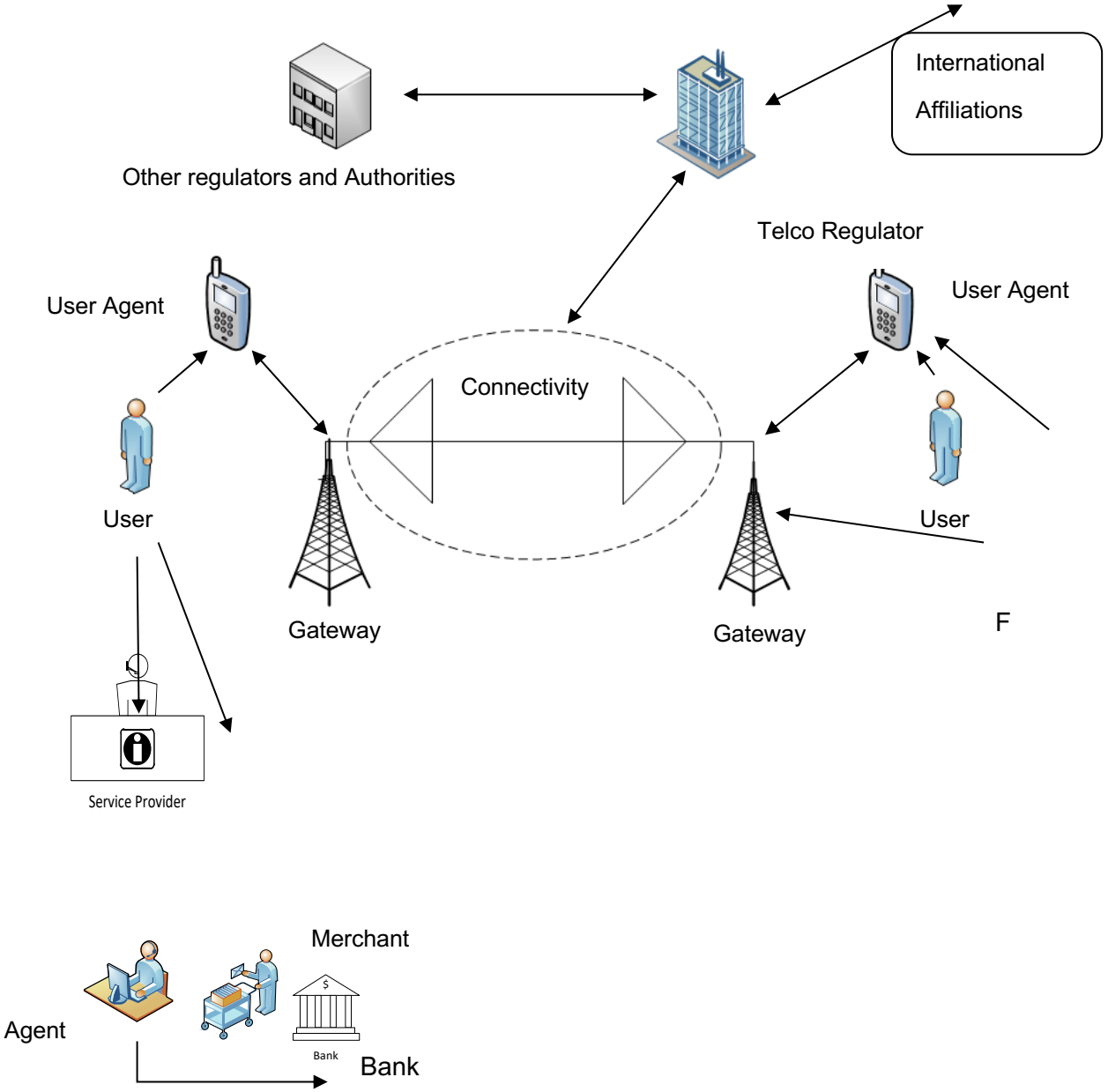



Figure A12: Rich Picture Service Providers

**Root Definition:**

Implement an approach that will ensure performance standards for every service provider is defined, measured and complied with. This will help reduce possible risk introduced by service providers in the ecosystem and further reduce threat of cybercrime.

C: Financial Services Regulator

A: All service providers

T: Implement standards for service providers

W: Well defined and measured standards for service providers will reduce the risk of cyber crime

O: Regulator

E: Mobile Financial Services ecosystem

**Conceptual Model:**

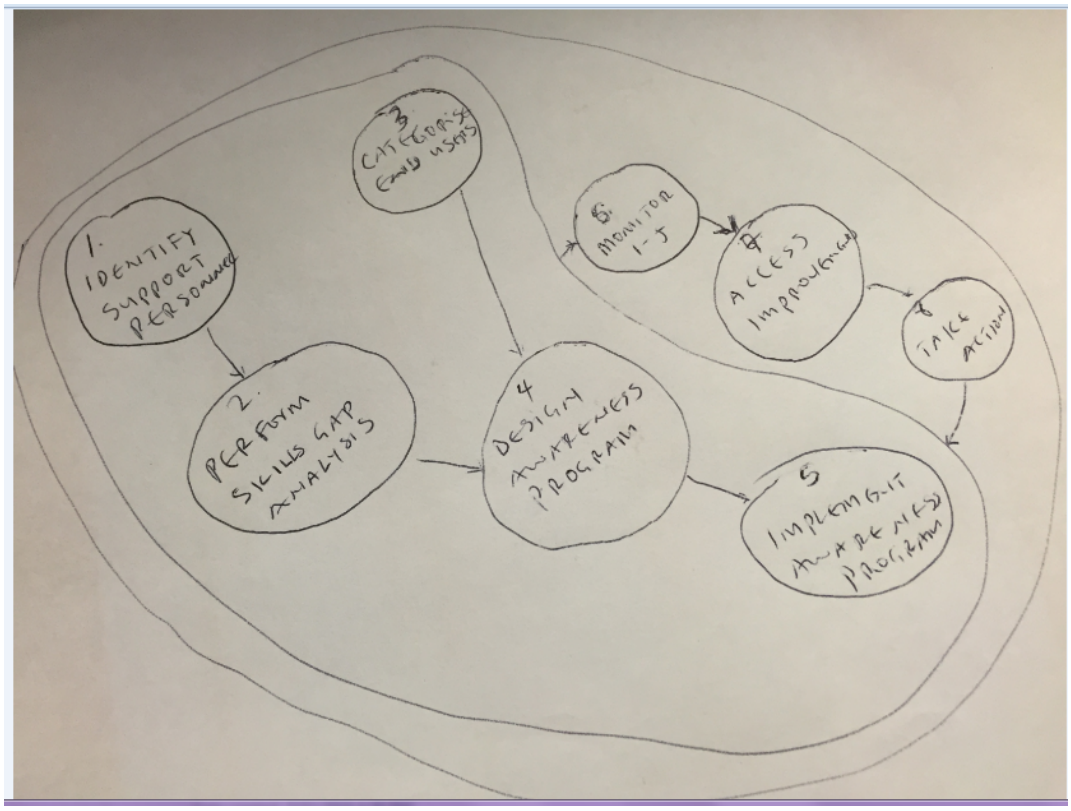



Figure A13: CM by Service Provider Group

IW Output by SP Group

P1 Broadband Service Provider

1. Lack of involvement of stakeholders in incident management
2. Lack of awareness
3. Lack of understanding of technology
4. Legal limitations
5. Lack of security awareness
6. Lack of sufficient government support
7. Infrastructural challenges

8. Poor coverage of network infrastructure in some areas
9. Poor management of telco facility due to political instability in certain areas

P2 Telco IT Head

1. Lack of infrastructure
2. Pressure on existing facility
3. Missing phones
4. Lack of proper phone security
5. Lack of enlightenment by users
6. Lack of proper security of information in transit
7. Social media exposing critical personal data
8. Trade-off between security and profitability by service providers
9. Only big fraud gets big attention
10. Lack of incident reporting
11. Lack of feedback on complaints
12. Lack of functional dispute resolution process
13. Cultural issues with money
14. Poor hand shake between transaction
15. Regulatory challenges
16. Lack of proper identity management
17. Lack of compliance
18. Lack of enforcement
19. Lack of trust due to bad perception and bad previous experiences
20. No proper investigation
21. Delay in investigation

P3 (Mobile Money Operator)

1. Lack of proper security measure by users
2. Fraudsters masquerading as customer care
3. Spam SMS
4. Conflicting government policies
5. Poor Telco service quality
6. Telco divesting into various business lines giving mobile money less quality of service
7. Uncompleted transactions
8. Delayed transactions
9. Fraudulent SMS alerts

P4 Telco Regulator

1. Lack of capacity to ensure telco compliance
2. Poor quality of service by telcos
3. Rogue mobile apps
4. Delay in transmission of transaction
5. Competing services by telcos
6. Insider abuse
7. Risk of fibre cuts
8. Risks of wiretaps
9. High cost of upgrading infrastructure by telcos
10. Risk of phone loss

P5 (Network SP)

1. Non assurance that all redundant access rules on the security appliance are eliminated and constant review of access rules are strictly implemented.

2. Standard High Availability (HA) Designs should be employed while deploying the Access authentication system on the network infrastructure.
3. Improper identification / creation of access and service ports on the security and network infrastructure could provide a leeway for malicious attack.
4. Deployment of network infrastructure that do not support or provide security features that are complaint with cybersecurity network best practice.
5. Absence or inadequate configuration for device and service session authentication on the network infrastructure.
6. Poor or lack of data encryption services across the network infrastructure being accessed by users and stakeholders.
7. Service access policies not applied in accordance with best practice or enterprise standards.
8. Weak identity management process as well as the absence of robust audit log services on the network infrastructure being access by mobile/remote users.
9. Lack of national policy and guidelines for cybersecurity in the financial industry;
10. Lack of national threat response strategy for cyber-attacks to avoid a system cybersecurity attack in the financial industry.

Grouping of Issues

| **Producer** | **Channel** |
|---|---|
| Lack of involvement of stakeholders in incident management | Infrastructural challenges |
| Legal limitations | Poor coverage of network infrastructure in some areas |
| Lack of sufficient government support | Poor management of telco facility due to political instability in certain areas |
| Trade-off between security and profitability by service providers | Lack of infrastructure |
| Only big fraud gets big attention | Pressure on existing facility |
| Lack of incident reporting | Lack of proper security of information in transit |
| Lack of feedback on complaints | Poor hand shake between transaction |
| Lack of functional dispute resolution process | Spam SMS |
| Regulatory challenges | Lack of capacity to ensure telco compliance |
| Lack of proper identity management | Poor quality of service by telcos |
| Lack of compliance | Rogue mobile apps |
| Lack of enforcement | Delay in transmission of transaction |
| No proper investigation | Competing services by telcos |
| Delay in investigation | |

| | |
|---|---|
| Conflicting government policies<br>Poor Telco service quality<br>Telco divesting into various business lines giving mobile money less quality of service<br>Uncompleted transactions<br>Delayed transactions<br>Fraudulent SMS alerts<br>Insider abuse<br>Lack of national policy and guidelines for cybersecurity in the financial industry;<br>Lack of national threat response strategy for cyber-attacks to avoid a system cybersecurity attack in the financial industry. | Risk of fibre cuts<br>Risks of wiretaps<br>High cost of upgrading infrastructure by telcos<br>Non assurance that all redundant access rules on the security appliance are eliminated and constant review of access rules are strictly implemented.<br>Standard High Availability (HA) Designs should be employed while deploying the Access authentication system on the network infrastructure.<br>Improper identification / creation of access and service ports on the security and network infrastructure could provide a leeway for malicious attack.<br>Deployment of network infrastructure that do not support or provide security features that are complaint with cybersecurity network best practice.<br>Absence or inadequate configuration for device and service session authentication on the network infrastructure.<br>Poor or lack of data encryption services across the network infrastructure being accessed by users and stakeholders.<br>Service access policies not applied in accordance with best practice or enterprise standards.<br>Weak identity management process as well as the absence of robust audit log services on the network infrastructure being access by mobile/remote users. |
| **Consumer** | |
| Lack of awareness<br>Lack of understanding of technology<br>Lack of security awareness<br>Missing phones<br>Lack of proper phone security<br>Lack of enlightenment by users<br>Social media exposing critical personal data<br>Cultural issues with money<br>Lack of trust due to bad perception and bad previous experiences<br>Lack of proper security measure by users | |

| | |
|---|---|
| Fraudsters masquerading as customer care<br>Risk of phone loss | |

Table A12: Grouping of Issues

Nominal Group Technique Output

| SN | Objectives | P1 | P2 | P3 | P4 | P5 | Total |
|---|---|---|---|---|---|---|---|
| 1 | Ensure every service provider has a business continuity strategy | 3 | 4 | 2 | 3 | 4 | 16 |
| 2 | Define minimum performance and availability level for all service providers | 1 | 3 | 3 | 5 | 3 | 15 |
| 3 | Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers | 2 | 5 | 1 | 4 | 5 | 17 |
| 4 | Develop end-to-end process on complaint management | 4 | 1 | 5 | 2 | 1 | 13 |
| 5 | Educate client on cybersecurity | 5 | 2 | 4 | 1 | 2 | 14 |

Table A13: Nominal Group Technique Output

Total Issues 103

Issues 166 +103= 269 = 9/P

Interpretive Structural Modelling

| SN | Objectives |
|---|---|
| 1 | Setup an industry wide cybersecurity operations centre (O1) |
| 2 | Mitigate risk associated with poor infrastructure (e.g. power, internet, technology) (O2) |
| 3 | Implement robust awareness programme on social engineering for users (O3) |
| 4 | Enforce segregation of duty in Banks to minimise possibility of insider abuse(O4) |
| 5 | Improve awareness on technology and information security(O5) |
| 6 | Understand familiar phone hackers' mode of operation(O6) |
| 7 | Understand Security put in place for Mobile Banking to improve trust in the process(O7) |
| 8 | Be open to change (O8) |
| 9 | Revise current cybersecurity act with input from all key stakeholders(O9) |
| 10 | Develop capacity building programme on cybersecurity for all key players (O10) |
| 11 | Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers (O11) |

| | |
|---|---|
| 12 | Ensure every service provider has a business continuity strategy (O12) |

Table A14: interpretive Structural Model

Top 2 NGT Output for Each group

| SN | Objectives |
|---|---|
| 1 | Setup an industry wide cybersecurity operations centre (O1) |
| 2 | Mitigate risk associated with poor infrastructure (e.g. power, internet, technology) (O2) |
| 3 | Implement robust awareness programme on social engineering for users (O3) |
| 4 | Enforce segregation of duty in Banks to minimise possibility of insider abuse(O4) |
| 5 | Improve awareness on technology and information security(O5) |
| 6 | Understand familiar phone hackers' mode of operation(O6) |
| 7 | Understand Security put in place for Mobile Banking to improve trust in the process(O7) |
| 8 | Be open to change (O8) |
| 9 | Revise current cybersecurity act with input from all key stakeholders(O9) |
| 10 | Develop capacity building programme on cybersecurity for all key players (O10) |
| 11 | Ensure adequate investment in cybersecurity is imbedded in the strategy of service providers (O11) |
| 12 | Ensure every service provider has a business continuity strategy (O12) |

