Designing for Cyber Security Risk-based Decision Making

Andrew W. M'manga

A dissertation submitted in partial fulfilment
of the requirements for the degree of
Doctor of Philosophy

Department of Computing and Informatics
Bournemouth University
January 2020

Abstract

Techniques for determining and applying cyber security decisions typically follow risk-based analytical approaches where alternative options are put forward based on goals and context, and weighed in accordance to risk severity metrics. These decision making approaches are however difficult to apply in risk situations bounded by uncertainty as decision alternatives are either unknown or unclear. This problem is further compounded by the rarity of expert security decision makers and the far-reaching repercussions of uninformed decision making.

The nature of operations in cyber security indicates that only a handful of systems are independent of the human operators, exposing the majority of organisations to risk from security threats and risks as a product of human decision making limitations. Addressing the problem requires considering factors contributing to risk and uncertainty during the early stages of system design, motivating the development of systems that are not only usable and secure, but that facilitate informed decision making as a central goal.

The thesis investigates this by posing the question; *what system design techniques should be taken into consideration to facilitate cyber security decision making during situations of risk and uncertainty?* The research was approached qualitatively with interviews as the main data elicitation approach. Grounded Theory was applied to five security decision making studies to inductively elicit, model, and validate design requirements for Risk-based Decision Making in cyber security.

Contributions arising from thesis work are: an identification of factors contributing to security analysts' risk practices and understanding, a model for communicating and tracing risk rationalisation by cyber security decision makers, a conceptual model illustrating the various concepts in cyber security decision making and their relationship, and guidelines and suggested implementation techniques guiding the specification of requirements for systems deployed in cyber security Risk-based Decision Making. The thesis is validated by applying the proposed design guidelines to inform an approach used to design a charity's secure data handling policy.

Dissertation Declaration

I agree that, should the University wish to retain it for reference purposes, a copy of my dissertation may be held by Bournemouth University normally for a period of 3 academic years. I understand that once the retention period has expired my dissertation will be destroyed.

Confidentiality

I confirm that this dissertation does not contain information of a commercial or confidential nature or include personal information other than that which would normally be in the public domain unless the relevant permissions have been obtained. In particular any information which identifies a particular individual's religious or political beliefs, information relating to their health, ethnicity, criminal history or sex life has been anonymised unless permission has been granted for its publication from the person to whom it relates.

Copyright

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and due acknowledgement must always be made of the use of any material contained in, or derived from, this thesis.

Requests for Information

I agree that this dissertation may be made available as the result of a request for information under the Freedom of Information Act.

Signed:
Name:
Date:
Programme:

Dedicated to Mom and Dad
I know you are watching over us

Acknowledgements

I would first like to thank my main Supervisor, Dr Shamal Faily for his unwavering support and guidance throughout the course of my study. I would also like to thank my second and third supervisors Professor Vasilis Katos and Dr John McAlaney, and my industrial supervisor Dr Chris Williams for there excellent advice, I was privileged to have a team that was truly their for me. A special thanks to all the members of the Bournemouth University Cyber Security Research Group.

I am also grateful to Bournemouth University and the Defences Science and Technology Laboratory (dstl) for funding the doctoral studentship.

Thank you to my parents for creating the foundation that has brought me this far, I know you would be proud.

Finally, I would like to thank my wife Caroline; my main source of motivation, leading critic, and the best teammate. It has been quite an adventure.

Original Work Declaration

This dissertation and the project that it is based on are my own work, except where stated, in accordance with University regulations.

Signed:

Contents

List of Tables

List of Figures

Acronyms

BOW	Best-Optimal-Worst
CDM	Critical Decision Method
CERT	Computer Emergency Response Team
CSE	Cognitive Systems Engineering
CSIRT	Computer Security Incident Response Team
CWA	Cognitive Work Analysis
DDoS	Distributed Denial of Service
DiCoT	Distributed Cognition for Teamwork
dstl	Defence Science and Technology Laboratory
GDPR	General Data Protection Regulation
GORE	Goal-Oriented Requirements Engineering
GRL	Goal-oriented Requirement Language
HCI	Human-Computer Interaction
IDS	Intrusion Detection System
IRC	Internet Relay Chat
IRIS	Integrating Requirements and Information Security
IS	Information Systems
ISP	Internet Service Provider
IT	Information Technology
KAOS	Knowledge Acquisition in autOmated Specification
NDM	Naturalistic Decision Making
OODA	Observe Orient Decide Act

RBDM	Risk-based Decision Making
RIDM	Risk-informed Decision Making
RPD	Recognition Primed Decision
RRF	Risk Rationalisation Flow
RRP	Risk Rationalisation Process

Chapter 1

Introduction

1.1 Thesis motivation

While the ever increasing number of security breaches in organisations can hint at a lack of security analysts' technical know knowledge, a growing attack surface and threat landscape (TalkTalk 2015, Mossack Fonseca 2016, Equifax 2017, Quora 2018), recent attacks cast doubt on the nature of decision making during security operations; raising the question - what factors do organisations consider when addressing risk and uncertain conditions?

To illustrate, compare the difference between Uber and Clarkson's (a shipping company) responses to ransom requests after the two companies were breached. Uber paid the attackers $100,000.00 to delete the stolen data but was later fined $148,000,000.00 by the Information Commissioner for breaching regulations (Lee 2018), while Clarkson refused to be held to ransom and made the news of the attack public. There is so far no adverse information on Clarkson's course of action (Davies 2017).

Security analysts are experts who review system environments by collecting and analysing data to provide insight into implementing and improving security. To maintain security, analysts use a variety of tools to facilitate decision making typically approached through the use of risk management standards and procedures (Fenz et al. 2014). The analysts' role is crucial in areas where automation cannot be applied fully or human intervention is necessary (human in the loop). While human intervention is of paramount importance, it is the mutual human-computer relationship that elevates awareness and facilitates decision making.

The systems-security relationship has generally been identified to have three user groups (Smetters and Grinter 2002). These are, the developers who implement security require-

ments at design, the security analysts who oversee the systems security infrastructure by enforcing and maintaining security rules, and the end users who (presumably) abide by the security rules. Despite the identification of the three user groups, there is a paucity of research focussing on design to facilitate the security experts' decision making (Flechais and Sasse 2009, Green and Smith 2016), and more so, from a Cognitive Systems Engineering perspective (Wilson et al. 2013).

Unlike traditional User-centered design approaches, Cognitive Systems Engineering considers cognitive requirements and the context within which decisions occur. Cognition relates to how people think and what they know, how they organise and structure information, and what they seek to understand better (Crandall et al. 2006, p. 3). Cognitive Systems Engineering focusses on the early stages of design, which implies addressing the rationale (why) behind the selection of certain design options, differing from later stages of design that address the "how" of design (Yu 2011). By focussing on the early stages, Cognitive Systems Engineering takes wider cognitive complexities in socio-technical systems into account, as opposed to the narrower user interaction view adopted by later-stage approaches focusing on Human Computer Interaction (HCI) design features (Roedl and Stolterman 2013).

Designing for Risk-based Decision Making (RBDM) means considering various forms of risk and uncertainty and providing reasonable assurance that design requirements for informed decision making are in place. Recent work on usable security (Faily 2018) has demonstrated how security and usability requirements may harmoniously be integrated during the early stages of design. Drawing inspiration from this, the aim of this research was identifying how RBDM may be facilitated during the early design stages. Requirements were elicited by investigating the decision making activities of security analysts.

