A “Soft” Approach to Analysing Mobile Financial Services Socio-Technical Systems

Stephen Ambore, Christopher Richardson, Huseyin Dogan. Edward Apeh, David Osselton
Cybersecurity Unit, Bournemouth University,
Dorset, UK
{S. Ambore, C.J. Richardson, H. Dogan, E. Apeh, D. Osselton}@bournemouth.ac.uk

Advances in mobile computing have presented a huge opportunity to provide Mobile Financial Services (MFS) to half of the world’s population who currently do not have access to financial services. However, cybersecurity concerns in the mobile computing ecosystem have slowed down the adoption of MFS. The adoption of MFS is further hampered by the lack of a clear understanding of the interaction between the complex infrastructures and human factors that exist in the ecosystem for Mobile Financial Services Socio-Technical Systems (MFSSTS). This paper presents the work in progress of investigating the problem of MFSSTS. It discusses the preliminary results and understanding obtained from using Human Factor approaches to build and analyse the model for MFSSTS.

Mobile Financial Services, Human Factor, Socio-Technical Systems, Soft Systems, Interactive Management, Cybersecurity

1. INTRODUCTION

Mobile Financial Services (MFS): the use of mobile platforms for providing financial services e.g. Mobile Banking and Mobile Payments is changing the landscape of financial operations. It now presents an opportunity for providing financial services to half of the world’s population who hitherto had no access to formal financial services: the “unbanked” (David 2006; Chatain et al. 2008). Banks now use mobile platforms as a means to drive down costs and increase the uptake of financial products (Valcke, 2016). Perceived risks trust and culture has impacted users’ intention to adopt MFS (Gao et al. 2015; Slade et al 2015). However, concerns about security remain a major drawback to the adoption of MFS (Fed, 2015; Chatain et al. 2008).

According to Gartner, Mobile Banking needs an ecosystem to succeed (Simpson, 2007). However, the ecosystem for MFS Socio-Technical Systems (STS) is highly complex, as it involves interaction that cut across organisations, technologies and at times national boundaries with unaligned regulations (Carayon, 2006).For instance, a typical mobile money operation like money transfer can traverse several organisations, technologies and geographies, each with its own mode of operation, before it is consummated. A Socio-Technical System is a combination of a social system and a technical system (Whitworth, 2006).

Furthermore, the Human Factor elements remain a concern impacting the security of information flow within an ecosystem (Kraemer et al. 2003; Kraemer et al. 2009). While STS has been well researched, to the best of my knowledge, no previous research exists on developing and analysing a STS for MFS. Furthermore, no work has also been done to analyse the Human Factor elements with a view of understanding their security impact on the information flow within MFSSTS.

This work is aimed at providing an understanding of MFSSTS from key stakeholders’ perspective and their understanding of the key elements that affects cybersecurity in the ecosystem.

The overarching motivation for this research is to mitigate cybersecurity risks in MSFSTS, and boost adoption of mobile platform for financial inclusion.

This paper highlights the results and understanding obtained from the work in progress of using Human Factor approaches (Dogan et al. 2009; Kannan et al. 2014) to analyse the models for MFSTS. It continues in Section 2 by highlighting the methodology used. Section 3 discusses the preliminary results obtained. The paper concludes in Section 4 with a discussion of the next steps.

2. METHODOLOGY

The initial results are based on Soft Systems approach and Interactive Management Techniques. Soft Systems approach is an action-oriented

Proceedings of British HCI 2016 Conference Fusion, Bournemouth, UK

process of inquiry into ill-defined problems (Checkland et al. 2010). The approach was preferred to Hard Systems and other Human Factor approaches because it clearly defines conceptual problem from user perspective. The Rich Picture technique provides a pictorial view of key stakeholders and their interactions. 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 MFSSTS.

Interactive Management (IM) workshops (Dogan et al. 2009) were then conducted for all 6 identified stakeholder groups, with each group coming up with its Soft Systems Model (SSM) based on their understanding of the ecosystem for MFSSTS. Key elements of the models obtained from the workshops were then consolidated to come up with a unified SSM of the MFSSTS. Idea Writing (IW) was also used to analyse the Human Factor issues in the models of the MFSSTS they had derived. Nominal Group technique (NGT) was then used to derive the objective for mitigating these issues.

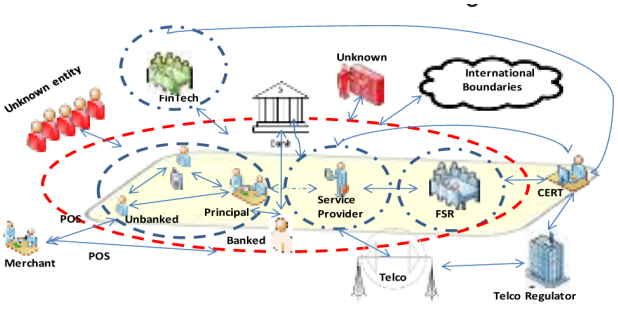
A total of 269 issues were generated from 30 participants in in the IW session. Furthermore, the 33 objectives for mitigating cybersecurity risk in the MFSSTS were generating from the NGT sessions.

Finally, Interpretive Structural Modelling (ISM) was used to identify relationships between the key objectives and how they influence each other. The technique helped to avoid focusing on solution even before critical analysis of the problem.