Table A15: Top 2 NGT Output for Each group

2. Relationship

| | O12 | O11 | O10 | O9 | O8 | O7 | O6 | O5 | O4 | O3 | O2 | O1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O1 | V | V | V | O | O | O | O | O | O | O | A | X |
| O2 | A | A | O | O | O | O | A | O | O | O | X | |
| O3 | O | A | A | O | X | O | A | A | V | X | | |
| O4 | O | O | O | O | A | O | O | A | X | | | |
| O5 | O | A | X | O | A | X | V | X | | | | |
| O6 | O | O | A | O | O | V | X | | | | | |
| O7 | O | O | A | O | A | X | | | | | | |
| O8 | O | V | O | X | X | | | | | | | |
| O9 | V | V | V | X | | | | | | | | |
| O10 | O | A | X | | | | | | | | | |
| O11 | X | X | | | | | | | | | | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O12 | X | | | | | | | | | | | |

Table A16: ISM Relationships

3. Reachability

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | O | 0 | 1 | 1 | 1 |
| O2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| O3 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| O4 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| O5 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| O6 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| O7 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| O8 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| O9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| O10 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| O11 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |
| O12 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |

Table A17: ISM Reachability Matrix

4. Transitive

| | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| O2 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| O3 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| O4 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| O5 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| O6 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| O7 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 |
| O8 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| O9 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| O10 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 |
| O11 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| O12 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |

Table A18: ISM Transitive Matrix

5. Levels

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,2,3,5,6,7,9,10,11,12 | 1,2,6,11,12 | 1,2,6,11,12 | |
| O2 | 1,2 | 1,2,5,6,9,11,12 | 1,2 | |
| O3 | 3,4,5,7,8,9,11 | 1,3,5,6,7,8,9,10,11,12 | 3,5,7,8,9,11 | |
| O4 | 4 | 3,4,5,6,1,8,9,10,11 | 4 | |
| O5 | 2,3,4,5,6,7,8,10 | 1,3,5,6,7,8,9,10,11,12 | 3,5,6,7,8,10 | |
| O6 | 1,2,3,4,5,6,7,8 | 1,5,6,7,8,9,10,11 | 1,5,6,7,8 | |
| O7 | 3,4,5,6,7,10 | 1,3,5,6,7,8,9,10,11 | 3,5,6,7,10 | |
| O8 | 3,4,5,6,7,8,9,10,11 | 3,5,6,8,9,10,11 | 3,5,6,8,9,10,11 | |
| O9 | 2,3,4,5,6,7,8,9,10,11 | 1,3,8,9 | 3,8,9 | |
| O10 | 3,4,5,6,7,8,10 | 1,5,7,8,9,10,11,12 | 5,7,8,10 | |
| O11 | 1,2,3,4,5,6,7,8,10,11 | 1,3,8,9,11,12 | 1,3,8,11 | |
| O12 | 1,2,3,5,10,11,12 | 1,8,9,11,12 | 1,11,12 | |

Table A19: ISM Level 1

Iteration 1 Level 1=2,4

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,2,3,5,6,7,9,10,11,12 | 1,2,6,11,12 | 1,2,6,11,12 | |
| O2 | 1,2 | 1,2,5,6,9,11,12 | 1,2 | i |
| O3 | 3,4,5,7,8,9,11 | 1,3,5,6,7,8,9,10,11,12 | 3,5,7,8,9,11 | |
| O4 | 4 | 3,4,5,6,1,8,9,10,11 | 4 | I |
| O5 | 2,3,4,5,6,7,8,10 | 1,3,5,6,7,8,9,10,11,12 | 3,5,6,7,8,10 | |
| O6 | 1,2,3,4,5,6,7,8 | 1,5,6,7,8,9,10,11 | 1,5,6,7,8 | |
| O7 | 3,4,5,6,7,10 | 1,3,5,6,7,8,9,10,11 | 3,5,6,7,10 | |
| O8 | 3,4,5,6,7,8,9,10,11 | 3,5,6,8,9,10,11 | 3,5,6,8,9,10,11 | |
| O9 | 2,3,4,5,6,7,8,9,10,11 | 1,3,8,9 | 3,8,9 | |
| O10 | 3,4,5,6,7,8,10 | 1,5,7,8,9,10,11,12 | 5,7,8,10 | |
| O11 | 1,2,3,4,5,6,7,8,10,11 | 1,3,8,9,11,12 | 1,3,8,11 | |
| O12 | 1,2,3,5,10,11,12 | 1,8,9,11,12 | 1,11,12 | |

Table A20: ISM Iteration 1

Iteration 2 Level 2 =3,5,7

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,3,5,6,7,9,10,11,12 | 1,6,11,12 | 1,6,11,12 | |
| O3 | 3,5,7,8,9,11 | 1,3,5,6,7,8,9,10,11,12 | 3,5,7,8,9,11 | II |
| O5 | 3,5,6,7,8,10 | 1,3,5,6,7,8,9,10,11,12 | 3,5,6,7,8,10 | II |
| O6 | 1,3,5,6,7,8 | 1,5,6,7,8,9,10,11 | 1,5,6,7,8 | |
| O7 | 3,5,6,7,10 | 1,3,5,6,7,8,9,10,11 | 3,5,6,7,10 | II |
| O8 | 3,5,6,7,8,9,10,11 | 3,5,6,8,9,10,11 | 3,5,6,8,9,10,11 | |
| O9 | 3,5,6,7,8,9,10,11 | 1,3,8,9 | 3,8,9 | |
| O10 | 3,5,6,7,8,10 | 1,5,7,8,9,10,11,12 | 5,7,8,10 | |
| O11 | 1,3,5,6,7,8,10,11 | 1,3,8,9,11,12 | 1,3,8,11 | |
| O12 | 1,3,5,10,11,12 | 1,8,9,11,12 | 1,11,12 | |

Table A21: ISM Iteration 2

Iteration 3 Level 3 =6,8

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,6,9,10,11,12 | 1,6,11,12 | 1,6,11,12 | |
| O6 | 1,6,8 | 1,5,6,7,8,9,10,11 | 1,6,8 | iii |
| O8 | 6,8,9,10,11 | 6,8,9,10,11 | ,6,8,9,10,11 | iii |
| O9 | 6,8,9,10,11 | 1,8,9 | 8,9 | |
| O10 | 6,8,10 | 1,5,7,8,9,10,11,12 | ,8,10 | |
| O11 | 1,6,8,10,11 | 1,3,8,9,11,12 | 1,8,11 | |
| O12 | 1,10,11,12 | 1,8,9,11,12 | 1,11,12 | |

Table A22: ISM Iteration 3

Iteration 4 Level 4 =10

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,9,10,11,12 | 1,11,12 | 1,11,12 | |
| O9 | ,9,10,11 | 1,9 | ,9 | |
| O10 | ,10 | 1,9,10,11,12 | 10 | IV |
| O11 | 1,10,11 | 1,9,11,12 | 111 | |
| O12 | 1,10,11,12 | 1,9,11,12 | 1,11,12 | |

Table A23: ISM Iteration 4

Itineration 5 Level 5=11,12

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| O1 | 1,9,11,12 | 1,11,12 | 1,11,12 | |
| O9 | ,911 | 1,9 | ,9 | |
| O11 | 1,11 | 1,9,11,12 | 1,11 | V |
| O12 | 1,11,12 | 1,9,11,12 | 1,11,12 | V |

Table A24: ISM Iteration 5

Iteration 6 Level 6=9

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,9, | 1,11,12 | 1, | |
| O9 | ,9 | 1,9 | ,9 | VI |

Table A25: ISM Iteration 6

Iteration 7 Level 7= 1

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1, | 1,11,12 | 1, | VII |

Table A25: ISM Iteration 7

Summary Table

| Objective | Reachability Set | Antecedent set | Intersection Set | Level |
|---|---|---|---|---|
| O1 | 1,2,3,5,6,7,9,10,11,12 | 1,2,6,11,12 | 1,2,6,11,12 | vii |
| O2 | 1,2 | 1,2,5,6,9,11,12 | 1,2 | i |
| O3 | 3,4,5,7,8,9,11 | 1,3,5,6,7,8,9,10,11,12 | 3,5,7,8,9,11 | ii |
| O4 | 4 | 3,4,5,6,1,8,9,10,11 | 4 | i |
| O5 | 2,3,4,5,6,7,8,10 | 1,3,5,6,7,8,9,10,11,12 | 3,5,6,7,8,10 | ii |
| O6 | 1,2,3,4,5,6,7,8 | 1,5,6,7,8,9,10,11 | 1,5,6,7,8 | iii |
| O7 | 3,4,5,6,7,10 | 1,3,5,6,7,8,9,10,11 | 3,5,6,7,10 | ii |
| O8 | 3,4,5,6,7,8,9,10,11 | 3,5,6,8,9,10,11 | 3,5,6,8,9,10,11 | iii |
| O9 | 2,3,4,5,6,7,8,9,10,11 | 1,3,8,9 | 3,8,9 | vi |
| O10 | 3,4,5,6,7,8,10 | 1,5,7,8,9,10,11,12 | 5,7,8,10 | iv |
| O11 | 1,2,3,4,5,6,7,8,10,11 | 1,3,8,9,11,12 | 1,3,8,11 | V |
| O12 | 1,2,3,5,10,11,12 | 1,8,9,11,12 | 1,11,12 | V |

Table A26: ISM Iteration Summary

Graph with nodes

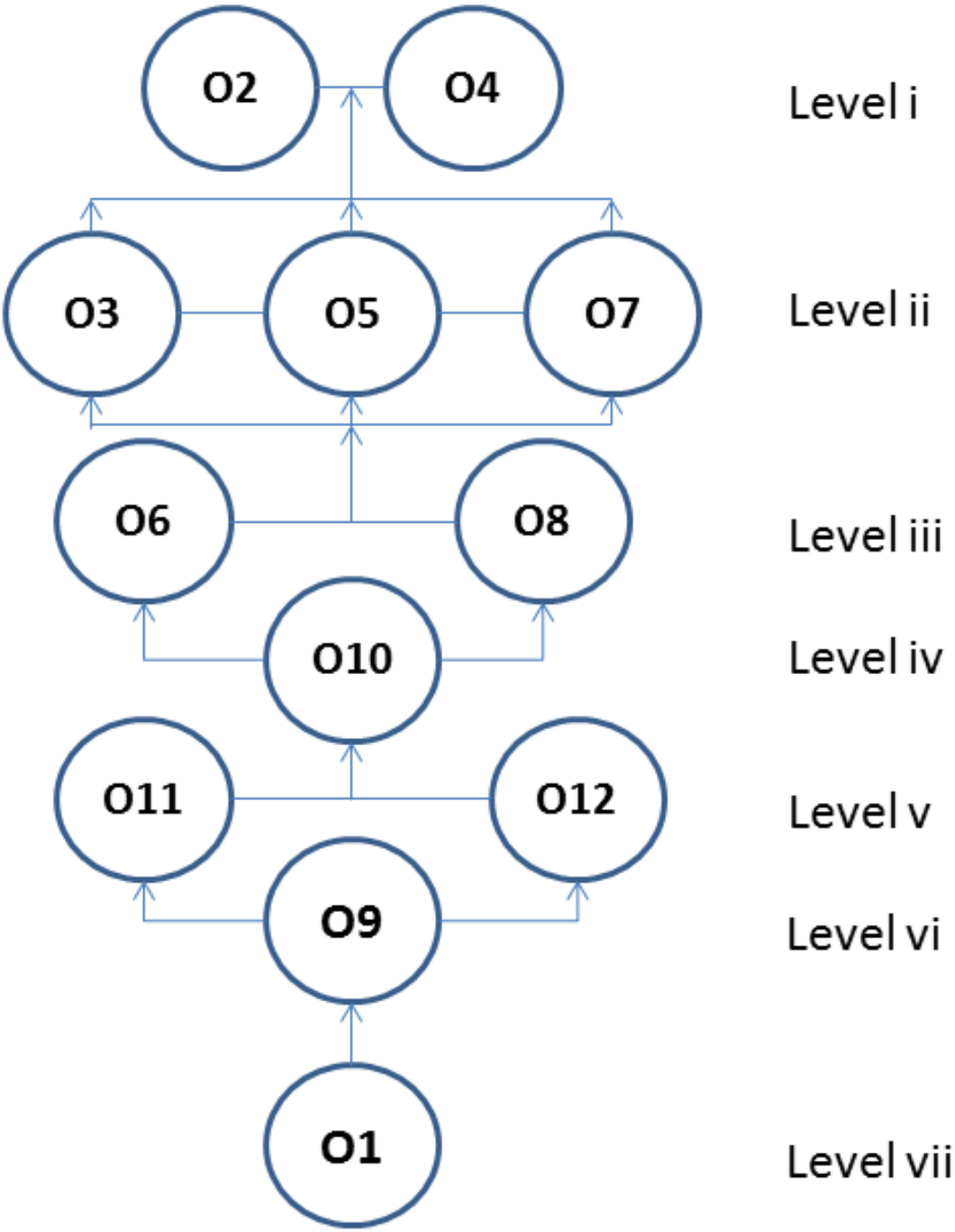



Figure A14: Graph Nodes

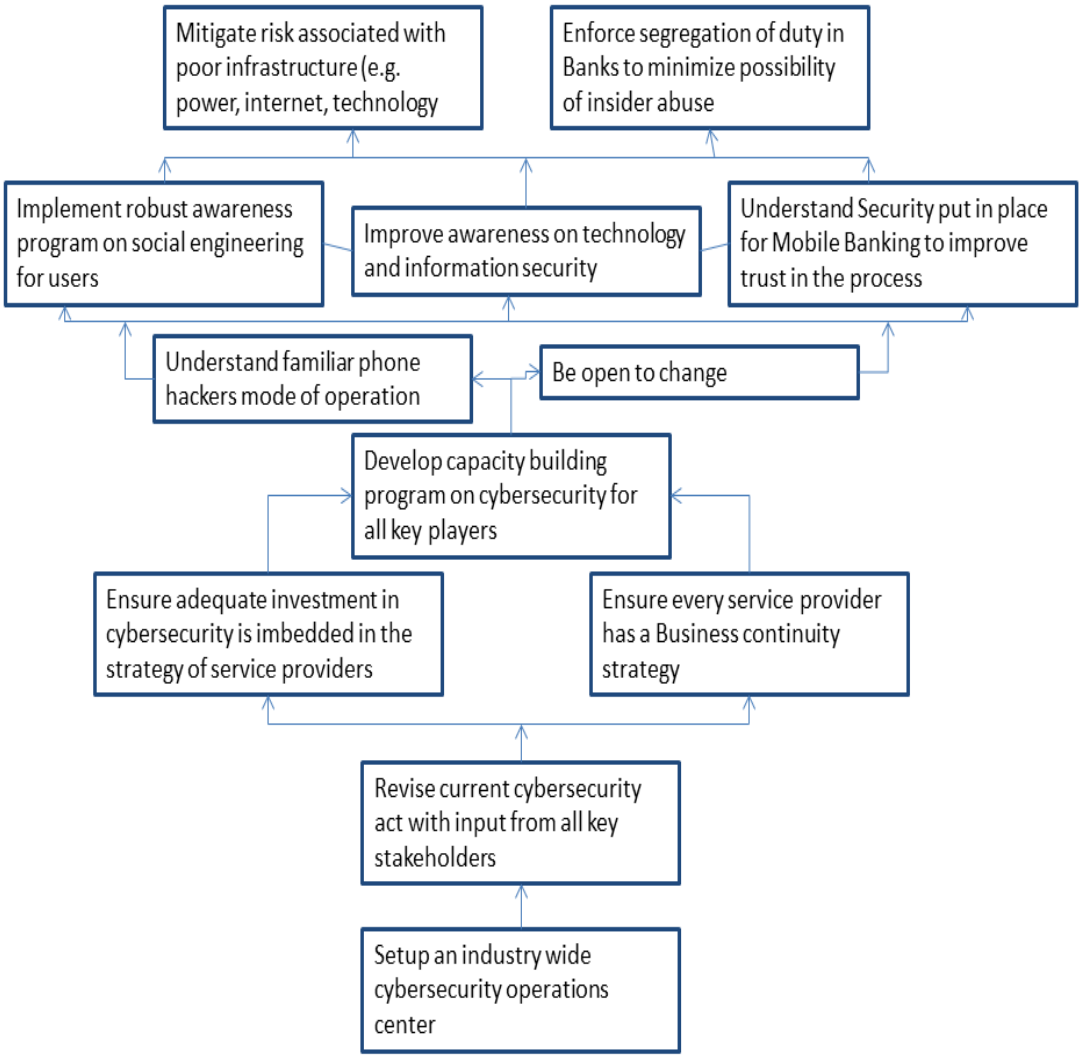



Figure A15: Graph with Objectives

# Appendix II: Usable Security User and DevOps Studies

**Usable Security User Survey Initial Analysis Output**

**Sample size**

The population size for the survey was approximately **50 million**, a sample size with **95% confidence level and 5% error rate** based on Cochran's formulas, the ideal sample size to satisfy the confidence level and error margin comes to **385**. However, supervisors agreed that a target sample size of **500** should be used**. A total of 698 responses** were obtained at the close of the survey.