Considering risk and uncertainty during the early stages of design has long been appreciated in industries with low error acceptance rates such as the safety-critical sector (Johnson et al. 2013, Lin et al. 2015). Here, they aim to address risk as early as possible with systems designed towards reducing error rates and attaining quick user response times (Fisher and Kingma 2001). It may be argued that the error threshold is relatively higher in non-safety-critical settings and that the response time is not as vital. However, this becomes trivial given the low-risk threshold prevalent in security, where it only requires one weak link to exploit an entire system (Sasse et al. 2001). Given the case, a call for approaches facilitating design for Risk-based Decision Making in cyber security is warranted.

1.2 Research question

What system design techniques should be taken into consideration to facilitate cyber security decision making during situations of risk and uncertainty?

The research question is broken into the following, aimed at addressing three main research areas illustrated in Figure 1.1.

- **Aim 1:** Identify factors influencing risk analysis practices deployed by cyber security risk-based decision makers.
- **Aim 2:** Propose approaches for adapting cyber security decision making techniques to design.
- **Aim 3:** Propose approaches supporting the specification of design requirements for systems facilitating cyber security Risk-based Decision Making.

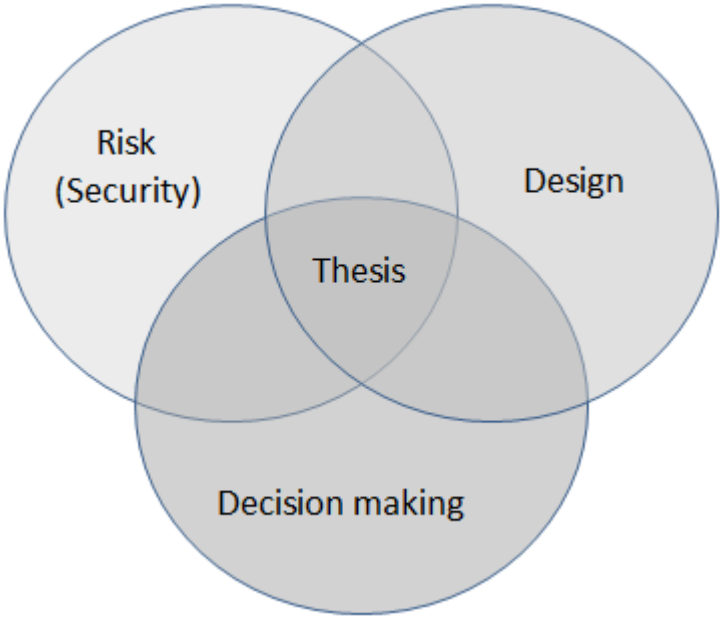


Figure 1.1: Research areas

1.3 Contributions

The principal claim of this thesis is the presentation of complementary elements supporting the specification of design requirements for systems deployed in cyber security RBDM. The contributions consists of:

- An identification of factors contributing to security analysts' risk practices and understanding.
- A normative model for communicating and tracing risk rationalisation by cyber security decision makers.
- A conceptual model illustrating the various concepts in cyber security decision making and their relationship.
- Guidelines and suggested implementation techniques guiding the specification of requirements for systems deployed in cyber security RBDM.

Based on our research dissemination activities (see Section 1.5), the assumption has sometimes been that the research is addressing RBDM in design as opposed to design for RBDM. While the two have similar research areas (see Figure 1.1), RBDM in design aims at investigating approaches for reducing risk in design; problems are from the design domain and solutions are for decision making (risk analysis approaches). Contrarily, design for RBDM aims at investigating approaches for reducing risk in decision making during system operations; problems are from the decision making domain and solutions are for design (design recommendations).

1.4 Organisation of the dissertation

The dissertation overview is illustrated in Figure 1.2 and detailed below.

Chapter 2 presents a literature survey covering the state-of-the-art in the three main research areas. Concepts from risk and its relation to security are reviewed before reviewing relevant concepts from decision-making focussed on human cognition. Next, approaches from User-Centered design are reviewed and the chapter concludes with reflections.

Chapter 3 describes the research approach supporting the thesis from a philosophical and methodological perspective. It presents the rationale behind the adoption of the research approach by considering identified gaps between decision making and design research.

To address the research gap in Chapter 2, empirical research is carried out in Chapter 4 to understand risk analysis practices deployed by cyber security risk-based decision-makers. The chapter reports on decision making from two risk analysis studies; first proactive and then reactive.

Chapter 5 builds on research in chapters 2 and 4, and is the first of two chapters aiming at adapting cyber security decision making techniques to design. The chapter presents a normative model for communicating and tracing the rationalisation of risk by cyber security decision-makers. The chapter discusses the model's design, before concluding with two validation studies.

Chapter 6 builds on findings from Chapter 5 and is the second aiming at adapting cyber security decision making techniques to design. It presents a conceptual model for designing for RBDM, illustrating the various concepts in cyber security decision making and their relationship. First, an integrated model is presented, before detailing and justifying the concepts in related sub-models using adaptations of events surrounding a Distributed-Denial-of-Service attack on a real organisation.

Chapter 7 instantiates the conceptual model presented in Chapter 6 by presenting design guidelines and suggested implementation techniques guiding the specification of requirements for systems deployed in cyber security RBDM. The chapter first presents the rationale behind guideline selection before detailing the guidelines.

Chapter 8 presents a case study used to validate the guidelines presented in Chapter 7 as a cumulation of work presented in this dissertation. This chapter reports on how the guidelines were used to inform an approach used to design a charity's secure data handling policy.

Chapter 9 concludes the dissertation by providing key research findings. It evaluates how the overall research question was satisfied, provides suggestions for future work, and closes by re-emphasizing the relevance and value of the research contribution.