The outcome of the workshops is discussed in the next section.

3. SOFT SYSTEMS AND IM RESULTS

The results obtained from the developed SSM show that there are "unknown" entities within the MFSSTS whose characteristics and interest needs to be analysed. The SSM also shows that care should be given to managing service providers as they play in all autonomous groups. Further details of the complex interactions in the MFSSTS can be seen in the consolidated SSM model in figure 1.



*Banked: Bank accounts owners, Unbanked: No bank account, Principal: Mobile Money Operator, FS R= Financial Services Regulator CERT: Authorities responsible for cyber-incident management, POS: Point of Sale

Figure 1: *Consolidated MFSSTS, showing relationship and information flow within key elements*

The ISM model identified setting up an effective Cybersecurity Operations Centre as the most influential objective, while mitigation of risk with poor infrastructure and segregation of duty to mitigate insider abuse did not influence other objectives. Figure 2 highlights the most influential objectives and their relationships.

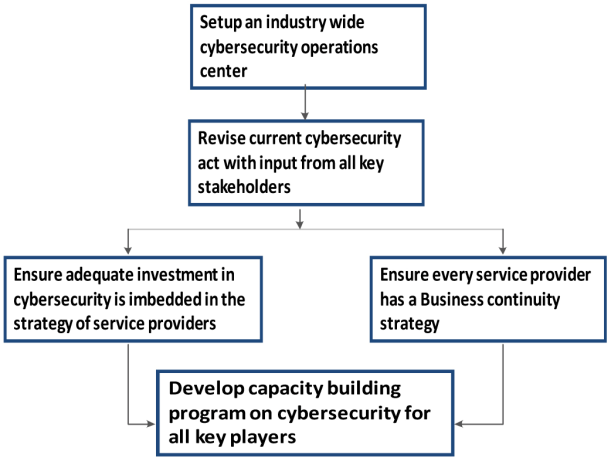


Figure 2: *ISM Model showing the most influential objectives of mitigation cybersecurity*

4. SUMMARY OF FINDINGS AND NEXT STEPS

This paper discussed the preliminary results obtained from using Human Factor approaches to build and analyse MFSSTS. Using Human Factor approaches has helped in the identification of key objectives for mitigating the cybersecurity concerns and risks in the interactions between the complex infrastructures and human behaviour in the ecosystem for MFSSTS. The relationships between the objectives were also identified. The setting up of a Cybersecurity Operations Centre was identified as the most influential objective for mitigating cybersecurity risks in the MFSSTS.

It was also discovered that unknown elements also play a significant role in the MFSSTS. The need to give great care to managing service providers as they were identified as being a key conduit of information within MFSSTS and thus having a high risk of being a single point of failure in the system was also highlighted.

Future work will seek to validate the developed MFSSTS models and the ISM model from this work with subject matter experts. The trustworthiness of the human factors elements identified within the MFSSTS will be further analysed, with a view to understanding the trusted and untrusted entities.

5. REFERENCES

David. P. (2006).The Enabling Environment For Mobile Banking In Africa, *Report Commissioned By Department For International Development (DFID).* Bankable frontier associates.

Chatain, P. L., Hernández-Coss, R., Borowik, K., & Zerzan, A. (2008). Integrity in Mobile Phone Financial Services. *World Bank Working Paper,* 146.

Valcke, J. (2016) Best practices in mobile security, *Biometric Technology Today*, Volume 2016, Issue 3, March 2016, Pages 9–11.

Gao, L., & Waechter, K. A. (2015). Examining the role of initial trust in user adoption of mobile payment services: an empirical investigation. *Information Systems Frontiers*, 1-24.

Slade, E. L., Dwivedi, Y. K., Piercy, N. C., & Williams, M. D. (2015). Modeling Consumers' Adoption Intentions of Remote Mobile Payments in the United Kingdom: Extending UTAUT with Innovativeness, Risk, and Trust. *Psychology & Marketing*, 32(8), 860-873.

Fed. (2015).The Federal Reserve report on *Consumers and Mobile Financial Services 2015* March 2015 page, 19,20.

Simpson, R. (2007). Mobile banking needs an ecosystem, as well as a platform, to succeed. *Gartner report* ID, (G00153070).

Carayon, P. (2006). Human factors of complex Socio-technical systems. Applied ergonomics, 37(4), 525-535.

Whitworth, B. (2006). Socio-technical systems. *Encyclopaedia of human computer interaction*, 533-541.

Kraemer, S., & Carayon, P. (2003). A Human Factors vulnerability evaluation method for computer and information security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 47, No. 12, pp. 1389-1393). SAGE Publications.

Kraemer,S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security*, 28(7), 509-520.

Dogan, H. Henshaw, M., & Urwin, E. (2009). A 'Soft' Approach to Requirements Capture to Support Through-Life Management.

Kannan, D. Diabat, A., & Shankar, K. M. (2014). Analysing the drivers of end-of-life tire Management using Interpretive Structural Modelling (ISM). *The International Journal of Advanced Manufacturing Technology*, 72(9-12), 1603-1614.

Checkland, P. & Poulter, J. (2010). Soft Systems Methodology. *In Systems approaches to managing change: A practical guide* (pp. 191-242). Springer London.