**Survey tool**

The Bournemouth University licensed survey tool; Bristol Online Survey (BOS) was used to design the online survey. A paper-based survey was also designed using Microsoft Word.

The survey was distributed electronically via social media links (Facebook and WhatsApp) and emails and could be completed using a PC, tablet, or mobile phone. Hard copies of the survey were also deployed to participants who preferred to complete the survey manually.

**Survey Pilot**

The paper-based survey was piloted with 15 participants, while the online version was piloted with 7 participants. The purpose of the pilot was to obtain feedback on the content and time demand for survey completion and to also test the survey logic. Paper-based participants completed the survey in an average of 11 minutes, while online participants completed the survey in an average of 9 minutes. This pilot was in addition to the detailed review of the content and structure of the questionnaires by the PGR supervisory team over 3 months.

Survey Feedback

The survey ran for 2 months. At the end of the survey, **698 participants** completed the survey. 328 responses were obtained via electronic channels. While 370 paper-based surveys were completed and returned. In the design of the online survey, a control was set to ensure only Mobile Financial Services Users completed the survey. Non-users instead of just exiting were directed to a short survey that examined why they do not use an MFS and what changes would make them use one. 29

respondents out of the 328 fell in this category. 53 of the paper-based responses had a large number of questions unanswered. A total of **616 participants** were eventually analysed.

**Survey Background**

The survey was analysed using the Bristol Online survey, SPSS statistical package, and Microsoft Excel 2016.

The 1st step in the survey was to clean the survey data. The deployed survey had 43 questions, however, due to multiple choice options and the 'others' option in some questions a total of 106 variables were generated. The clean-up focused on 8 questions that gave participants the option of selecting more than one option in a question. For Instance, a participant might use both an Apple phone and a Samsung phone to access MFS. Also, a participant could use more than one MFS service etc. These various combinations needed to be accounted for in the data. At the end of the exercise, 65 clean variables were obtained.

The survey had 8 sections as follows:

**Participants details**

This section had 5 questions that sought to understand the age, income, and educational level of **participants along with employment status and type of employment.**

Product Type and Means of Use:

This section gathered information on phone type, MFS type, and means of access to the MFS product.

**Experience**

The section has five questions that seek to obtain feedback from user frustration levels. Based on the complexity or ease of use of the products.

Awareness

The awareness section measures the awareness of privacy, products, roles, and responsibilities of participants on the system they use

Maintenance

This section sought to understand user behaviour as regards basic application and phone housekeeping tasks and how it impacts security and usability

Usability

This section gauges user perception on various elements of usability of the MFS

Security

This section sought to understand user perception of confidentiality, integrity, and availability of this system

Social Context

The last section examines how trust and environmental issues might impact on usable security.

Stand out Questions

A couple of standout questions were included to measure perception versus actual. Questions were asked to gather information on participant whose MFS have been compromised in the past and their use behaviours. An 'additional feedback' section was added to capture any other thoughts.

In addition to analysing responses to individual questions, this analysis would benefit from an aggregate user view for 6 of the 8 categories above. For instance, instead of just gauging a participant's perception of confidentiality as a measure of security, an aggregated view of a participant's perception on a combination of confidentiality, integrity, and availability would provide a more circumspect view on security. As such, each of the 6 sections (awareness, maintenance, usability security, and social context were aggregated and added as additional variables). The 1st 2 sections; 'participant's details' and 'product type' cannot be aggregated because the questions in the sections are not related but seek to measure independent aspect of product and product usage.

The description of the compound variables is as follows:

| SN | Compound variable | Measures | Value |
|---|---|---|---|
| 1 | Experience | Systems (phone + product) Complexity | Complex, neutral, easy |
| 2 | Awareness | Privacy | High or Low |

| | | | |
|---|---|---|---|
| 3 | Maintenance | Understanding relationship between updates and security/privacy | Yes or No |
| 4 | Usability | Satisfaction with usability attributes | Satisfied, partially satisfied, not satisfied |
| 5 | Security | Satisfaction with security attributes | Secure, not sure, not secure |
| 6 | Social Context | Trust level on use behaviour | Impact, neutral, no impact |

Table B1: Compound Variables

The set of variables above were coded and added as scale measurements to the cleaned survey data.

Survey Approach

With a data set of 43,120 unique elements, it was imperative to approach the analysis of this survey in a way that would provide insight into the data, keeping in mind the objective of the survey which includes:

- Understanding elements central to usable security in MFS;
- User perception on usability security, trust, and privacy
- Impact of user behaviour on usable security

A review of available survey tool was done with a view to understand the most suitable resource that will answer the questions of this exploratory survey. The following tools were identified and used for the analysis of the data.

1. Descriptive Statistics tool.
   This tool provides basic descriptive statistics e.g. frequency of the collated data. It helps to summarise and provide descriptive information about the collated data. It provides number of occurrences for responses, mean, median mode etc. It enables one to draw conclusion on data based on analysis of the collected input. The analysis of the collated data from this survey would benefit from descriptive statistics tools.

2. Correlation: Bivariate Analysis
   This analysis sought to understand relationship between variables in the survey, describes the effect that two or more phenomena occur together and their linkage. Since this research seeks to understand relationships between variables it would benefit from correlation. In this research for instance, this would provide insight into the relationship between user privacy perception and privacy awareness.

3. Cross tabulation

This helps compare relationships between two variables, it facilitates the examination of relationships within the data that might not have been otherwise apparent when analysing survey responses in their entirety. It would provide information like the relationship between age groups and authentication behaviours,

4. Principal Component Analysis (PCA)

Principal Component Analysis (PCA) is an exploratory multivariate analysis technique which seeks to describe the underlying structure in a data matrix. PCA is a technique for investigating the interdependence within groups of variables. It is concerned with the relationships between observable variables and unobservable latent variables presumed to be generating the observations. In this research for instance, relationships that might not be apparent from the use of the tools previously discussed, are likely to be observed using PCA. PCA helps check if there are variables not visible to using simple correlation techniques and cross-tabulation.

As explained earlier, in the analysis approach to this report, some similar questions in the questionnaire were grouped in other to explain underlying responses from the questions from the group, PCA helps to achieve this. The grouping helps to simply and reduce the amount of data needs to be analysed without any negative impact of the final output.

Survey Analysis Output

As described in the previous section, descriptive statistics, correlation and PCA were conducted on the final datasets with the following outputs.