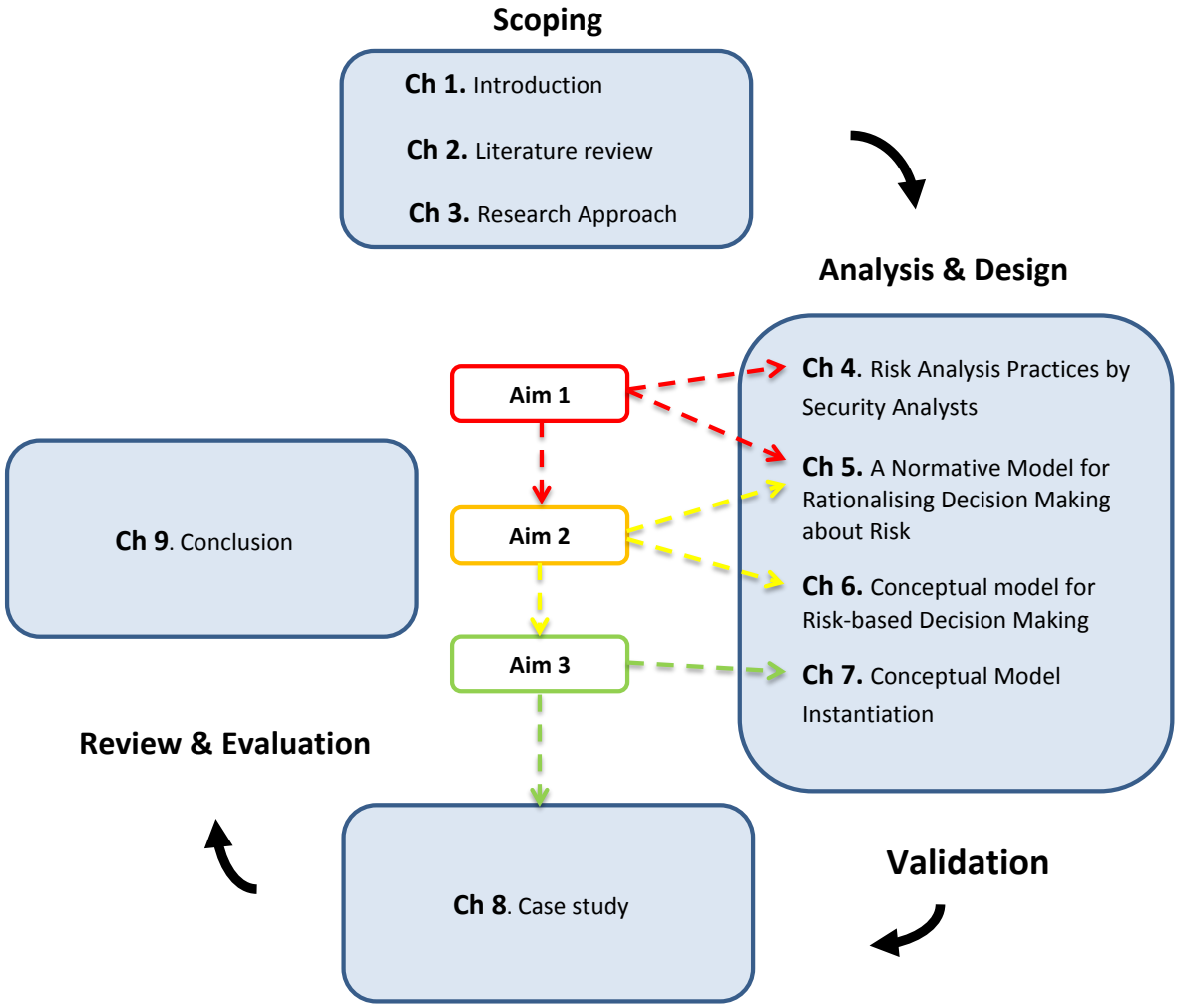


Figure 1.2: Dissertation overview

1.5 Publications arising form thesis work

This section presents material in Chapters 4 to 6 that have been published in peer-reviewed journals, conference proceedings and workshops.

- M'manga, A., Faily, S., McAlaney, J., and Williams, C. 2017. Folk Risk Analysis: Factors Influencing Security Analysts' Interpretation of Risk. In Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS). Online proceedings. *Contributing to Chapter 4
- M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y., and Miyamoto, D. 2018. Qualitative Adaptation: Informing Design for Risk-based Decision Making. In Proceedings of the 32nd International BCS Human Computer Interaction Conference. Online proceedings. *Contributing to Chapter 4
- M'manga, A., Faily, S., McAlaney, J., Williams, C. 2018. Rationalising Decision Making about Risk: A Normative Approach. In Proceedings of the 12th International Symposium on Human Aspects of Information Security & Assurance (HAISA), pp. 263-271. *Contributing to Chapter 5
- M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y., and Miyamoto, D. 2019. A Normative Decision Making Model for Cyber Security. Journal of Information and Computer Security. In press. *Contributing to Chapter 5
- M'manga, A., Faily, S., McAlaney, J., and Williams, C. 2017. System Design Considerations for Risk Perception. In Proceedings of the 11th IEEE International Conference on Research Challenges in Information Science, pp. 322-327. *Contributing to Chapter 6

1.6 Chapter summary

This chapter introduced the research upon which the thesis is founded. This included the research motivation and the research question and related aims. The chapter presented an overview of the research themes, identified the main research contributions and elaborated what the thesis addresses. In summary, The dissertation investigates how to effectively embed RBDM within cyber security system design.

Chapter 2

Literature Review

2.1 Outline

In this chapter reviews the state-of-the-art in three research areas contributing to designing for RBDM in cyber security, namely risk and security, decision making, and User-Centered design.

The justifications for selecting the three areas are; to design for cyber security risk-based decision-makers, the nature of activities and the risks the decision-makers address must first be understood. This required a review of the fundamental meaning of risk in general, and risk as it relates to cyber security. Because the research aims to provide design recommendations for systems facilitating human decision making, work that investigates cognition and decision making is then reviewed to understand how it may be used to facilitate design. While, it is appreciated that social factors such as team collaboration (Champion et al. 2012, Buchan and Taylor 2016) or Groupthink (Turner and Pratkanis 1998) play a role in decision making, the research scope focusses on the individual decision-makers, however, investigations shall be made on how the findings translate to team/group decision making in future work. Next, the body of work on systems design under the User-Centered design philosophy is reviewed with the aim of identifying best practice for eliciting and specifying design requirements. In conclusion, a brief review on the relationship between automation and decision making is presented.

The identification of literature was based on keyword (and combinations) searches in academic databases and search engines. These include ACM Digital Library, IEEE Explore, ScienceDirect and Scopus for computing publications, and PsycINFO, PsycBOOKS, PsycARTICLES, and APA PsycNET for psychology related publications. Snowballing from one publication to another was also used where necessary. Due to the interdisciplinary nature of the research, keywords used were sometimes specific to a dis-

Sample Keyword Search
Risk
Risk analysis
Risk perception
Risk-based decision making
Situation awareness
Contextual awareness
Uncertainty
Decision making
Naturalistic decision making
Security analyst activities
Security information workers
Decision automation
Design for security
Design for decision
Human cognition
User centered design

Table 2.1: Sample literature survey keywords

cipline. Where non-specific keywords were used, searches were repeated in different disciplinary databases due to difference in application and translation of terms. For example, a search for the keywords “risk decision making” in Computing databases generally returned publications on the application of risk approaches in decision making, while psychology databases returned results on understanding the root cause for a decision in risky situations. Table 2.1 provides sample keywords used in the literature survey.

Contributions from this chapter are in the presentation of the state-of-the-art and the identification of limitations in the research areas in facilitating design for cyber security RBDM - upon which the thesis is motivated.

2.2 Risk

This section aims to bring out an understanding of risk decision making in cyber security. To do this, the first goal is to gain an understanding of the fundamental meaning of risk and uncertainty; from which, RBDM is derived, and the second goal is to investigate RBDM in relation to the security analysts.

2.2.1 Risk and uncertainty

The meaning of risk has been the bone of contention for many years (Adams 2012, Fischhoff et al. 1984). Originally risk was viewed as the probability of something adverse happening (Royal Society 1983, Fischhoff and Kadvany 2011). This view presented the notion of unwanted outcomes to uncertainty. In recent years, the meaning has changed to include positive future outcomes to uncertainty, thus promoting neutral sounding risk definitions like “effect of uncertainty on objectives” (ISO 2009).

Risk is divided into objective and perceived risk (Royal Society 1983). Objective risk refers to the scientific understanding of risk that is capable of measurement such as insurance and public health. Perceived risk relates to the subjective assumptions people hold (Fagan and Khan 2016). Perceived risk is characterised by ideologies and beliefs such as the assumption that risk is low when benefit is high, and high when benefit is low.

In the 1738 study, later known as the Expected Utility theory (Bernoulli 1954), Bernoulli observed that objective and perceived risk are actually complementary and not mutually exclusive. He stated that although people may be faced with the same uncertainties, the willingness to take risks is based on the rational judgement on individual circumstances and not just the perceived gain.

More recently, the Prospects theory has taken this further by suggesting that risk decision making is sometimes not a rational process, but that decisions are made based on a reference point (Kahneman and Tversky 1979, Kahneman 2003). For example, a person who has won one bet may bet again in the belief they are likely to win again, even though the second bet is completely independent (in probability terms) from the first.