Descriptive Stats: Frequency

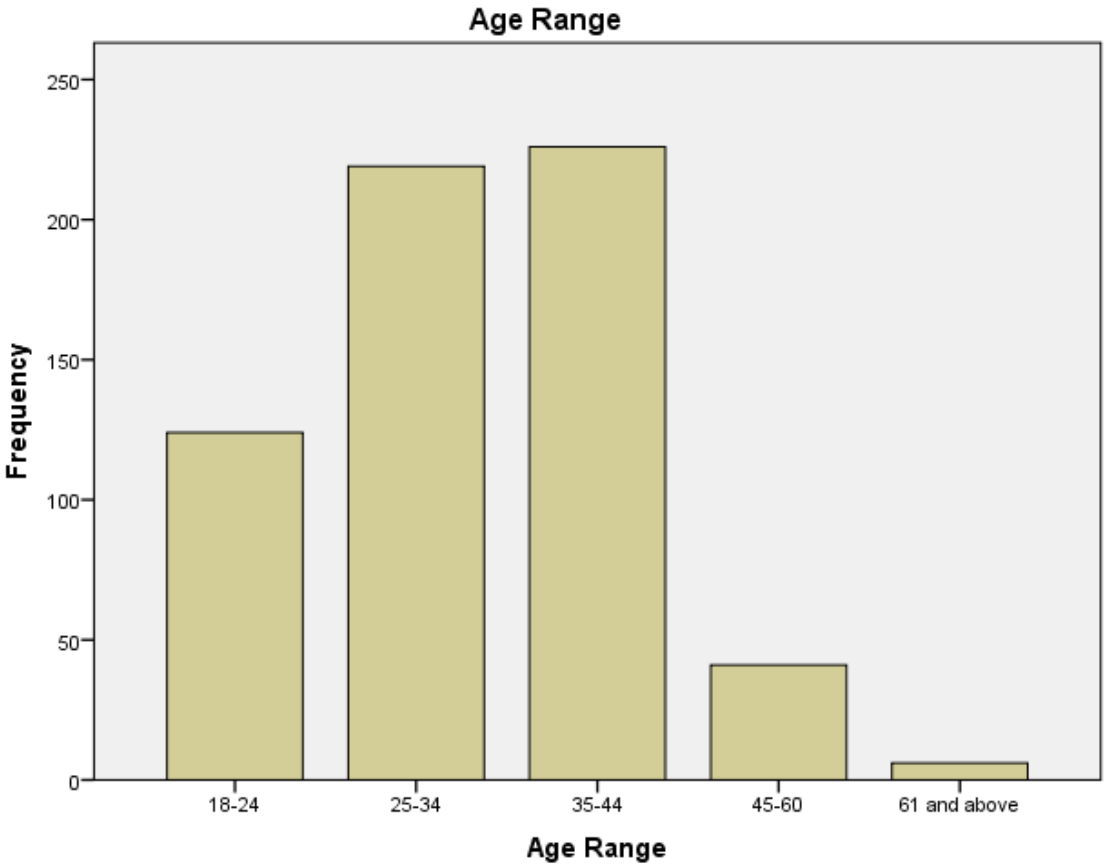



Figure B1: Age Frequency

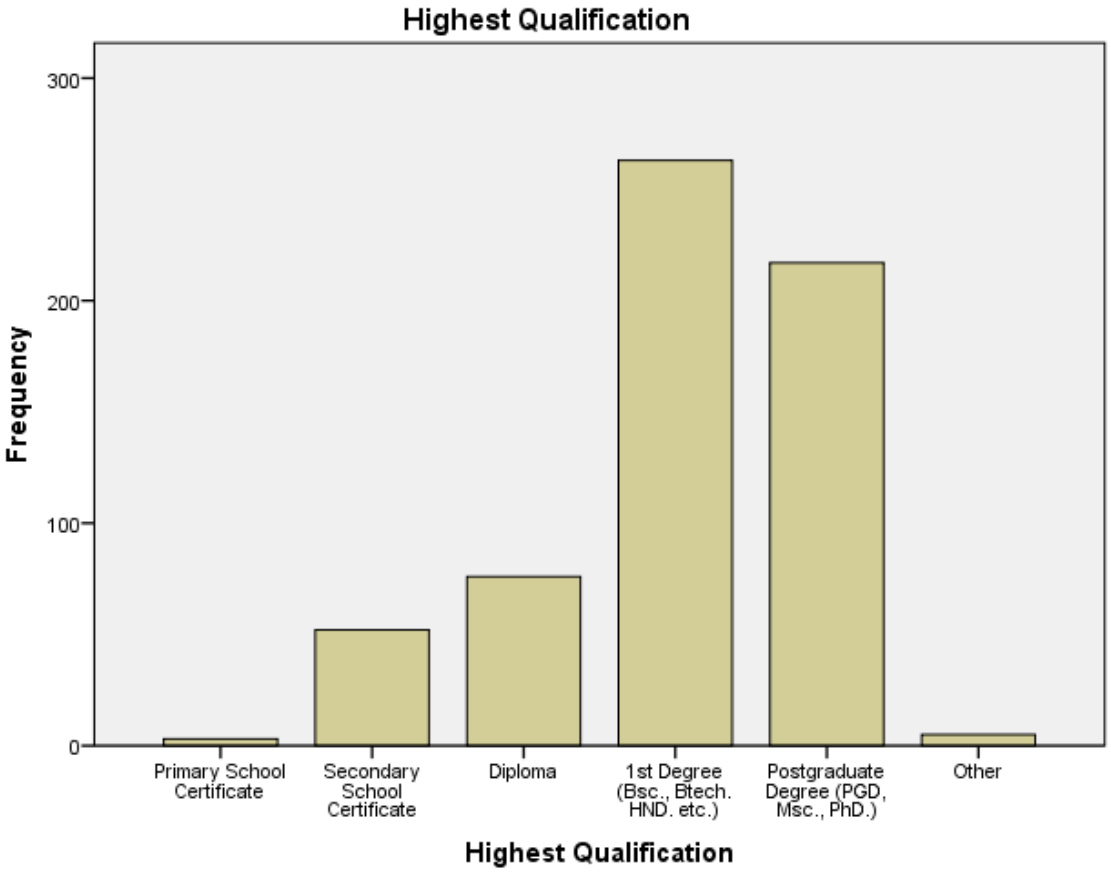



Figure B2: Qualification

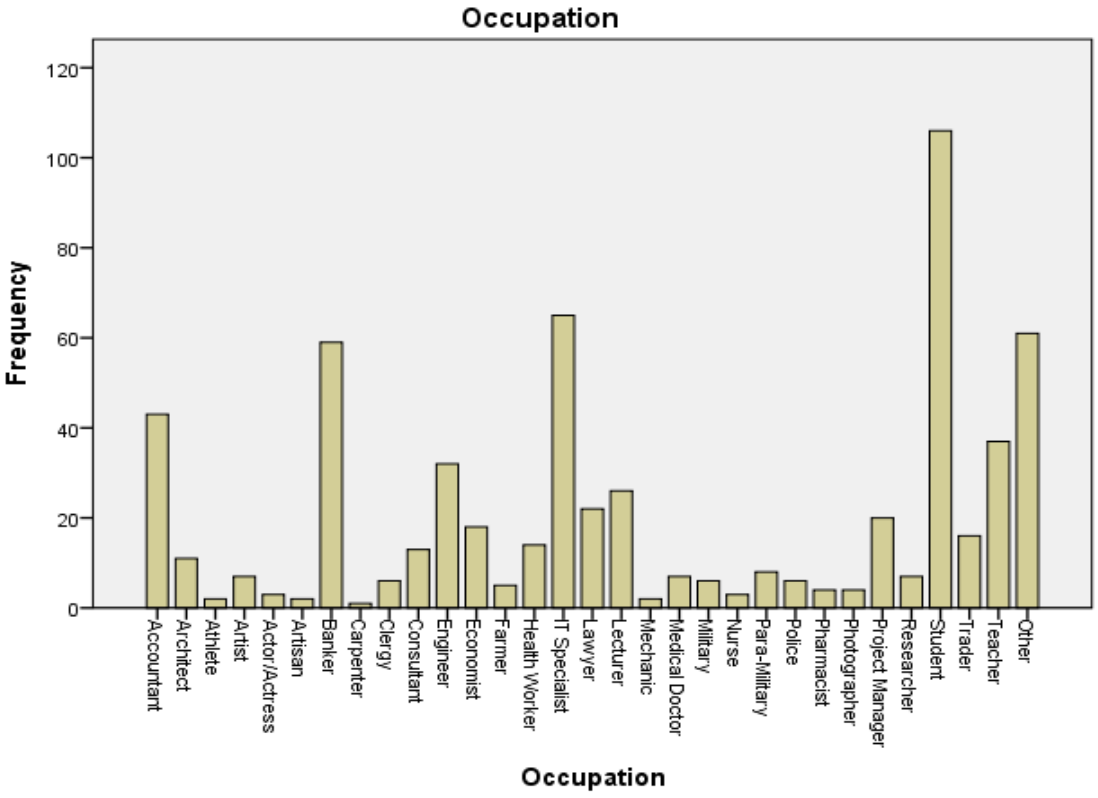



Figure B3: Occupation

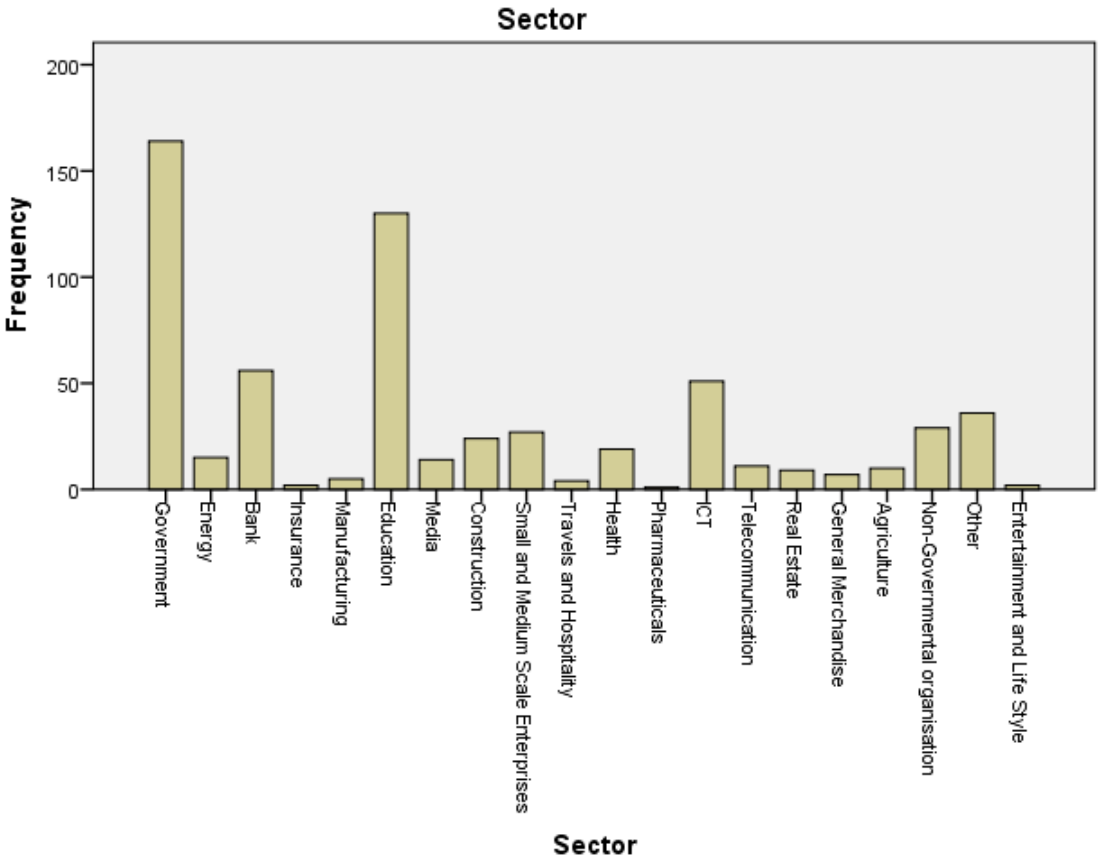



Figure B4: Sector

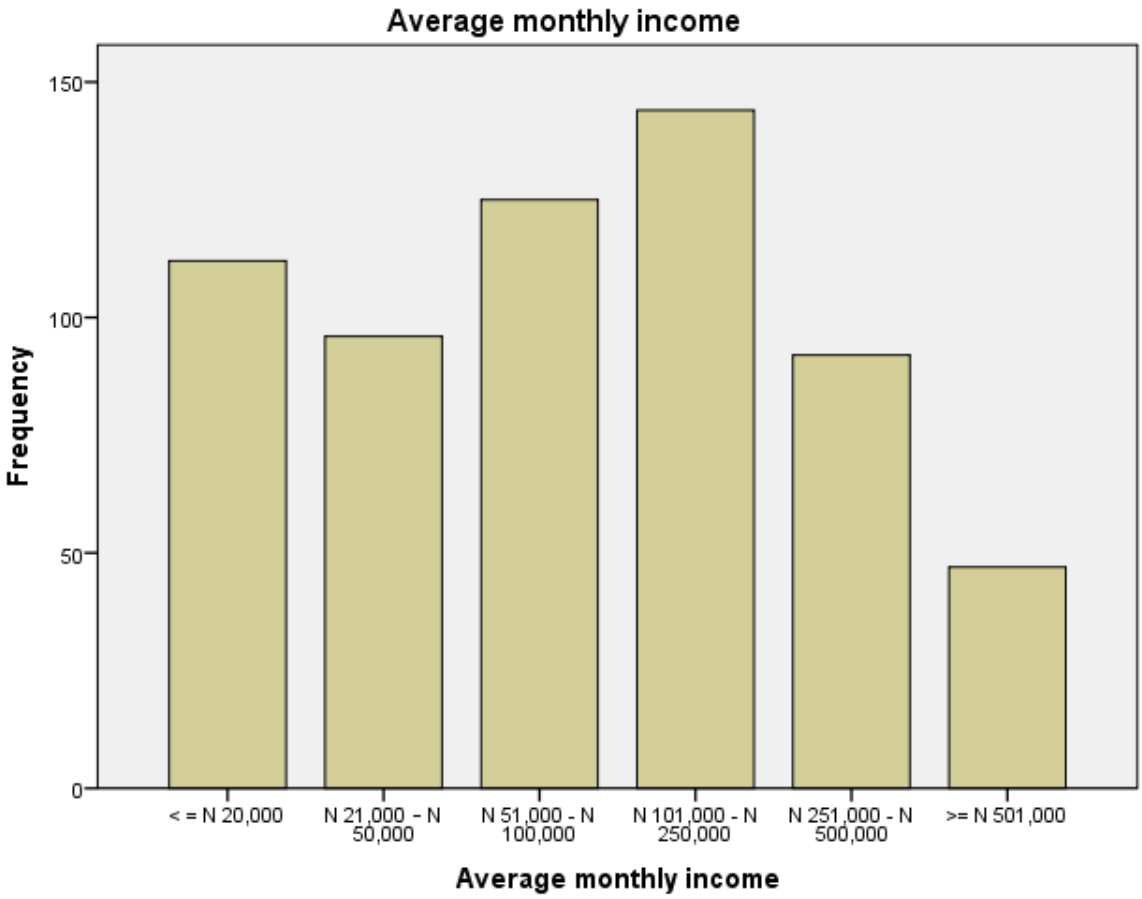



Figure B4: Income

Figure B4: Income

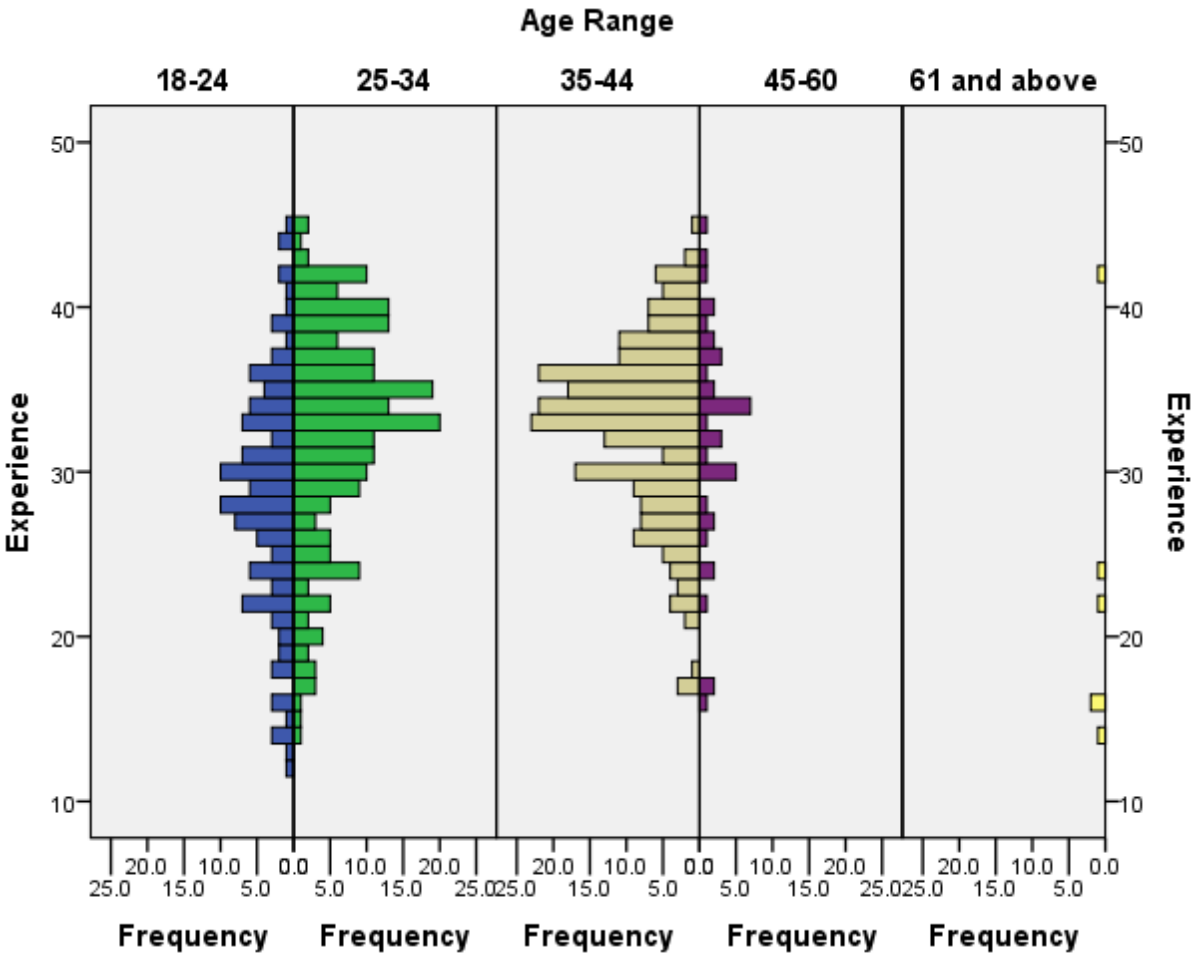



Figure B5: Age Range

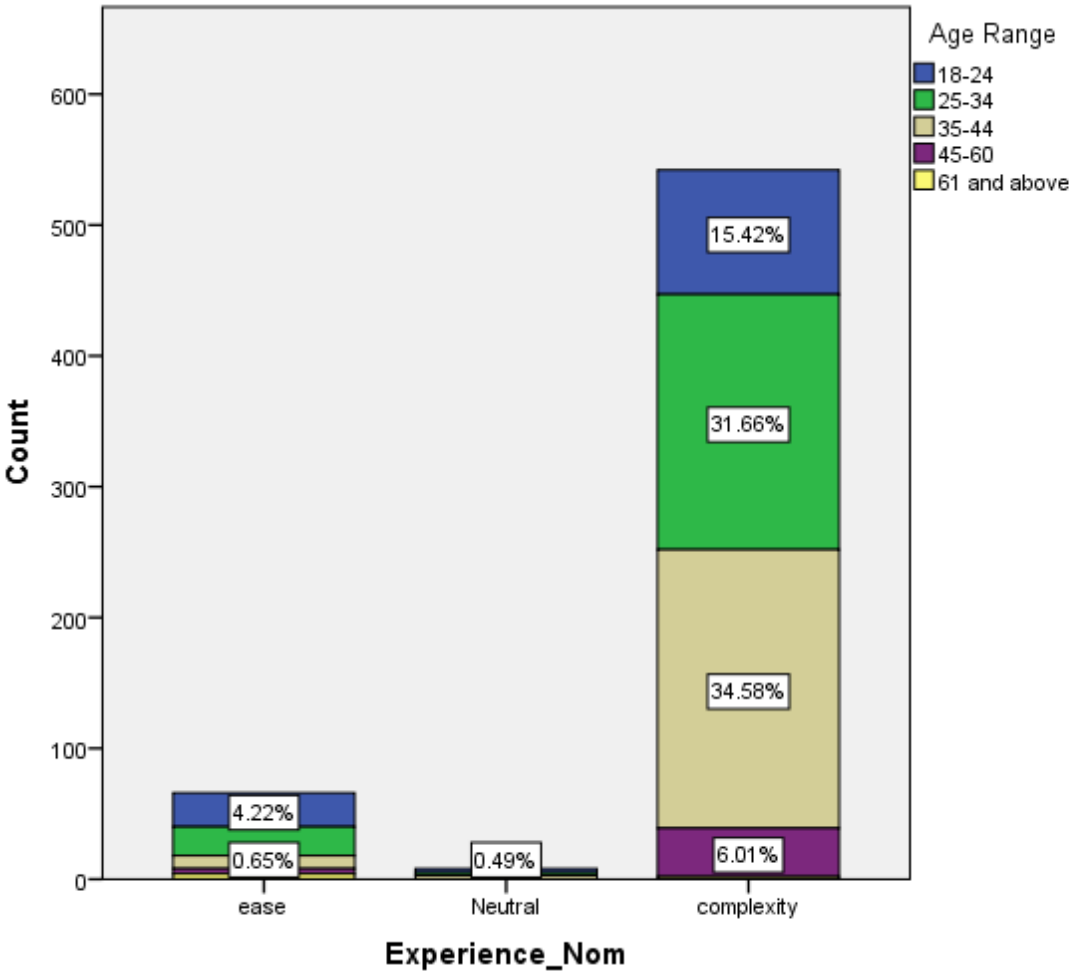



Figure B6: Experience

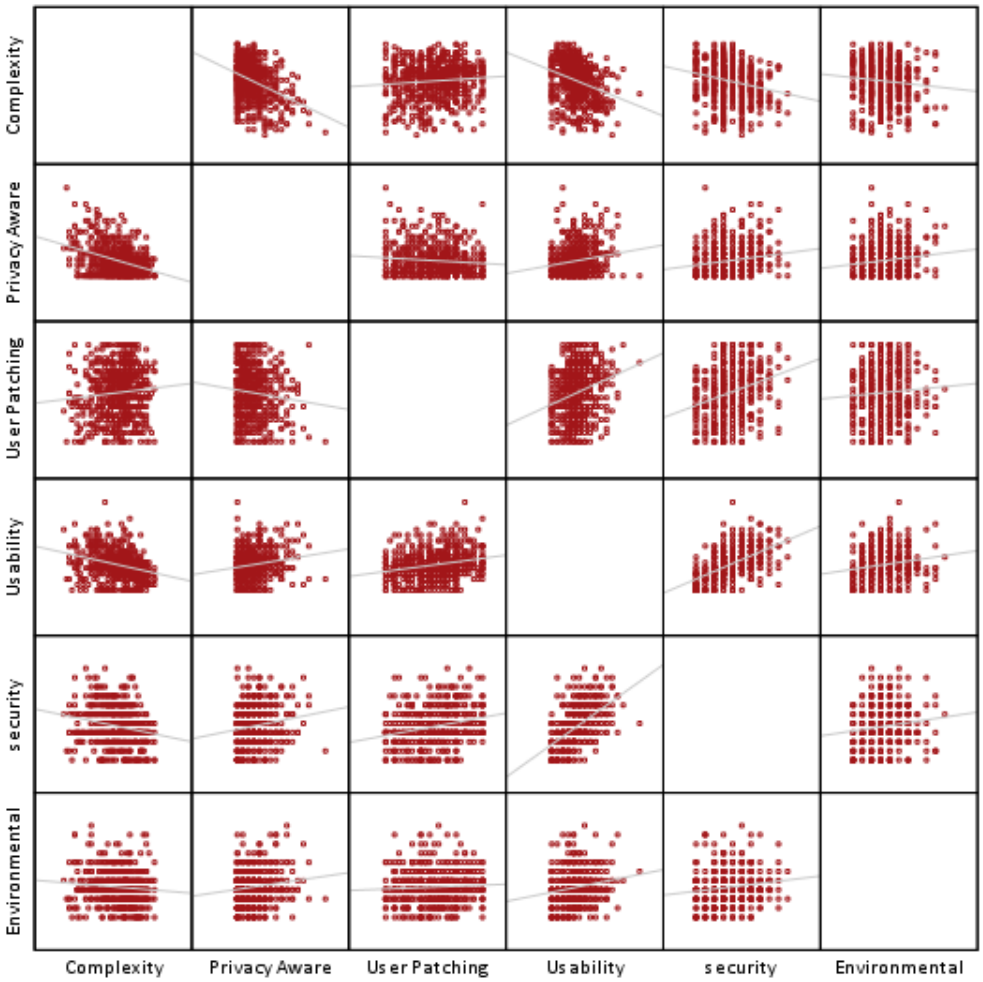



Figure B7: PCA Matrix

**Statistics**

| | | Experience_Nom | Awareness_Nom | Maintenance_Nom | Usability_Nom | Socialcontext_Nom |
|---|---|---|---|---|---|---|
| N | Valid | 616 | 616 | 616 | 616 | 616 |
| | Missing | 0 | 0 | 0 | 0 | 0 |
| Mean | | 2.77 | 1.80 | 1.17 | 1.50 | 1.60 |
| Minimum | | 1 | 1 | 1 | 1 | 1 |
| Maximum | | 3 | 2 | 2 | 3 | 3 |

Table B2: PCA Statistics

**Experience_Nom**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | ease | 66 | 10.7 | 10.7 | 10.7 |
| | Neutral | 8 | 1.3 | 1.3 | 12.0 |
| | complexity | 542 | 88.0 | 88.0 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table B3: Experience Nom

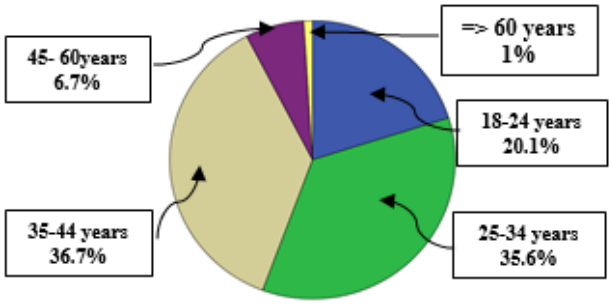



Figure B8: Age Distribution of Respondent

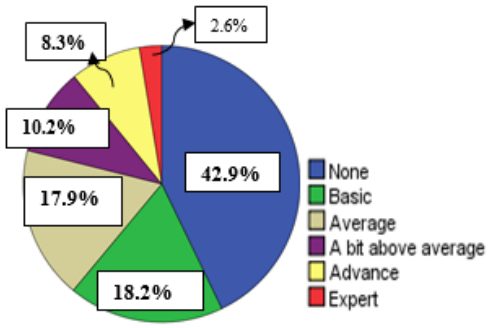



Figure B9: User knowledge of Rogue Applications

**Awareness_Nom**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | high privacy | 125 | 20.3 | 20.3 | 20.3 |
| | low privacy | 491 | 79.7 | 79.7 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table B4: Awareness_Nom

**Maintenance_Nom**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Yes | 509 | 82.6 | 82.6 | 82.6 |
| | No | 107 | 17.4 | 17.4 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table B5: Maintenance_Nom

**Socialcontext_Nom**

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | context impact | 371 | 60.2 | 60.2 | 60.2 |
| | neutral | 119 | 19.3 | 19.3 | 79.5 |
| | no context impact | 126 | 20.5 | 20.5 | 100.0 |
| | Total | 616 | 100.0 | 100.0 | |

Table B6: Socialcontext_Nom


Figure B10: Scree Plot

1. Descriptive statistics

| | Mean | Std. Deviation | Analysis N |
|---|---|---|---|
| Experience | 31.67 | 6.622 | 616 |
| Awareness | 6.75 | 2.586 | 616 |
| Maintenance | 19.14 | 5.670 | 616 |
| Usability | 8.60 | 2.461 | 616 |
| security | 6.68 | 1.915 | 616 |
| Social context | 6.29 | 1.717 | 616 |

Table B8: Descriptive statistics

2. Correlation

**Correlation Matrix**

| | Experience | Awareness | Maintenance | Usability | security | Social context |
|---|---|---|---|---|---|---|
| Experience | 1.000 | -.376 | .092 | -.302 | -.216 | -.096 |
| Awareness | -.376 | 1.000 | -.100 | .173 | .165 | .135 |
| Maintenance | .092 | -.100 | 1.000 | .249 | .264 | .062 |
| Usability | -.302 | .173 | .249 | 1.000 | .552 | .174 |
| security | -.216 | .165 | .264 | .552 | 1.000 | .136 |
| Social context | -.096 | .135 | .062 | .174 | .136 | 1.000 |

Table B9: Correlation Matrix

3. KMO and Bartlett's Test

| KMO and Bartlett's Test | | |
|---|---|---|
| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | | .638 |
| Bartlett's Test of Sphericity | Approx. Chi-Square | 494.897 |
| | Df | 15 |
| | Sig. | .000 |

Table B10: KMO

4. Total variance explained

**Total Variance Explained**

| Component | Initial Eigenvalues | | | Extraction Sums of Squared Loadings | | | Rotation Sums of Squared Loadings[a] |
|---|---|---|---|---|---|---|---|
| | Total | % of Variance | Cumulative % | Total | % of Variance | Cumulative % | Total |
| 1 | 2.027 | 33.788 | 33.788 | 2.027 | 33.788 | 33.788 | 1.833 |
| 2 | 1.322 | 22.029 | 55.817 | 1.322 | 22.029 | 55.817 | 1.126 |
| 3 | .931 | 15.514 | 71.331 | .931 | 15.514 | 71.331 | 1.055 |
| 4 | .685 | 11.421 | 82.751 | .685 | 11.421 | 82.751 | 1.421 |
| 5 | .602 | 10.026 | 92.777 | | | | |
| 6 | .433 | 7.223 | 100.000 | | | | |

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Table B11: Total Variance Explained

5. Commonality

| Communalities | | |
|---|---|---|
| | Initial | Extraction |
| Experience | 1.000 | .662 |
| Awareness | 1.000 | .605 |

| | | |
|---|---|---|
| Maintenance | 1.000 | .638 |
| Usability | 1.000 | .702 |
| security | 1.000 | .686 |
| Social context | 1.000 | .987 |

Extraction Method: Principal Component Analysis.

Table B12: Communalities

6. Component matrix

**Component Matrix[a]**

| | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Usability | .800 | | | |
| security | .760 | | | |
| Experience | -.580 | .535 | | |
| Maintenance | .313 | .735 | | .540 |
| Awareness | .487 | -.606 | | .525 |
| Social context | .373 | | .920 | |

Extraction Method: Principal Component Analysis.

a. 4 components extracted.

Table B13: Component Matrix

7. Pattern Matrix

**Pattern Matrix[a]**

| | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Usability | .869 | | | |
| security | .841 | | | |
| Maintenance | | .947 | | |
| Social context | | | .992 | |
| Awareness | | | | .973 |
| Experience | -.388 | .316 | | -.526 |

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.[a]

a. Rotation converged in 8 iterations.

Table B13: Pattern Matrix

8. Structure Matrix

**Structure Matrix**

| | Component | | | |
|---|---|---|---|---|
| | 1 | 2 | 3 | 4 |
| Usability | .873 | | | |
| security | .844 | | | |
| Maintenance | | .949 | | |
| Social context | | | .996 | |
| Awareness | | | | .927 |
| Experience | -.479 | .377 | | -.686 |

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

Table B14: Structure Matrix

9. Component matrix

**Component Correlation Matrix**

| Component | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1.000 | .125 | .130 | .264 |
| 2 | .125 | 1.000 | .065 | -.200 |
| 3 | .130 | .065 | 1.000 | .091 |
| 4 | .264 | -.200 | .091 | 1.000 |

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

Table B15: Component Matrix

Cross tabulation

1. What is the relationship between Age and Complexity of MFS?

**Age Range * Experience_Nom Crosstabulation**

| | | | Experience_Nom | | | |
|---|---|---|---|---|---|---|
| | | | ease | Neutral | complexity | Total |
| Age Range | 18-24 | Count | 26 | 3 | 95 | 124 |
| | | % of Total | 4.2% | 0.5% | 15.4% | 20.1% |
| | 25-34 | Count | 22 | 2 | 195 | 219 |
| | | % of Total | 3.6% | 0.3% | 31.7% | 35.6% |
| | 35-44 | Count | 10 | 3 | 213 | 226 |
| | | % of Total | 1.6% | 0.5% | 34.6% | 36.7% |
| | 45-60 | Count | 4 | 0 | 37 | 41 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | % of Total | 0.6% | 0.0% | 6.0% | 6.7% |
| | 61 and above | Count | 4 | 0 | 2 | 6 |
| | | % of Total | 0.6% | 0.0% | 0.3% | 1.0% |
| Total | | Count | 66 | 8 | 542 | 616 |
| | | % of Total | 10.7% | 1.3% | 88.0% | 100.0% |

**Data Privacy * Awareness_Nom Crosstabulation**

| | | | Awareness_Nom | | |
|---|---|---|---|---|---|
| | | | high privacy | low privacy | Total |
| Data Privacy | None | Count | 29 | 101 | 130 |
| | | % of Total | 4.7% | 16.4% | 21.1% |
| | Basic | Count | 18 | 111 | 129 |
| | | % of Total | 2.9% | 18.0% | 20.9% |
| | Average | Count | 35 | 111 | 146 |
| | | % of Total | 5.7% | 18.0% | 23.7% |
| | A bit above average | Count | 12 | 84 | 96 |
| | | % of Total | 1.9% | 13.6% | 15.6% |
| | Advance | Count | 24 | 59 | 83 |
| | | % of Total | 3.9% | 9.6% | 13.5% |
| | Expert | Count | 7 | 25 | 32 |
| | | % of Total | 1.1% | 4.1% | 5.2% |
| Total | | Count | 125 | 491 | 616 |
| | | % of Total | 20.3% | 79.7% | 100.0% |

**Socialcontext_Nom * Maintenance_Nom Crosstabulation**

| | | | MaintenanceNom | | |
|---|---|---|---|---|---|
| | | | Yes | No | Total |
| Socialcontext_Nom | context impact | Count | 324 | 47 | 371 |
| | | % of Total | 52.6% | 7.6% | 60.2% |
| | neutral | Count | 87 | 32 | 119 |
| | | % of Total | 14.1% | 5.2% | 19.3% |
| | no context impact | Count | 98 | 28 | 126 |
| | | % of Total | 15.9% | 4.5% | 20.5% |
| Total | | Count | 509 | 107 | 616 |
| | | % of Total | 82.6% | 17.4% | 100.0% |

**Training/Sensitization I received was sufficient * Socialcontext_Nom Crosstabulation**

| | | | Socialcontext_Nom | | | |
|---|---|---|---|---|---|---|
| | | | context impact | neutral | no context impact | Total |
| Training/Sensitization I received was sufficient | Yes | Count | 154 | 35 | 46 | 235 |
| | | % of Total | 25.0% | 5.7% | 7.5% | 38.1% |
| | No | Count | 217 | 84 | 80 | 381 |
| | | % of Total | 35.2% | 13.6% | 13.0% | 61.9% |
| Total | | Count | 371 | 119 | 126 | 616 |
| | | % of Total | 60.2% | 19.3% | 20.5% | 100.0% |

| # | Diagnostic Questions | Strongly Agree | Agree | Slightly Agree | Slightly Agree | Disagree | Strongly Disagree |
|---|---|---|---|---|---|---|---|
| 1 | For the topic being researched there is one single reality, the task of the researcher is to discover it | X | | | | | |
| 2 | The reality of the topic being researched exists separately from the researcher | | X | | | | |
| 3 | A researcher cannot be separated from what is being researched and so will inevitably be subjective | | | | | X | |
| 4 | A variety of data collection techniques should be used in research, both quantitative and qualitative | X | | | | | |
| 5 | The reality of what is being researched exists independently of people's thoughts, beliefs and knowledge of their existence | | | | | | X |
| 6 | Researchers must remain objective and independent from the phenomena they are studying, ensuring that their own values do not impact on data interpretation | | X | | | | |
| 7 | This research should be practical and applied | X | | | | | |
| 8 | This research should integrate different perspectives to help interpret the data | X | | | | | |
| 9 | This researcher needs to employ methods that allow in-depth exploration of the details behind a phenomenon | X | | | | | |
| 10 | This research is value laden | | | | | X | |
| # | Diagnostic Questions | Strongly Agree | Agree | Slightly Agree | Slightly Agree | Disagree | Strongly Disagree |
| 1 | For the topic being researched there is one single reality, the task of the researcher is to discover it | X | | | | | |
| 2 | The reality of the topic being researched exists separately from the researcher | | X | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3 | A researcher cannot be separated from what is being researched and so will inevitably be subjective | | | | | X | |
| 4 | A variety of data collection techniques should be used in research, both quantitative and qualitative | X | | | | | |
| 5 | The reality of what is being researched exists independently of people's thoughts, beliefs and knowledge of their existence | | | | | | X |
| 6 | Researchers must remain objective and independent from the phenomena they are studying, ensuring that their own values do not impact on data interpretation | | X | | | | |
| 7 | This research should be practical and applied | X | | | | | |
| 8 | This research should integrate different perspectives to help interpret the data | X | | | | | |
| 9 | This researcher needs to employ methods that allow in-depth exploration of the details behind a phenomenon | X | | | | | |
| 10 | This research is value laden | | | | | X | |