Bernoulli and Kahneman’s theories exemplify the difference between normative and descriptive approaches to decision making (see Section 2.3.1), where the first tries to identify optimal choice while the latter scrutinises real-life choices. However, the two theories do not fully consider uncertainty as they are posited on the premise that probabilistic alternatives are known before decisions are made.

Uncertainty is a view held regardless of the nature of the risk (wanted, unwanted, objective and perceived). Adams (1995) differentiates the meaning of risk and uncertainty by stating that risk is when the odds are known, but the actual outcomes are unknown (known probability of outcome). For example, there is a chance that system security will be compromised, how that might happen is unknown but we can identify probable vectors of compromise. Uncertainty is when both odds and outcomes are unknown (un-

known probability of outcome). For example, when might the compromise happen and what might the impact be? The idea that risk and uncertainty as separate factors may be traced back to Frank Knight's 1921 publication on economics (Knight 2009) where he argued that risk is a value susceptible to measurement, while uncertainty is not.

Like risk, uncertainty has also been divided into subcategories, the two most common being aleatoric; resulting from randomness, and epistemic; resulting from a limited data of knowledge. From a statistical perspective, the two are essential in calculating probability, however, the dissertation's interest lies in the understanding that epistemic uncertainty is subjective and varies from person to person, while aleatoric is not (O'Hagan 2004).

2.2.2 Risk-based Decision Making

The body of work in security fails to present a substantial definition for the term "Risk-based Decision Making". This may be attributed to the fact that security is synonymous with risk and the literature narrative has focussed on decision making in security, where risk is implied, or the literature has focussed on risk, where decision making is implied. This differs from the safety-critical literature, where the focus is on safety and not security. Here RBDM is used to describe a process where a set of alternatives are considered during risk response to arrive at optimal choice (Lin et al. 2015, Macesker et al. 2002).

Though a consensus on the definition of RBDM does not seem available, the one posed by the U.S coast guards appears widely accepted. They define RBDM as *"the process that organises information about the possibility for one or more unwanted outcomes to occur into a broad, orderly structure that helps decision makers make more informed management choices"* (Macesker et al. 2002).

An alternative to the use of RBDM, has been to substitute it for the term risk-informed decision making (RIDM) Ersdal and Aven (2008). Here too, the literature lacks a consensus as to whether RBDM and RIDM are indeed interchangeable terms. The opposing school of thought view RBDM processes as limited to technical analysis that do not consider wider contextual factors and deliberation (Stamatelatos et al. 2006, Dezfuli et al. 2010). Following these lines, RIDM has been defined as *"a deliberative process that uses a set of performance measures, together with other considerations, to inform decision-making*" (Dezfuli et al. 2010)

Based on this analysis, both the definitions presented above are deemed unsuitable for this research. The RBDM definition suggests a process where information is structured

broadly and orderly for management decision making. Risk-based Decision Making is not exclusive to management decision making and organising information in broad and orderly structures is sometimes not possible during uncertainty. On the other hand, the RIDM definition is presented in a neutral form that does not capture the presumption of risk or uncertainty, but rather focusses on performance measures.

As an alternative, the following working definition is proposed: *"an endeavour to make an informed decision on the possibilities of uncertain and undesired outcomes".* The proposed is considered suitable as it does not limit the definition to management choice, it does not assume information availability and structure, and it captures the requirement of making an informed decision without overlooking the risky and uncertain environment within which the decision is made.

2.2.3 Risk and security

This section builds on the understanding of risk and uncertainty from the precious sections by exploring risk in security with a focus on the analysts. The section first clarifies who the security analysts are, before exploring their activities as reported by the literature. The section concludes by reporting on challenges to eliciting security knowledge from analysts - knowledge essential for informing design for RBDM.

2.2.3.1 The security analyst

Understanding security experts and considering techniques for facilitating their operations is a growing research area (Werlinger et al. 2010, Sundaramurthy et al. 2015, Hibshi et al. 2016). This may be attributed to the realisation that it is not only the novice (Furnell 2005), but even experts require usable security (Chiasson et al. 2007), and the increasing focus on human aspects of security in academic forums (USENIX 2018, HAISA 2019). It is worth noting that not all security experts are equal, warranting the clarification of who a security analyst is.

The researcher's understanding of security analysts is expressed in the Workshop on Security Information Workers' (WSIS 2018) definitions of intelligence analysts, and that of Security and system administrators which are; "one who collects and analyses data about security matters to understand information and make predictions", and "one who deploys and manages security-sensitive software and hardware systems".

Campbell et al. (2015) proposed a model for matching one's 'critical thinking abilities' to cyber security job roles which could equally be used to represent the analyst's role. Illustrated in Figure 2.1, the critical thinking abilities they identified are: *Proactive* - ability to

hypothesize possible outcomes and come up with solutions, *Reactive* - vigilance and an ability to detect anomalous activities, *Deliberate* - critical thinking ability, and *Real-time action* - ability to act quickly and accurately. Matching the critical thinking abilities to the analyst's role would clearly result in overlaps, however, analysts would typically fall under the horizontal axis in Figure 2.1, with work activities related to real-time defending and deliberations on exploitations.

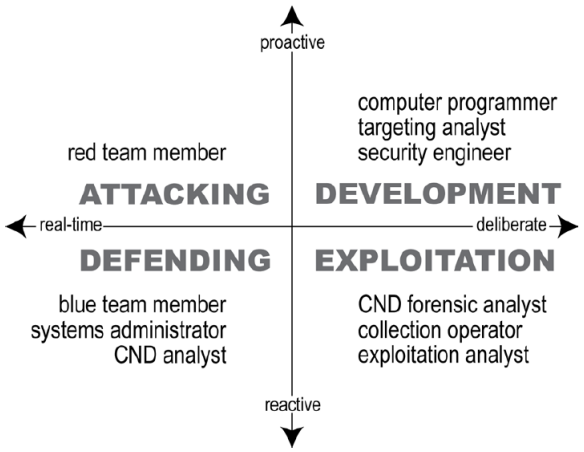


Figure 2.1: Cyber Aptitude and Talent Assessment (Campbell et al. 2015)

2.2.3.2 Security analysis activities

The previous section hinted on security analysis activities while defining who the analysts are. In this section, we review the analysts' activities as reported by the literature.

Li et al. (2010) discussed risk and uncertainty from a cyber situation awareness perspective and grouped analysts' activities as prior security management, real-time intrusion and detection, and posterior forensic analysis. They state that prior security management activities occur before an incident and dwell on identifying the likelihood of exploitation based on inherent system weaknesses (static uncertainty). In real-time intrusion and detection, activities focus on the unpredictable nature of the threat environment such as when or how an attack would occur (dynamic uncertainty). Lastly, the activities in forensic analysis also focus on dynamic uncertainty as analysts explore data to establish the whys and hows of an incident.

Investigations on analysts' workflows and decision processes by D'Amico et al. (2005) concluded that tasks vary from organisation to organisation, but six functions distinctly describe analysts' work processes. These are *Triage analysis*; the weeding of false positives and escalation of suspicious activities. *Escalation analysis*; investigating potential

incidents from triage and tip-offs. *Correlation analysis*; searching for patterns and trends in data and related incidents. *Threat analysis*; using additional data sources for intelligence. *Incidence response analysis*; recommendation or implementation of a response to a confirmed incident. And *forensic analysis*; gathering and preserving evidence for investigation.

Though other investigations on analysts' activities have mostly touched on points highlighted above (Werlinger et al. 2010, Grispos et al. 2015, Gutzwiller et al. 2016, Bridges et al. 2018), there are subtle differences in focus. For example, Li et al. (2010) focussed on phases pre-to-post incident, while D'Amico et al. (2005) focussed on analysis tasks. In Addition, Li et al, aim to highlight the nature of uncertainty, while the D'Amico et al, have it implied in risk.

Adnan et al. (2015) proposed a work practices model in a bid to introduce conformity to the presentation of analysts' activities and noted that research has mainly focused on monitoring activities (a part of incident detection) and incident containment (a part of incident analysis), while analysts' training and awareness activities are mostly overlooked.

While these examples highlight the different analysts' activities from a research point of view, overlaps would be expected in practice as an analyst could cover multiples roles and the activities may not be so well defined.

2.2.3.3 Eliciting security knowledge

There have been multiple research efforts exploring analysts' risk decision making. While research interests have been different, the general goal has been in understanding the analysts' risk perception and response thereof. A question posed by the researcher when reviewing the literature was; what is an effective approach for eliciting analysts' security knowledge?

For the most part, studies have used interviews and/or questionnaires for elicitation and a variety of techniques for analysis e.g., situation awareness (Hibshi et al. 2016), Grounded Theory (Botta et al. 2007), card sorting (Paul and Whitley 2013), and critical incident reviews (D'Amico et al. 2005). It is noted that studies using observation for elicitation e.g., Kandogan and Haber (2005) and Sundaramurthy et al. (2014) are less common and reasons expressed have included analysts unavailability for studies. Kotulic and Clark (2004) expresses that the overarching problem in security research is the sensitive nature of security operations that cause a general mistrust of outsiders, making empirical research difficult.

2.2.4 Risk summary

This Section reviewed the meaning of risk and uncertainty and identified how they relate to RBDM in cyber security by providing a working definition. The review touched on the analyst' activities and the elicitation of their knowledge.

Based on these finding, it becomes clear that identifying an effective approach for eliciting analysts' security knowledge is only part of the requirement, overcoming the analyst availability problems is also an area of concern. D'Amico et al. (2005) demonstrates that the use of hypothetical scenarios (Section 2.4.2.1) addresses some of the concerns as scenarios have proven effective at reducing sensitivity in security and promote discussions. However, solutions to the analyst unavailability problem are yet to be identified.

2.3 Decision making

In this section, techniques used for analysing and understanding human cognition and decision making are reviewed with the aim of understanding how they may be used to facilitate design for RBDM. The review begins by reviewing the differences in normative, descriptive, and prescriptive decision theories, before reviewing research on human perception and judgement. Next, the section reviews perspectives to decision making and awareness models, and concludes by reviewing context-oriented approaches to decision making.

2.3.1 Decision theory

Decision theory looks at decision making from three perspectives, namely normative, descriptive (Kahneman and Tversky 1979), and prescriptive (Bell et al. 1988). As alluded to in Section 2.2.1, the normative perspective focus on how decisions should be made in respect to rational choice, while the descriptive perspective reflects decisions people actually make. Normative methods can be a measure of what design for decision making should aspire to promote, while descriptive methods provide case-specific insight on areas that require improvement. On the other hand, the prescriptive perspective refers to the investigation and development of models and decision aids for facilitating better choice.

Distinctions in the three perspectives are also seen in their evaluation. Normative methods are evaluated by their theoretical adequacy, descriptive methods by their empirical

validity and prescriptive methods by their ability to aid and improve decision making (Bell et al. 1988).

2.3.2 Perception and judgement

This Section reviews human perception and judgement as it relates to heuristics, biases and mental models, and concludes by reviewing the criticisms to this line of research.

2.3.2.1 Mental models

When encountering uncertain environments lacking established norms, decision-makers depend on their perception to analyse and interpret environments (Endsley 1995). Perception is driven by a cognitive blueprint known as a mental model. In other words, mental models are a cognitive way of understanding one's environment through logical mapping and are a product of one's knowledge and beliefs (Gentner 2001). This may be a security analyst working-out system functionality or picking out cues in unfamiliar network activities based on known patterns. As a conceptual product of one's experience, training, and beliefs, mental models constantly evolve as new knowledge is acquired. Similarly different mental models are developed for different systems and processes.

Mental models may be categorised into two groups. The first is task-based where the decision maker has little to no knowledge on a system's or an environment's internal workings, so they operates through memorised sequences. The second is based on knowledge of components, processes and their interrelation (Carroll et al. 1987). When driven by knowledge, the decision maker has a better understanding and easily updates the model as new information is acquired (Johnson and Seifert 1994).

Design for decision making should, therefore, aspire to design systems where the knowledge driven mental models are attainable. However, mental models raise a few questions for system design. Should system models be designed to match the decision-maker's perceived model, be simplified to ease understanding, or should the decision-maker be expected to learn system models proposed by designers?

2.3.2.2 Heuristics

When faced with time limitations, decision-makers validate their hypothesis by matching the limited available information against known patterns (part of their mental model) to arrive at conclusions. The matching is a form of mental shortcut subconsciously taken to quickly solve problems. For example, Werlinger et al. (2010) report that security analysts identify attack activity just by spotting Internet Relay Chat (IRC) traffic on a network.

Tversky and Kahneman (1973) referred to these processes as judgement heuristics and explained that although heuristics provide quick answers when time is limited, they are sometimes imperfect (Kahneman 2011, Fiske and Taylor 2013). For example, non-malicious Twitter traffic could be flagged as malicious due to its popularity among hackers.

This example illustrates the representative heuristic, where decisions are influenced by a supposed representative sample. The decisions are not completely intentional, but subconsciously triggered by quick evaluation and promoted by time limitations. The representative heuristic is one of three heuristics initially proposed by Tversky and Kahneman (1974). The other are the availability heuristic, and the adjustment and anchoring heuristic (Tversky and Kahneman 1974). Continued research by Finucane et al. (2000), Gilovich et al. (2002) has seen additional heuristics identified.

2.3.2.3 Biases

The reliance on imprecise information for decision making leads to systematic errors known as decision biases. Biases are a product of inaccurate mental models, heuristics and other personal factors (Kahneman 2011). In the framing bias, for example, a decision maker's risk tolerance may be influenced by how a set of options are described. Compare an intrusion detection system (IDS) that reports 40% of incoming traffic as malicious, to one that reports 60% of incoming traffic as non-malicious. In essence, the two systems are reporting the same information, however, an analyst's interpretation of the two may differ (Kahneman and Tversky 1979). Biases are not always coincidental as they may sometimes be the product of conscious and deliberate action. For example, the confirmation bias may be the product of actively seeking out evidence that supports an inaccurate or false claim (Nickerson 1998, Endsley 2018).

2.3.2.4 Heuristics and biases criticism

The research on heuristics and biases has not been without its criticisms. In its support is the view that it is better to wrongly assume an incident is imminent than to ignore an actual one and suffer the consequences (Nesse 2005).

In contrast, the opposing view claims that heuristic and biases are actually not errors in judgement but results of narrowly focused research. They state that the design of the experiments used for these studies have embedded shortcomings. Usually, participants are requested to select between two options having one correct answer, this does not reflect true probability (statistical) which dwells on frequencies and not single true or false events (Gigerenzer 1991). It has also been argued that heuristics and biases are prod-

ucts of experimental designs that cannot be replicated in natural settings (Fraser et al. 1992, Kahneman and Klein 2009).