# Appendix III: Requirement Study

| ID | Requirement | Type | MoSCoW | Principles | Status |
|---|---|---|---|---|---|
| | **SOLUTION REQUIREMENTS: FUNCTIONAL** | | | | |
| **FR001** | The system shall implement mechanisms to ensure the integrity of user financial transactions. | Functional | Must-have | Integrity | Validated |
| **FR002** | The system shall perform regular checks to validate the integrity of stored user data and transaction records. | Functional | Must have | Integrity | Validated |
| **FR003** | The system shall provide security controls proportionate to users' knowledge, time, and transaction type. | Functional | Must-have | Proportionality | Validated |
| **FR004** | The system shall offer adjustable security settings to allow users to customise the level of security. | Functional | Must have | Proportionality | Validated |
| **FR005** | The system shall provide clear and understandable security notifications and alerts to users. | Functional | Must-have | Transparency | Validated |
| **FR006** | The system shall display the current security status and relevant information in an easily accessible manner. | Functional | Must have | Transparency | Validated |
| **FR008** | The system shall provide users with the ability to review and revert security choices made. | Functional | Should-have | Empowerment | Validation |
| **FR009** | The system shall support multiple authentication options to verify user identity. | Functional | Must-have | Identity | Validated |
| **FR010** | The system shall ensure that user authentication mechanisms minimise cognitive | Functional | Must have | Identity | Validated |

| | | | | | |
|---|---|---|---|---|---|
| | load for easy identity verification. | | | | |
| **FR011** | The system shall provide timely and accurate feedback on transaction status and error conditions. | Functional | Must-have | Reliability | Validated |
| **FR012** | The system shall have robust error handling mechanisms to recover from errors and ensure reliable execution of security functions. | Functional | Must have | Reliability | Validated |
| **FR013** | The system shall offer user-friendly and context-sensitive help and guidance for security-related tasks. | Functional | Must-have | User Support | Validated |
| **FR014** | The system shall provide relevant security information and instructions without overwhelming the user. | Functional | Must have | User Support | Validated |
| **FR015** | The system shall adhere to accessibility standards and guidelines for users with disabilities. | Functional | Must-have | Accessibility | Validated |
| **FR016** | The system shall provide alternative modes of interaction and accommodate users with visual or hearing impairments. | Functional | Must have | Accessibility | Validated |
| **FR017** | The system shall display valid certificates and security indicators to verify the authenticity of the application. | Functional | Must-have | Authenticity | Validated |
| **FR018** | The system shall notify users when they are interacting with potentially non- | Functional | Must have | Authenticity | Validated |

| | | | | | |
|---|---|---|---|---|---|
| | trustworthy sources or suspicious activities. | | | | |
| **FR019** | The system shall adhere to relevant industry regulations, data protection laws, and privacy policies. | Functional | Must-have | Compliance | Validated |
| **FR020** | The system shall provide necessary audit logs and security measures to ensure compliance with applicable standards and regulations. | Functional | Must have | Compliance | Validated |
| **FR021** | The system shall integrate security controls seamlessly into the user's workflow. | Functional | Must-have | Alignment | Validated |
| **FR022** | The system shall align security mechanisms with the user's mental model and existing mobile financial service interactions. | Functional | Could have | Alignment | Validated |
| **FR023** | The system shall provide users with options and flexibility in choosing security measures. | Functional | Must-have | Freedom | Validated |
| **FR024** | The system shall allow users to adjust security settings to balance security requirements and user convenience. | Functional | Should-have | Freedom | Validated |
| | **SOLUTION REQUIREMENTS: NON-FUNCTIONAL** | | | | |
| **NFR001** | The system shall provide fast and responsive security controls and actions. | Non-functional | Must-have | Proportionality, Empowerment | Validated |
| **NFR002** | The system shall handle concurrent user transactions efficiently and without significant performance degradation. | Non-functional | Should-have | Proportionality, Reliability | Validated |

| | | | | | |
|---|---|---|---|---|---|
| **NFR003** | The system shall have an intuitive and user-friendly interface for ease of use. | Non-functional | Must-have | Empowerment, User Support | Validated |
| **NFR004** | The system shall minimise user cognitive load when interacting with security features. | Non-functional | Must have | Empowerment, Alignment | Validated |
| **NFR005** | The system shall employ encryption mechanisms to protect user data during transmission and storage. | Non-functional | Must-have | Integrity, Confidentiality | Validated |
| **NFR006** | The system shall enforce strong access controls to prevent unauthorised access to sensitive information and functions. | Non-functional | Must-have | Integrity, Empowerment, Compliance | Validated |
| **NFR007** | The system shall implement secure authentication mechanisms to verify user identity and protect MFS users against unauthorised access. | Non-functional | Must-have | Identity, Integrity, Compliance | Validated |
| **NFR008** | The system shall have mechanisms in place for monitoring and detecting security breaches or suspicious activities. | Non-functional | Must have | Integrity, Authenticity, Compliance | Validated |
| **NFR009** | The system shall ensure high availability and minimal downtime to facilitate continuous access to services. | Non-functional | Must-have | Reliability | Validated |
| **NFR010** | The system shall have mechanisms to recover from failures and restore data integrity in case of system disruptions. | Non-functional | Must-have | Integrity, Reliability | Validated |

| | | | | | |
|---|---|---|---|---|---|
| **NFR011** | The system shall maintain consistent performance and functionality even under peak load conditions. | Non-functional | Should-have | Reliability | Validated |
| **NFR012** | The system shall be compatible with a wide range of mobile devices and operating systems. | Non-functional | Must-have | Alignment, Compatibility | Validated |
| **NFR013** | The system shall integrate with existing mobile financial service platforms and systems seamlessly. | Non-functional | Should-have | Alignment, Compatibility | Validated |
| **NFR014** | The system shall be scalable to accommodate an increasing number of users and growing transaction volumes. | Non-functional | Must-have | Proportionality, Alignment | Validated |
| **NFR015** | The system shall handle future enhancements and additional security features without significant performance degradation. | Non-functional | Should-have | Proportionality, Reliability | Validated |
| **NFR016** | The system shall be modular and well-documented to facilitate easy maintenance and future updates. | Non-functional | Must-have | User Support, Empowerment, Transparency | Validated |
| **NFR017** | The system shall have mechanisms to apply security patches and updates in a timely and efficient manner. | Non-functional | Must-have | Integrity, Reliability, Compliance | Validated |
| **NFR019** | The system shall provide users with clear information about the collection, use, and sharing of their personal data. | Non-functional | Must-have | Transparency, Empowerment | Validated |
| **NFR020** | The system shall generate comprehensive audit logs for | Non-functional | Must-have | Compliance | validated |

| | | | | | |
|---|---|---|---|---|---|
| | security-related events and actions. | | | | |
| **NFR022** | The system shall ensure that security customization does not compromise the overall security of the system. | Non-functional | Must-have | Freedom | Validated |
| **NFR023** | The system shall provide clear instructions and guidance on the implications of adjusting security settings, in media formats that the user can consume (Audio, video, text etc) | Non-functional | Must-have | Freedom, Empowerment | Validated |
| **NFR024** | The system shall provide mechanisms for administrators to review and analyse security-related logs and reports. | Non-functional | Must-have | User Support, Compliance | Validated |
| **NFR025** | The system shall implement data encryption algorithms to ensure the integrity of user financial transactions and data. | Technical | Must-have | Integrity | Validated |
| **NFR026** | The system shall employ secure hash algorithms to validate the integrity of stored user data and transaction records. | Technical | Could-have | Integrity | Validated |
| **NFR027** | The system shall optimise resource usage to provide security controls that are proportionate to the device's capabilities. | Technical | Must-have | Proportionality | Validated |
| **NFR028** | The system shall implement security measures that do not excessively impact the performance and | Technical | Should-have | Proportionality | Validated |

| | | | | | |
|---|---|---|---|---|---|
| | responsiveness of the application. | | | | |
| **NFR029** | The system shall provide clear and concise security-related notifications and alerts to the user. | Technical | Must-have | Transparency | Validated |
| **NFR030** | The system shall display relevant security information in a user-friendly manner, ensuring transparency in the security features. | Technical | Should-have | Transparency | Validated |
| **NFR032** | The system shall offer options for users to manage their security preferences and make informed choices. | Technical | Should-have | Empowerment | Validated |
| **NFR033** | The system shall integrate with reliable and secure user identity verification services (e.g., biometrics, two-factor authentication). | Technical | Must-have | Identity | Validated |
| **NFR036** | The system shall employ redundant and failover systems to provide continuous availability and resilience. | Technical | Should-have | Reliability | Validated |
| **NFR037** | The system shall provide detailed documentation and user manuals to assist users in understanding and utilizing security features. | Technical | Must-have | User Support | Validated |
| **NFR038** | The system shall offer responsive technical support channels (e.g., helpdesk, live chat) to address user queries and issues. | Technical | Must-have | User Support | Validated |

| | | | | | |
|---|---|---|---|---|---|
| **NFR039** | The system shall be compatible with popular mobile device platforms (e.g., iOS, Android) and their respective versions. | Technical | Must-have | Alignment, Compatibility | Validated |
| **NFR040** | The system shall integrate seamlessly with existing mobile financial service infrastructure and APIs. | Technical | Should-have | Alignment, Compatibility | Validated |
| **NFR041** | The system architecture shall support horizontal scalability to handle increasing user demand and transaction volume. | Technical | Should-have | Proportionality, Alignment | Validated |
| **NFR042** | The system shall employ load balancing mechanisms to distribute traffic and ensure optimal system performance. | Technical | Could-have | Proportionality, Reliability | Validated |
| **NFR043** | The system shall follow modular and well-documented coding practices to facilitate system maintenance and updates. | Technical | Must-have | User Support, Transparency, Alignment | Validated |
| **NFR046** | The system shall implement data anonymization techniques to minimise the exposure of user-sensitive information. | Technical | Should-have | Confidentiality | Validated |
| **NFR048** | The system shall support a wide range of security configurations and options based on user preferences. | Technical | Must-have | Freedom | Validated |
| **NFR049** | The system shall provide real-time application response and feedback when users adjust security settings. | Technical | Should-have | Freedom | Validated |
| | **TRANSITION REQUIREMENTS** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| **TR001** | The transition process shall align with existing security frameworks and procedures. | Transition | Must-have | Alignment | Validated |
| **TR002** | The transition plan shall minimise disruption to ongoing operations and user experience. | Transition | Must-have | Alignment | Validated |
| **TR003** | User training materials shall be provided to facilitate understanding and adoption of new security heuristics. | Transition | Must-have | User Support, Empowerment | Validated |
| **TR004** | Education programmes shall be conducted to raise awareness about the importance of mobile financial security and best practices. | Transition | Should-have | User Support, Empowerment | Validated |
| **TR005** | The migration process from the existing security framework to the new heuristics shall be smooth and seamless. | Transition | Must-have | Alignment, Reliability | Validated |
| **TR006** | A phased approach to migration shall be followed to ensure a gradual transition without significant disruption to users. | Transition | Must-have | Alignment, Reliability | Validated |
| **TR007** | Clear communication channels shall be established to provide ongoing support and guidance during the transition period. | Transition | Must-have | User Support | Validated |
| **TR010** | A knowledge base or FAQ section shall be available to provide self-help resources for users during the transition. | Transition | Should-have | User Support, Empowerment | Validated |

| | | | | | |
|---|---|---|---|---|---|
| **TR011** | The new security heuristics shall undergo thorough testing and validation to ensure their effectiveness and reliability. | Transition | Must-have | Reliability | Validated |
| **TR012** | Test scenarios and conditions shall be designed to verify compliance with industry standards and regulatory requirements. | Transition | Should-have | Compliance | Validated |
| **TR013** | Mechanisms shall be in place to collect user feedback on the usability and effectiveness of the new security heuristics. | Transition | Should-have | User Support, Empowerment | Validated |
| **TR016** | Feedback from users and stakeholders shall be used to refine and improve the security heuristics through iterative processes. | Transition | Could-have | User Support, Empowerment | Validated |

# Appendix IV: Requirement and Heuristics

| ID | Requirement | Type | MoSCoW | Principles |
|---|---|---|---|---|
| | **SOLUTION REQUIREMENTS: FUNCTIONAL** | | | |
| **FR001** | The system shall implement mechanisms to ensure the integrity of user financial transactions. | Functional | Must-have | Integrity |
| **FR002** | The system shall perform regular checks to validate the integrity of stored user data and transaction records. | Functional | Must have | Integrity |
| **FR003** | The system shall provide security controls proportionate to users' knowledge, time, and transaction type. | Functional | Must-have | Proportionality |
| **FR004** | The system shall offer adjustable security settings to allow users to customise the level of security. | Functional | Must have | Proportionality |
| **FR005** | The system shall provide clear and understandable security notifications and alerts to users. | Functional | Must-have | Transparency |
| **FR006** | The system shall display the current security status and relevant information in an easily accessible manner. | Functional | Must have | Transparency |
| **FR008** | The system shall provide users with the ability to review and revert security choices made. | Functional | Should-have | Empowerment |
| **FR009** | The system shall support multiple authentication options to verify user identity. | Functional | Must-have | Identity |
| **FR010** | The system shall ensure that user authentication mechanisms minimise cognitive load for easy identity verification. | Functional | Must have | Identity |
| **FR011** | The system shall provide timely and accurate feedback on transaction status and error conditions. | Functional | Must-have | Reliability |
| **FR012** | The system shall have robust error handling mechanisms to recover from errors and ensure reliable execution of security functions. | Functional | Must have | Reliability |

| | | | | |
|---|---|---|---|---|
| **FR013** | The system shall offer user-friendly and context-sensitive help and guidance for security-related tasks. | Functional | Must-have | User Support |
| **FR014** | The system shall provide relevant security information and instructions without overwhelming the user. | Functional | Must have | User Support |
| **FR015** | The system shall adhere to accessibility standards and guidelines for users with disabilities. | Functional | Must-have | Accessibility |
| **FR016** | The system shall provide alternative modes of interaction and accommodate users with visual or hearing impairments. | Functional | Must have | Accessibility |
| **FR017** | The system shall display valid certificates and security indicators to verify the authenticity of the application. | Functional | Must-have | Authenticity |
| **FR018** | The system shall notify users when they are interacting with potentially non-trustworthy sources or suspicious activities. | Functional | Must have | Authenticity |
| **FR019** | The system shall adhere to relevant industry regulations, data protection laws, and privacy policies. | Functional | Must-have | Compliance |
| **FR020** | The system shall provide necessary audit logs and security measures to ensure compliance with applicable standards and regulations. | Functional | Must have | Compliance |
| **FR021** | The system shall integrate security controls seamlessly into the user's workflow. | Functional | Must-have | Alignment |
| **FR022** | The system shall align security mechanisms with the user's mental model and existing mobile financial service interactions. | Functional | Could have | Alignment |
| **FR023** | The system shall provide users with options and flexibility in choosing security measures. | Functional | Must-have | Freedom |
| **FR024** | The system shall allow users to adjust security settings to balance security requirements and user convenience. | Functional | Should-have | Freedom |

| | SOLUTION REQUIREMENTS: NON-FUNCTIONAL | | | |
|---|---|---|---|---|
| **NFR001** | The system shall provide fast and responsive security controls and actions. | Non-functional | Must-have | Proportionality, Empowerment |
| **NFR002** | The system shall handle concurrent user transactions efficiently and without significant performance degradation. | Non-functional | Should-have | Proportionality, Reliability |
| **NFR003** | The system shall have an intuitive and user-friendly interface for ease of use. | Non-functional | Must-have | Empowerment, User Support |
| **NFR004** | The system shall minimise user cognitive load when interacting with security features. | Non-functional | Must have | Empowerment, Alignment |
| **NFR005** | The system shall employ encryption mechanisms to protect user data during transmission and storage. | Non-functional | Must-have | Integrity, Confidentiality |
| **NFR007** | The system shall implement secure authentication mechanisms to verify user identity and protect against unauthorised access. | Non-functional | Must-have | Identity, Integrity, Compliance |
| **NFR008** | The system shall have mechanisms in place for monitoring and detecting security breaches or suspicious activities. | Non-functional | Must have | Integrity, Authenticity, Compliance |
| **NFR009** | The system shall ensure high availability and minimal downtime to facilitate continuous access to services. | Non-functional | Must-have | Reliability |