Fundamentally, heuristics and biases are not different from each other. When they work they are seen as a good thing and called a heuristic, but when they do not work and lead to an incorrect decision they are called a bias.

2.3.3 Perspectives to decision making

An alternative research approach on decision making is based on analysing the context, or in other words, the circumstances under which the decisions are made. Broadly put, this may be divided into Rational (Simon 1972) and Naturalistic Decision Making (NDM) (Klein 1999) discussed in this section.

2.3.3.1 Rational decision making

Rational decision making focuses on the information availability context. It exemplifies seeking the best course of action to meet one's objective through informed analysis. The assumption is that through the collection of information, decision makers generate a picture of the environment they wish to act on. Once adequate information has been collected, decision alternatives are identified, weighed and the most realistic (satisfactory) option for achieving the desired goal is selected.

The opposite of rational decision making is decision making under bounded rationality. These are situations where decision-makers aim at selecting the best option from a limited information spectrum. Selection is based on "satisfising" which denotes achieving a reasonable result albeit knowing its deficiencies (Simon 1972). Below, we describe the Decision Ladder Template, a model representing the normative and rational perspectives.

Decision Ladder Template

The decision ladder template (Figure 2.2) represents rational decision making by illustrating the generic steps necessary for decision making. The ladder comprises boxes representing information processing activities, and ovals representing states of knowledge that are outputs of the activities. The left side of the ladder represents observation of the current state (situation analysis), and the right represents planning and execution of actions. Rational decision making is sequential; passing through every node of the ladder, however, experience can lead to shortcuts in decision making represented by arrows in the centre on the ladder (Rasmussen 1974, Lintern 2010). Application of the Decision Ladder Template to understanding security decision making includes research by Gerber et al. (2016).

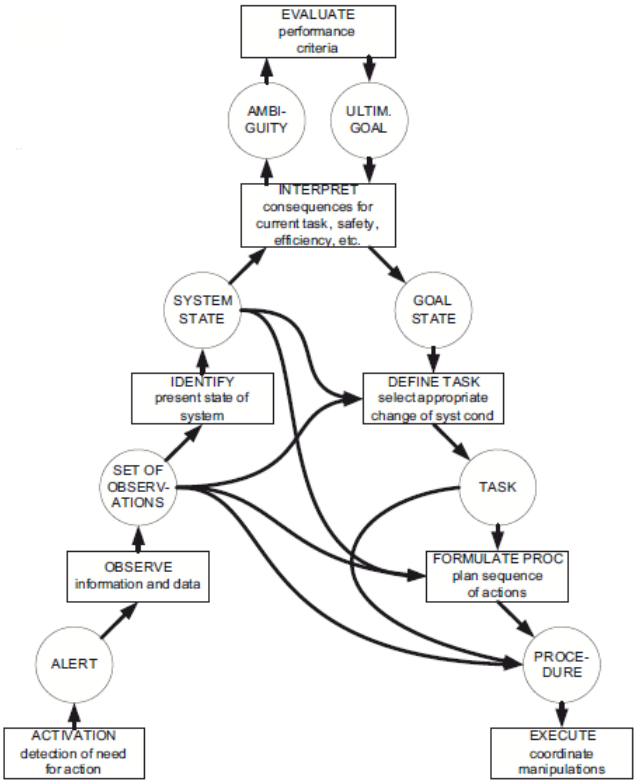


Figure 2.2: Decision Ladder Template (Rasmussen 1974)

2.3.3.2 Naturalistic decision making

Naturalistic decision making focusses on real-world settings as the research context in which decisions are made irrespective of information availability and emphasis is placed on understanding decision making in complex environments. While NDM usually takes place under bounded-rationalities, this does not imply that NDM is the opposite of rational decision making; the opposite is actually decision making in controlled environments (contrived knowledge elicitation) e.g., lab-based studies (Shadbolt and Smart 2015).

Findings from NDM research have indicated that decision-makers usually satisfice due to the limited information in dynamic and time-limited environments, and the findings have highlighted the role experience plays in analysing minimal alternatives to identify a course of action (Klein 2008, Orasanu and Connolly 1995, Azuma et al. 2006).

As Klein (2008) suggests, the aim of NDM research and its models is not to replace rational decision making models, but that it belongs on an opposite end where satisficing is required over optimising. The Recognition Primed Decision (RPD) model is explained next due to its prominence among the NDM models.

Recognition Primed Decision model

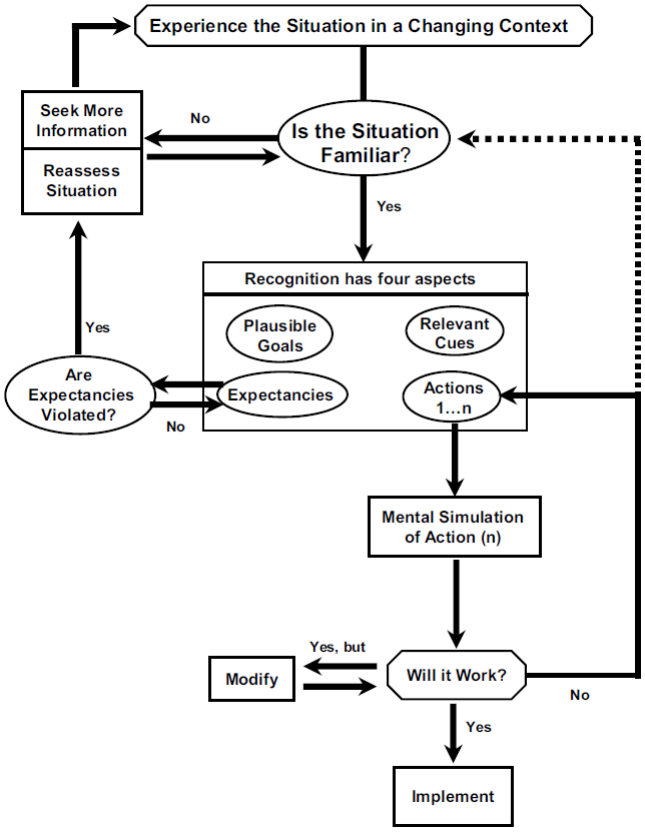


Figure 2.3: Recognition Primed Decision model (Klein 2008)

The Recognition Primed Decision model (Figure 2.3) follows the notion that ambiguity cannot be reduced by the passive collection of information and weighing of alternatives but through experience based pattern-matching leading to actions. The patterns highlight the most relevant cues, provide expectancies, identify plausible goals, and hint on suitable actions to a situation. Based on pattern-matching, rapid and good decision are possible (Klein 2008).

The model has three variants, each relating to a higher level of certainty. The first variant operates on the notion that when confronted with time pressure and uncertain conditions, decision-makers will fetch for similar experienced situations from memory to understand the present situation (pattern-matching). When a matching experience is identified, a course of action is taken in accordance with the pattern. In the event that a matching experience is not identified, the second variant kicks in, where additional information that may help pattern-matching is sought. In the final variant, mental simulation is used to identify possible flaws in the fetched patterns before action implementation. Alternative options are only considered after the unsuccessful execution of a match (Klein 1993).

2.3.4 Awareness models

It must be noted that this research distinguish decision making models (addressed in Section 2.3.3) to situation awareness models addressed below. Unlike reviews that place the two in one basket e.g., Grant and Kooter (2005), the researcher believe that decision making models aim at identifying techniques used for selecting suitable options to arrive at an informed decision. To achieve this, they deconstruct the decision making process into a series of steps representing strategies for identifying and weighing alternatives. On the other hand, awareness models aim at identifying techniques used to attain awareness; they do not deconstruct steps taken to decision making, but rather identify the steps taken for sense-making (Pirolli and Card 2005). Awareness models are reviewed in this section because they serve as a prerequisite to decision making.