# Appendix V: Test Scripts

Test Case Summary

| Heuristics | Android | | | IOS | | |
|---|---|---|---|---|---|---|
| | Pass | Partial Pass | Fail | Pass | Partial Pass | Fail |
| Integrity | 90 | 8 | 2 | 92 | 6 | 2 |
| Proportionality | 95 | 5 | 0 | 91 | 8 | 1 |
| Transparency | 90 | 8 | 3 | 93 | 8 | 0 |
| Empowerment | 90 | 7 | 3 | 90 | 7 | 3 |
| Identity | 88 | 9 | 3 | 91 | 9 | 0 |
| Reliability | 84 | 11 | 5 | 83 | 14 | 3 |
| User Support | 92 | 8 | 0 | 92 | 8 | 0 |
| Accessibility | 88 | 12 | 0 | 88 | 12 | 0 |
| Authenticity | 92 | 8 | 0 | 88 | 13 | 0 |
| Compliance | 100 | 0 | 0 | 100 | 0 | 0 |
| Alignment | 90 | 8 | 2 | 92 | 6 | 2 |
| Freedom | 87 | 0 | 13 | 87 | 0 | 13 |

Proportionality test Extract:

| Expected Results | Post conditions | MF1 Test Result | MF2 Test Result |
|---|---|---|---|
| Security controls should dynamically adjust based on the user's knowledge, time, and type of transaction without any breaches. | System returns to stable state, ready for the next transaction. | Pass | Pass |
| The system should respect the customised security settings without any compromises. | System returns to stable state with customised settings saved for future transactions. | Pass | Pass |
| The system should demonstrate fast and responsive security controls consistently. | System remains stable, ready for next operation. | Pass | Pass |
| The system should handle concurrent transactions without significant performance degradation. | System remains stable, ready for next batch of concurrent transactions. | Pass | Pass |
| The system should scale seamlessly to handle the increase without crashing or slowing down significantly. | System remains stable, ready for further scaling tests. | Pass | Pass |

| | | | |
|---|---|---|---|
| The system should integrate the new features without significant performance degradation. | System remains stable, ready for further enhancements. | Pass | Pass |
| The system should optimise resource usage efficiently, adapting to the device's capabilities without compromising security. | System remains stable, ready for the next transaction. | Pass | Pass |
| The application should maintain acceptable levels of performance and responsiveness even with enhanced security measures. | System remains stable, ready for next operation. | Pass | Pass |
| The system should scale horizontally without issues, accommodating the increased demand efficiently. | System returns to stable state, ready for further scalability tests. | Pass | Pass |
| The load balancing mechanisms should distribute traffic evenly, preventing system overloads and ensuring optimal performance. | System remains stable, ready for the next batch of traffic. | Pass | Pass |

Proportionality Test Extract with Comments

| Expected Results | Post conditions | MF8 Test Result | Comments |
|---|---|---|---|
| Security controls should dynamically adjust based on the user's knowledge, time, and type of transaction without any breaches. | System returns to stable state, ready for the next transaction. | Pass | MF4 showed a slight delay in security control adjustments. |
| The system should respect the customised security settings without any compromises. | System returns to stable state with customised settings saved for future transactions. | Pass | MF6 displayed minor issues when custom settings were applied. |
| The system should demonstrate fast and responsive security controls consistently. | System remains stable, ready for next operation. | Pass | Security controls operated efficiently across platforms. |
| The system should handle concurrent transactions without significant performance degradation. | System remains stable, ready for next batch of concurrent transactions. | Pass | No significant performance degradation observed. |
| The system should scale seamlessly to handle the increase without crashing or slowing down significantly. | System remains stable, ready for further scaling tests. | Pass | System scaled successfully without noticeable issues. |

| | | | |
|---|---|---|---|
| The system should integrate the new features without significant performance degradation. | System remains stable, ready for further enhancements. | Pass | New features integrated successfully without performance issues. |
| The system should optimise resource usage efficiently, adapting to the device's capabilities without compromising security. | System remains stable, ready for the next transaction. | Pass | Resource usage optimised successfully across various devices. |
| The application should maintain acceptable levels of performance and responsiveness even with enhanced security measures. | System remains stable, ready for next operation. | Pass | Security measures enhanced without affecting performance. |
| The system should scale horizontally without issues, accommodating the increased demand efficiently. | System returns to stable state, ready for further scalability tests. | Pass | Horizontal scalability demonstrated successfully. |
| The load balancing mechanisms should distribute traffic evenly, preventing system overloads and ensuring optimal performance. | System remains stable, ready for the next batch of traffic. | Pass | Load balanced effectively in high traffic scenarios. |

# Appendix VI: Ethics Documentation

Bournemouth University

## Research Ethics Checklist

| About Your Checklist | |
|---|---|
| **Ethics ID** | 39606 |
| **Date Created** | 20/09/2021 23:05:14 |
| **Status** | Approved |
| **Date Approved** | 21/10/2021 06:26:40 |
| **Date Submitted** | 20/09/2021 23:13:40 |
| **Risk** | Low |

| Researcher Details | |
|---|---|
| **Name** | Stephen Ambore |
| **Faculty** | Faculty of Science & Technology |
| **Status** | Postgraduate Research (MRes, MPhil, PhD, DProf, EngD, EdD) |
| **Course** | Postgraduate Research - FST |
| **Have you received funding to support this research project?** | No |

| Project Details | |
|---|---|
| **Title** | Cybersecurity for the Unbanked |
| **Start Date of Project** | 26/01/2016 |
| **End Date of Project** | 26/01/2022 |
| **Proposed Start Date of Data Collection** | 26/09/2021 |
| **Original Supervisor** | Huseyin Dogan |
| **Approver** | Marcin Budka |

**Summary - no more than 600 words (including detail on background methodology, sample, outcomes, etc.)**

I had earlier sought and obtained ethics approval for the 1st part of my PhD study which examined the supply and demand side factors that affect Usable Security in Mobile Financial Services.

As part of these studies, through an iterative approach 12 usable security heuristics were identified. The application of these heuristics are meant to improve usable security in Mobile Financial Services. The heuristics were then validated by experts and the outcome of the study published at a conference.

The next step is the exploitation phase of my PhD work where the developed heuristics will be applied to conduct evaluation of Usable Security problem in Mobile Financial Services (MFS) and to develop Mobile Financial Services solution. To achieve this, Heuristics evaluation will be conducted where 5 experts will conduct heuristics evaluation on selected Mobile Financial Service System. The second part of the exploitation will be carried out as a hackathon where participants will use the heuristics to develop components of MFS to enable me to recommend usable security guide for Mobile Financial Services developers.



Printed On 21/10/2021 22:40:27

Bournemouth University

# Research Ethics Checklist

| | |
|---|---|
| **Reference Id** | 16976 |
| **Status** | Approved |
| **Date Approved** | 12/09/2017 |

## Researcher Details

| | |
|---|---|
| **Name** | Stephen Ambore |
| **School** | Faculty of Science & Technology |
| **Status** | Postgraduate Research (MRes, MPhil, PhD, DProf, DEng) |
| **Course** | Postgraduate Research - FST |
| **Have you received external funding to support this research project?** | No |
| **Please list any persons or institutions that you will be conducting joint research with, both internal to BU as well as external collaborators.** | Dr. Christopher Richardson, Dr. Huseyin Dogan, Dr. Edward Apeh, Prof. David Osselton |

## Project Details

| | |
|---|---|
| **Title** | CyberSecurity for the Unbanked |
| **Proposed Start Date of Data Collection** | 04/09/2017 |
| **Proposed End Date of Project** | 04/12/2017 |
| **Original Supervisor** | Christopher Richardson |
| **Approver** | Research Ethics Panel |

Bournemouth University

# Participant Information Sheet

## Title of the research project:

Cybersecurity for the Unbanked

## Invitation

You are being invited to take part in a study. Before you go ahead, it is important for you to understand the reason for the study and what it entails. Please take a few minutes to carefully read the following information. Also, please feel free to contact me should you require more information.

## Researcher

This study is being carried out by Stephen Ambore a PhD researcher at Bournemouth University under the faculty of Science and Technology. The research falls in the Cybersecurity domain with specific focus on building a Cybersecurity framework for Mobile Financial Services (MFS).

## Research Funders

This research is self-funded and is conducted as a PhD research in Bournemouth University.

## Purpose of the project

As part of this PhD study, through an iterative approach 12 usable security heuristics were identified. The application of these heuristics ~~are~~ meant to improve usable security in Mobile Financial Services.

The next step is the exploitation phase of my PhD work where the developed heuristics will be applied to conduct evaluation of Usable Security problem in Mobile Financial Services (MFS) and to develop Mobile Financial Services solution. To achieve this, Heuristics evaluation will be conducted where experts will conduct heuristics evaluation on selected Mobile Financial Service System. The second part of the exploitation will be carried out as a hackathon where participants will use the heuristics to develop components of MFS to enable me to recommend usable security guide for Mobile Financial Services developers.

-

## Why have I been chosen?

You have been chosen to participate in this study based on your role as Cybersecurity/ and HCI experts.

## Do I have to take part?

Taking part in this study is entirely voluntary and you can also pull out at any point in the research should you no longer wish to continue, but we would love to hear from you. The evaluation session will last about three hours. During the session you will be required to use the set of heuristics we

Bournemouth University

have developed to evaluate usable security in MFS, you will also be expected to compare this with existing heuristics. The set of heuristics would be sent to you upfront and the would be conducted online. All participants Personal Identifiable Information (PII) if any shall be anonymised.

### What are the advantages and possible disadvantages or risks of taking part?

Whilst there are no immediate benefits for those people participating in the study, it is hoped that this work will improve trust in the use of Mobile Financial Services and making access to financial services available to about 21,7billion of the world's population who currently do not have access to formal banking services. There are no foreseeable risks or discomfort expected as a result of participating in the interviews. The interview will be conducted at your convenient time, within the time limit of this research work.

### Will my taking part in this project be kept confidential?

All the information that we collect from you during the course of the research will be kept strictly confidential and no personal identifiable data will be required. You will not be able to be identified in any reports or publications. All data relating to this study will be kept for 5 years on a Bournemouth University password protected secure network.

### What type of information will be sought from me?

The study will only collect data to evaluate the performance of the heuristics in identifying usable security problem in Mobile financial services.

### Will I be recorded, and how will the recorded media be used?

Written notes will be taken by the researcher during the interview, the purpose of taking the notes is to ensure your thought are accurately captured, this would be sent to you to verify if what was noted represent your exact opinion. No other use will be made of the feedback without your written permission, and no one outside the project will be allowed access to the original notes.

### Definition of key terms

Mobile Financial Services: The use of mobile phones for conducting financial transactions include: Mobile Banking Application, Mobile Money, and Mobile Payment solutions using mobile phones.

The International Standard Organisation (ISO) definition of Usability: the effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments.

The Nielsen Norman Group a foremost usability research group defines usability by 5 quality components as follows:

## Participant Agreement Form

**Full title of project: Cybersecurity for the Unbanked**

**Name, position and contact details of researcher: Stephen Ambore, PhD Researcher, Bournemouth University.**

**Name, position and contact details of supervisor: Dr Huseyin Dogan, Bournemouth University.**

| | **Please Initial or Tick Here** |
|---|---|
| I have read and understood the participant information sheet for the above research project | |
| I confirm that I have had the opportunity to ask questions. | |
| I understand that my participation is voluntary. | |
| I understand that I am free to withdraw up to the point where the data is processed and become anonymous, so my identity cannot be determined. | |
| During the interview, I am free to withdraw without giving reason and without there being any negative consequences. | |
| Should I not wish to answer any particular question(s), I am free to decline | |
| I give permission for members of the research team to have access to my anonymised responses. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the outputs that result from the research. | |
| I agree to take part in the above research project. | |

| Name of Participant | Date | Signature |
|---|---|---|
| | | |

# Appendix VII: Demand-Side Survey Questionnaire

**Understanding Usability and Security Elements in the Use of Mobile Financial Services (MFS) Applications**

**Survey Questionnaire**

| **Supervisors: Dr. C Richardson, Dr. H. Dogan, Dr. E. Apeh, Prof. D. Osselton** | **PGR Researcher**: S.Ambore |
|---|---|

**Background**

**The mobile phone has changed the way we do things. One major area of change is the use of the mobile phone to conduct financial transactions in a way that was hitherto only possible in a physical bank. The use of mobile phones to provide financial services is known as Mobile Financial Services (MFS). MFS products include Mobile Banking (e.g easyMoney from Zenith Bank, and FirstMobile from First bank), Mobile Money (e.g Teasy,Paga) and Mobile Payment (readycash, easyPay).**

**We are interested in finding out how we can make these products more secure and easy to use for you. To achieve that we would like to learn from your experience of the use of MFS so far.**

**We also intend to enlighten you on a few things about threats you should be aware of when using MFS in the process of completing this questionnaire.**

**Your feedback is highly valuable in understanding how we can make these products serve you better.**

**Please be assured that any information that you provide in this questionnaire will be treated with utmost confidentiality.**

| **Section 1: Participants Details** | |
|---|---|
| **Age Range** | a. ☐ 18-24<br>b. ☐ 25-34<br>c. ☐ 35-44<br>d. ☐ 45-60<br>e. ☐ 61 and above |
| **Highest Qualification** | a. ☐ Primary School Certificate<br>b. ☐ Secondary School Certificate<br>c. ☐ Diploma Holder<br>d. ☐ 1st Degree (Bsc., Btech. HND. etc.)<br>e. ☐ Postgraduate Degree (PGD, Msc., PhD.)<br>f. ☐ Uneducated |
| **Occupation** | |
| **Sector** | |
| **Average Monthly income** | a. ☐ < ₦ 20,000<br>b. ☐ ₦ 21,000 – ₦ 50,000<br>c. ☐ ₦ 51,000 - ₦ 100,000<br>d. ☐ ₦ 101,000 - ₦ 250,000<br>e. ☐ ₦ 251,000 - ₦ 500,000<br>f. ☐ > ₦ 501,000 |

| **Section 2: Product type and means of use** |
|---|
| 1. I use this phone type? |

a. ☐ iPhone
b. ☐ Samsung
c. ☐ Blackberry
d. ☐ HTC
e. ☐ Others (please specify)

2. I use this Mobile Financial Services (MFS) product (select all that apply)
   a. ☐ Mobile Payment
   b. ☐ Mobile Money
   c. ☐ Mobile Banking
   d. ☐ Others(please specify)

3. I have been using MFS for
   a. ☐ ≤6 months
   b. ☐ 7-12 months
   c. ☐ ≥12 months and beyond

4. My decision to use MFS was influenced by (select all that apply)
   a. ☐ It is cheaper than other means
   b. ☐ It is more convenient than going to the bank
   c. ☐ Ease of use
   d. ☐ I can use it anywhere and at anytime
   e. ☐ Others (please specify)