Awareness is defined as the knowledge or perception of a situation. Situation awareness is, therefore, the knowledge or perception of a situation, essential for effective decision making. The term situation awareness is understood in two-fold. The first as a concept for understanding situations critical for decision making as defined above, the second as a theory for attaining awareness proposed by Endsley (1995). Two situation awareness models; Endsley's theory of situation awareness and the Observe Orient Decide Act (OODA) loop are detailed below.

2.3.4.1 Theory of Situation Awareness

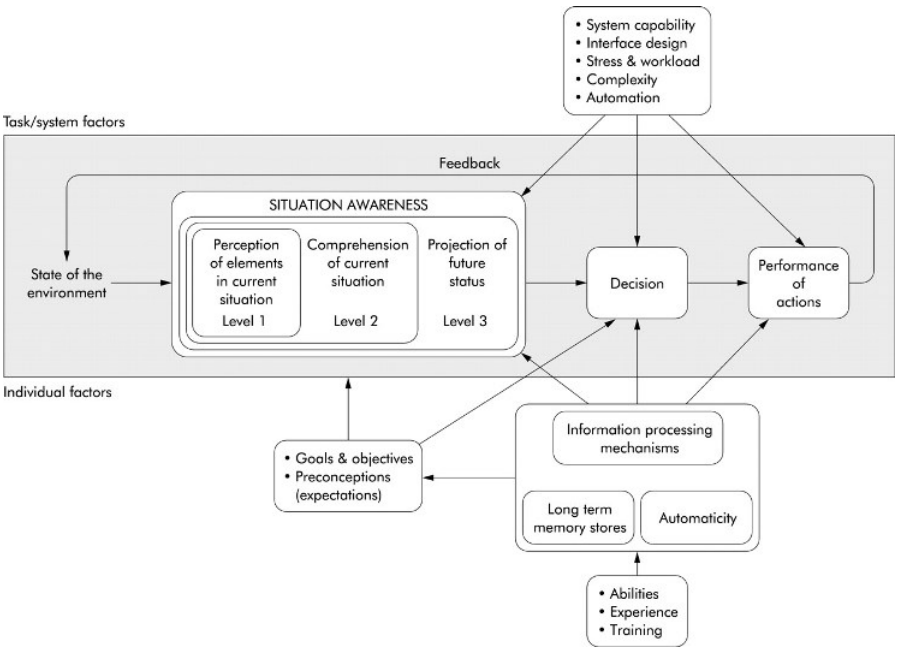


Figure 2.4: Situation Awareness model (Endsley 1995)

The theory of situation awareness (Figure 2.4) divides the process to gaining aware-

ness into three main steps, namely Perception of the environment, Comprehension of its meaning, and the Projection of future status. Based on the three Endsley defines situation awareness as *"the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."*

Originally modelled for awareness in aviation, its popularity has increased in HCI over the past thirty years and more recently in cyber security as a theme for analysing human performance in complex and dynamic environments (Jajodia et al. 2010, Hibshi et al. 2016). Situation awareness has been applied in the study of system design to identify factors such as attention and working memory shortfalls that limit user awareness and affect reaction to system and environmental changes (Salmon et al. 2006).

Unlike other awareness models that present their steps only as requirements towards awareness, situation awareness presents each progressive step as a level of partial awareness gradually increasing through the model (levels 1 to 3). Because of its origins in aviation, some of its theoretical elements have no translation in other disciplines. For example, the understanding of space (spatial context) is important in aviation but not applicable to security (Parush 2017).

2.3.4.2 Observe Orient Decide Act (OODA)

The OODA loop (Figure 2.5) is an awareness model developed to strategically observe and out-think opponents, comprising of the four main stages of Observe, Orient, Decide and Act (Boyd 1996, Osinga 2007). Unlike Endsley's situation awareness that has widely been adopted in HCI and cyber security, OODA has mostly been limited to military command and control. OODA does not consider awareness on an incremental basis but as a cumulative sum of the three stages and does not take the projection of a future state into account (Grant and Kooter 2005). OODA is, however, unique in highlighting the need for information outside the decision maker's immediate environment to improve perception.

As the examples have indicated, awareness models only dwell on understanding situations and not the strategies deployed in identifying or weighing possible alternatives. A comparison between awareness and decision making models is therefore incorrect and misleading as awareness is only a subset of decision making.

2.3.5 Context oriented approaches

Unlike the approaches discussed above, context oriented approaches propose that the decision making focus should not only be on the human but extended to artefacts sup-

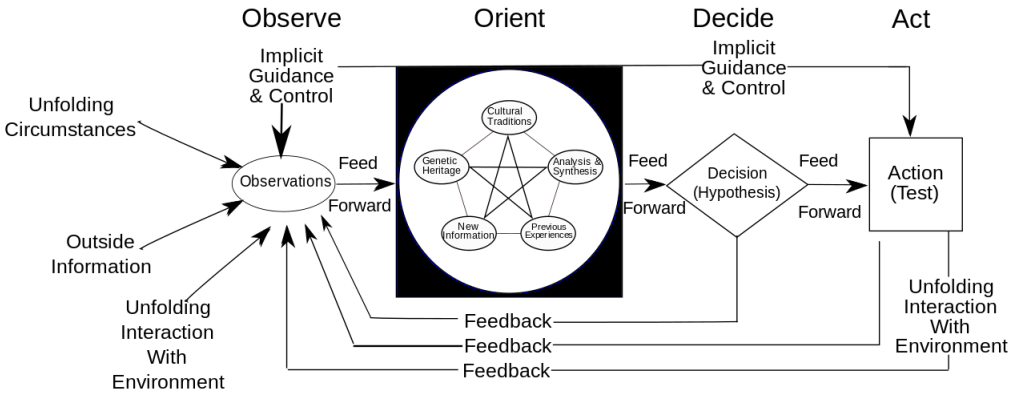


Figure 2.5: OODA loop (Boyd 1996)

porting awareness in the decision-makers environment and the situation within which they operate.

This view is motivated by the question; is situation awareness (concept) limited to the mind? Stanton et al. (2010) summarised the contextual views of situation awareness into the three groups of; in-the-world - *having real-time information of the world*, in-the-mind - *an individual's psychological phenomenon*, and in-interaction - *the human and technical agents and the way they interact*. The view facilitates the understanding of socio-technical systems of which decision-makers are a part. Detailed below are Distributed cognition and Situated action - two examples of context oriented approaches.

2.3.5.1 Distributed Cognition

Distributed Cognition is a theory based on the idea that cognition is distributed among individuals (social group), between people and external artefacts, and the relation between past and present events (Hollan et al. 2000, Hutchins 2000). A plane is an example of Distributed Cognition at work through its distribution and coordination of activities. People to artefact cognition may be seen in a pilot's communication with passengers and cabin crew through an intercom; the actual flying done from a central location (pilot's seat) is also mediated by technology with buttons to move flaps on the sides of the plane and levers to control landing wheel below. Person to person cognition is seen in the direct conversation between pilots and co-pilots, purposefully positioned in close proximity. The plane is a socio-technical system and cognition is distributed among its artefacts and individuals to achieve a common goal (Hutchins and Klausen 1996).