5. I set up the MFS on my phone by
   a. ☐ Downloading from the apps store
   b. ☐ Installing via SDTK (SIM Development tool kit)
   c. ☐ Was done for me by service provider
   d. ☐ I am not sure
   e. ☐ Others (please specify)

6. I use this connectivity option to enable me access MFS on my phone
   a. ☐ Wi-Fi only
   b. ☐ Phone Data only
   c. ☐ Both Wi-Fi and phone data, but more of Wi-Fi
   d. ☐ Both Wi-Fi and phone data, but more of phone data
   e. ☐ Others(please specify)

7. I predominantly conduct a MFS transaction via (select all that apply)
   a. ☐ Contactless(scanning)
   b. ☐ USSD(SMS like payment instructions e.g. *776#)
   c. ☐ Mobile App (app installed on phone)
   d. ☐ Others (please specify)

8. I secure my MFS through the following means (select all that apply)
   a. ☐ Token
   b. ☐ PIN
   c. ☐ Biometry
   d. ☐ Others (explain)

**Section 3: Experience**

9. The MFS I use is
   a. ☐ Easy to navigate
   b. ☐ Complex
   c. ☐ Meets my needs
   d. ☐ Secure
   e. ☐ Others (please specify)

10. It is difficult for me to complete a task on the MFS I use
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

11. I often experience errors in my transactions
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

12. I often perform a single task several times due to the complexity of the MFS
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

13. I often perform a single task several times due to lack of sufficient knowledge
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

14. The most frustrating part of using the product for me is

| | | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagr |
|---|---|---|---|---|---|
| a | I frequently forget my PIN | | | | |
| b | Poor Network | | | | |
| c | Unsatisfactory level of support from operators | | | | |
| d | How to navigate the system | | | | |
| e | How to be sure I did the right thing with my transactions | | | | |
| f | Others (please specify) | | | | |

15. My financial details has been compromised via my mobile phone
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

**Section 3: Awareness**

16. I often share my phone with friends and family
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

17. I use the same PIN for my phone and MFS
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

18. I forget my MFS PIN
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

19. I write down my MFS PIN or secret questions somewhere in my phone so I don't forget
    a. ☐ Never
    b. ☐ Seldom
    c. ☐ Usually
    d. ☐ Often
    e. ☐ Always

20. Please select the indicator that you agree with the most for each item in the table below

| | | Strongly Agree | Agree | Neither Agree Nor Disagree | Disagr |
|---|---|---|---|---|---|
| a | PIN authentication is sufficient for me to access my MFS | | | | |
| b | I would need an additional level of authentication to PIN, to improve my confidence in the security of my MFS | | | | |
| c | My bank/operator responds speedily to any fraud related issues I raise to them | | | | |
| d | I know what to do to ensure no one accesses my sensitive financial details in the event I lose my phone | | | | |
| e | I know my responsibility as a mobile account owner | | | | |
| f | I know the banks/operators responsibility for ensuring I use MFS securely | | | | |
| g | I know how to escalate any issue to the banks/operators | | | | |

21. I can differentiate real Mobile apps from rouge ones
    a. ☐ Yes, my bank/MFS operator showed me how
    b. ☐ Yes, it is on the FAQ from my bank/Operator
    c. ☐ Yes, due to my awareness of cybersecurity and Information Technology
    d. ☐ Yes, based on URL
    e. ☐ Yes, based on source
    f. ☐ Yes, based on look and feel
    g. ☐ No, I cannot differentiate
    h. ☐ Others (Please explain)

22. Please select the indicator that tallies the most with your knowledge level of the items in the table below

| | | None | Basic | Average | A bit above average | Advanc |
|---|---|---|---|---|---|---|
| a | Ransomware | | | | | |
| b | Spyware | | | | | |
| c | Smishing (SMS phishing) | | | | | |
| d | Mobile Malware | | | | | |
| e | Rogue applications | | | | | |
| f | Cybersecurity | | | | | |
| e | Data Privacy | | | | | |

23. I received training/ sensitization on how to use MFS before I started using it
    a. ☐ yes
    b. ☐ No

23b. Training/Sensitization I received was sufficient
    a. ☐ yes
    b. ☐ No

24. I am aware that a procedure/process exists, to guide my action in the event I misplace my phone or suspicious transactions emanate from my phone
    a. ☐ Strongly Agree

b. ☐ Agree
c. ☐ Neither Agree nor disagree
d. ☐ Disagree
e. ☐ Strongly Disagree

25. No one else has access to my MFS account
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

**Section4: Maintenance**

26. I perform an upgrade of the Operating system I use for MFS
    a. ☐ As soon as it is available
    b. ☐ Never
    c. ☐ Seldom
    d. ☐ Always
    e. ☐ It is done automatically by my service provider
    f. ☐ I don't know

27. I perform an upgrade of the mobile application I use for MFS
    a. ☐ As soon as it is available
    b. ☐ Never
    c. ☐ Seldom
    d. ☐ Always
    e. ☐ It is done automatically by my service provider
    f. ☐ I don't know

28. The security of my MFS transaction depends on how often I update my mobile OS
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

29. The security of my MFS transaction depends on how often I update the mobile application I use for MFS
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

30. I use a phone antivirus
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

31. I update my phone antivirus
    a. ☐ Always
    b. ☐ Often
    c. ☐ Usually
    d. ☐ Seldom
    e. ☐ Never

**Section5: Usability**

32. I am satisfied with the reliability of the MFS
    a. ☐ Extremely satisfied
    b. ☐ Very satisfied
    c. ☐ Somewhat satisfied
    d. ☐ Not so satisfied
    e. ☐ Not at all satisfied

33. The MFS I use is easy to navigate
    a. ☐ Strongly Agree
    b. ☐ Agree

c. ☐ Neither Agree Nor disagree
d. ☐ Disagree
e. ☐ Strongly Disagree

34. I am satisfied with the available help options
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

35. The MFS I use is visually appealing
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

**Section6: Security**

36. The financial transactions I conduct using MFS are protected from unauthorised disclosures
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

37. The financial transactions I conduct using MFS are accurate and consistent throughout their life-cycle
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

38. The MFS service I use is available and is at the required level of performance at all times
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor Disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

**Section 7: Social Context**

39. I prefer a secure transaction than an easy to use MFS system
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

40. I will prefer an easy to use MFS than an MFS that is too complex to use because of security controls
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

41. I prefer an MFS system that is easy to use, yet secure
    a. ☐ Strongly Agree
    b. ☐ Agree
    c. ☐ Neither Agree Nor disagree
    d. ☐ Disagree
    e. ☐ Strongly Disagree

42. I am distracted or prone to making errors when conducting MFS transactions on my phone because of (select all that apply)
    a. ☐ In coming phone calls during transactions
    b. ☐ Environment of use

| |
|---|
| c. ☐ Low battery life<br>d. ☐ Weak network strength or poor network connectivity<br>e. ☐ Others (please specify) |
| 43. The maximum daily transactions limit set by my bank/operator on my MFS is<br>☐ Too restrictive, I want more with same level of security<br>☐ Too restrictive I want more with increased level of security<br>☐ Too restrictive, I want more with reduced level of security<br>☐ Too relaxed, I want more with increased level of security<br>☐ Just fine<br>☐ Others (please explain) |
| **Section 6:** Additional Information |
| Please provide any additional information you might like to share based on your experience with MFS products |

Thank you for contributing towards ensuring to a more user-centred and secure Mobile Financial Services applications.

# Appendix VIII: Supply-Side Survey Questionnaire

**Understanding Usability and Security Elements in the Use of Mobile Financial Services Applications**

**Semi-Structures Interview for MFS Developers and Solution Providers**

| **Supervisors: Prof. D. Osselton, Dr. C Richardson, Dr. H. Dogan, Dr. E. Apeh** | **PGR Researcher**: S.Ambore |
|---|---|

**Background**

**The aim of this survey is to understand the elements of mobile financial services that affects user experience and security of financial transactions using Mobile Financial Services (MFS) platforms. Mobile Financial Services which is the use of mobile phones for the purpose or financial transaction include: Mobile Banking Application, Mobile Money, Mobile Payment solutions using mobile phones.**

**Your feedback is high valuable in understanding usability and security elements that affect the use of these applications.**

| **Section 1: Participant Details** | |
|---|---|
| **Name** | |
| **Role/Position** | |
| **Years of Experience** | |
| **Phone** | |
| **Email** | |

| **Section 2: Process and procedure** |
|---|
| 1. What mythologies do you use in developing MFS products |
| 2. Describe the requirement elucidation process for the MFS product you provide for your customers |
| 3. Are there any guidelines, standards or regulation you adhere to in developing? |
| 4. How do you deploy update? ☐ As soon as there is a need. ☐ Update are done at a predetermined frequency |
| 5. How do customers get access to the solution: ☐ Push , ☐ Pull- Through Apps store ☐ Other means (State) |
| 6. Do you have any capability to manage the MFS product of the customer remotely? |
| 7. Do you have a mechanism for obtaining user feedback on their experience with the use of the MFS product? |
| 8. Describe your strategy/approach to user awareness on the use of the MFS |
| 9. Are customer aware of their responsibility and that of your organisation in securing transactions in MFS product |

| **Section 3: Usage** |
|---|

| |
|---|
| 10. How do you ensure security of transactions on MFS products: |
| 11. How do you ensure that users are comfortable using the solution in terms of ease of use, ease of learning, little or no error during transactions etc. |
| 12. From your experience how can you ensure effective security while improving user experience? |
| 13. Can your end-users identify between genuine MFP app and fake once? |
| 14. Are there any peculiarities with the use of mobile phone for financial transactions? |
| 15. Can MFS product users perform offline operations |
| 16. What specific element should be considered in ensuring financial transactions using mobile phone is relatively secure while not compromising ease of use of the solution |
| 17. In order of priority, least 5 elements that are crucial in usable security for MFS |

| **Section 4: Additional comments** |
|---|
| |

# Appendix IX: Heuristics Validation Questionnaire

**Development of Heuristics for evaluation of Usable Security of Mobile Financial Services (MFS) Applications**

**Semi-Structured Interview for validation**

**Researcher: Stephen Ambore**

| **Section 1: Participant Details** | |
|---|---|
| **Role/Position** | |
| **Years of Experience** | |
| **Field of Expertise** | |
| **Location (Work)** | |

| **Q 2: Please share your thoughts on evaluating usable security in Mobile Financial Services (50 words)** |
|---|
| |

| **Q 3: What is your perception on the impact of the following elements on usable security evaluation** |
|---|
| 1. Integrity |
| |
| 2. Proportionality |
| |
| 3. Transparency |
| |
| 4. Empowerment |
| |
| 5. Identity |
| |
| 6. Reliability |
| |
| 7. User Support |
| |
| 8. Accessibility |
| |
| 9. Authenticity |
| |
| 10. Compliance |
| |
| 11. Alignment |
| |
| 12. Freedom |

| |
|---|
| **Q 4: What other element would you like added to the list in Q3 above that can help the evaluation of usable security in MFS and why?** |
| |
| **Q 5: Are there elements in the list in Q3 that you believe should not be there? Which element(s) and why?** |
| |
| **Q 6: Please list all elements in Q3 including any one you have added in order of importance from the most important to the list important** |
| |
| **Additional Comment** |
| |

Thank you for your time and valuable feedback. Please be assured that we shall treat the information you have provided with utmost confidentiality.

# GLOSSARY

| # | Terminology | Description |
|---|---|---|
| 1 | Mobile Financial Services | The use of mobile phones to provide financial services. Mostly in the form of Mobile Banking, Mobile Payment or Mobile Money |
| 2 | Mobile Banking | Leveraging mobile phones to provide banking services for existing bank customers |
| 3 | Mobile Payment | Using mobile financial services for payment purposes. |
| 4 | Mobile Money | Using the mobile phone to provide financial services mostly for customers without a bank account |
| 5 | Usable Security | A human aspect of cybersecurity that focuses on the usability of security controls as a means to mitigate cybersecurity concerns |
| 6 | Financial Inclusion | Enabling access to financial services for economically active individuals through savings, payments, credit, insurance, or pensions |
| 7 | Unbanked | Economically active individuals without a formal bank account |
| 8 | Demand-side | Users of mobile financial services |
| 9 | Supply-side | Developers, administrators, testers and evaluators of mobile financial services. |
| 10 | DevOps | DevOps is a model that considers the supply-side of systems development which consist of developers, administrators and operations, and not treating those elements in isolation. |
| 11 | NASA TLX | The NASA Task Load Index (NASA-TLX) is an approach used to assess user workload. |
| 12 | Multi-Factor Authentication | This is an authentication method that requires users to have more than one method of authentication to have access to a system. |
| 13 | Two-Factor Authentication | This is a multi-factor authentication model that requires two authentication factors; usually who you are and what you have. |
| 14 | Heuristics | This is a model for decision making under uncertainty that requires lesser variables to make a decision when compared to conventional decision-making processes. |
| 15 | Heuristics evaluation | This is a usability testing approach that applies usability heuristics to identify usability problems in a system. |

| # | Terminology | Description |
|---|---|---|
| 16 | Hackathon | This is an innovative process that encourages the development of novel solutions. Participants are often expected to build a minimum viable product. Prize awards are given to top participants. |
| 17 | Black-box testing | This is a testing technique that does not require the understanding of the internal workings of the system. |
| 18 | White-box testing | This is a testing technique that reveals the internal logic of the system to be tested. |
| 19 | Fintech | Leveraging technology to develop unique financial solutions mostly to address niche areas. |
| 20 | Neobank | These are banks that leverage technology to provide financial services, without the full regulatory requirements of a conventional bank. |
| 21 | MoSCoW | “Must-have, should-have, could-have, won’t-have” (MoSCoW). It is an approach for prioritising solution requirements. |
| 22 | User acceptance test | This is a user-led test that assesses if the final products meet user requirements. |
| 23 | Test Script | Tool use for user acceptance test consisting of the various test conditions and test scenarios. |
| 24 | Human factors | The human element in a sociotechnical system. |
| 25 | Sandbox | A controlled environment that is isolated from regulation and market for the purpose of testing new innovations. |
| 26 | Test-and-learn | The process of testing a new solution in a controlled environment and addressing any observed market, operational or regulatory risks before full launch. |
| 27 | CERT | Computer Emergency Response Team is a team set up to manage computer related incidents. |
| 28 | Sociotechnical system | A system that has consideration for stakeholders and elements in a social interaction that leverages technology. |
| 29 | QR code | Quick Response (QR) code. Provides a capability to store and read data more efficiently than bar codes. One of its major applications is to drive contactless digital payment. |
| 30 | PCI DSS | Payment Card Industry Data Security Standard (PCI DSS) is a standard that guides card security in payment systems. |
| 31 | USSD | Unstructured Supplementary Service Data (USSD). Provides the capability for feature or basic mobile phone owners to leverage GSM network to send and receive |

| # | Terminology | Description |
|---|---|---|
| | | services using short codes. Most mobile money implementations in developing economies leverage USSD to reach the underserved. |
| 32 | SMS | Short Message Service (SMS). Enables message exchange between mobile phone owners. Financial services providers now leverage SMS to share financial information with customers. |
| 33 | API | Application Programming Interface (API). This provides a mechanism to integrate an existing function or module into a new one, in a reusable manner. MFS developers integrate security APIs to MFS to improve MFS security. |
| 34 | OTP | One Time Password (OTP). This is a multi-factor authentication approach that sends a one-time password to a user through a trusted channel to facilitate authentication. |
| 35. | TLS | Transport Layer Security (TLS). A security technique applied to mitigate the risk of data eavesdropping and man-in-the-middle attacks. |