As part of their investigation on errors in the design of complex process plants, Busby (2001) identified that Distributed Cognition among individuals involves two phenomena: cues - signals or clues used to determine how and when to act, and norms - standards

or patterns regarded as typical. While the two are instrumental in supporting work in complex environments, there is the problem that their understanding is subjective and different from person to person, highlighting a need for formality in Distributed Cognition procedures.

As an approach for improving existing or proposed system designs, Distributed Cognition has been criticised for lacking a standard approach or reusable representative models. In an attempt to address this, Wright et al. (2000) proposed a resources model aimed at improving the Distributed Cognition to HCI link. The model presents six information structures that may be used to analyse interactions independent of technological implementation. These are:

- Plan - presentation of where one is in a task
- Goal - Indicators that steer one in the right direction
- Possibility - presentation of alternative options
- History - presentation of previous actions
- Action effect relations
- State - representation of present state

While useful, the proposals above only address what could be done when applying Distributed Cognition, but not how. Work by Blandford and Furniss (2005) and later adapted in Rajkomar and Blandford (2012) address the problem by proposing representational models for design using DiCoT (Distributed Cognition for Teamwork), a structured approach to analysing a system in terms of Distributed Cognition. The DiCoT models include:

- Information flows - analysing information flows among the actors of the system
- Physical layout - analysing how physical structures support communication among actors and facilitate access to artefacts
- Social structures - analysing social distribution of cognition within a system
- Artefacts - analysing the design and use of artefacts in cognitive work

To the best of the researcher's knowledge, DiCoT has only been applied in healthcare, however, as a theory, Distributed Cognition has been used in understanding security practices (Botta et al. 2011).

2.3.5.2 Situated Action

While Distributed Cognition's focus is on cognitive systems composed of humans and artefacts, Situated action focusses on the events between individuals and their environment (situation). Its approach is to investigate activities that prompt decision making in cognisance to the uniqueness of each situation. Introduced by Suchman (1987), it is argued that plans are not the result of actions abstracted from circumstances, rather it is the circumstances that influence plans leading to intelligent action. In other words, plans should be the product of problem situations.

In relation to systems design, Situated Action may be used to specify designs that are based on common user actions in particular situations. Application, however, seems limited to tangible actions e.g., printing.

2.3.6 Decision making summary

This section reviewed the literature on decision making with the aim of understanding how proposed theories, models and approaches may be used to facilitate design for RBDM. While most of the reviewed literature contributes to this research, particular focus is placed on Normative decision making from the decision theories, OODA from the awareness models, and Distributed cognition from the context-oriented approaches. The three are applied to the research from Section 4 onwards and are selected for their focus on investigating how decisions should be made (Normative decision making), how awareness for decision making is attained irrespective of expertise (OODA), and the role decision-makers environment plays in facilitating decision making (Distributed cognition).

2.4 Design

The review on design is divided into three sections, The first and second sections review design approaches related to cognitive user-centricity and traditional user-centricity respectively. The final section takes a jump forwards and investigates implications to decision making after design by focussing on the effects of automation to decision making.

In the previous section, techniques used for investigating user awareness and decision making in socio-technical systems were reviewed. In this section, approaches facilitating requirements elicitation and specification under the User-Centered/Human-Centered design philosophy are reviewed. User-centered design is defined as an approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability

knowledge and techniques (ISO 9241-210 2010). In addition to this, ISO 9241-210 elaborates that the meaning of usability is not confined to ease of product use, but among other things includes perception aspects of the system-user experience which is essential for decision making.

2.4.1 Cognitive user-centricity

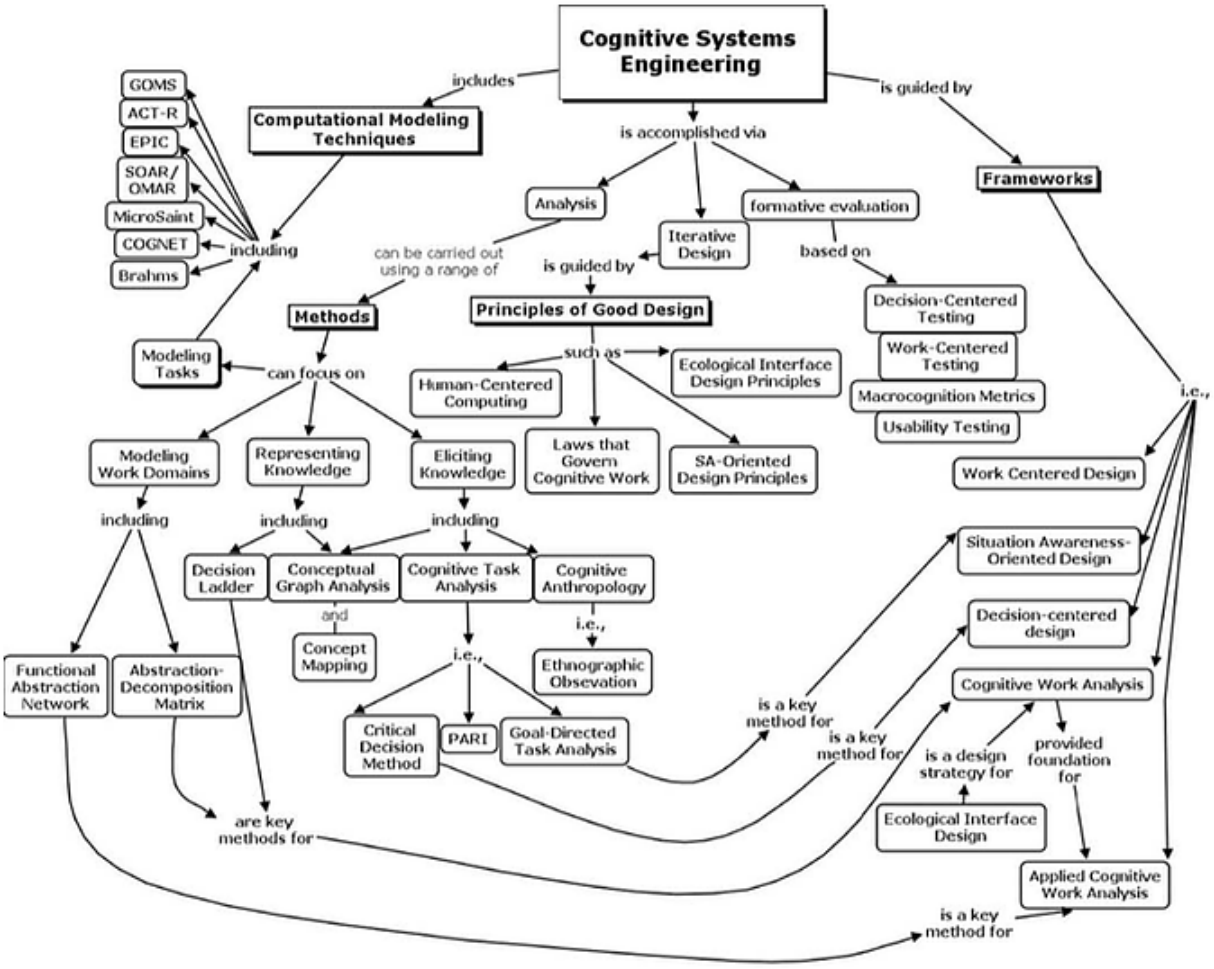


Figure 2.6: Cognitive Systems Engineering concepts (Militello et al. 2009)

User-centered design approaches that take cognitive requirements into account form what is known as Cognitive Systems Engineering (CSE). CSE is defined as *"an approach to the design of technology, training, and processes intended to manage cognitive complexity in socio-technical systems"* (Militello et al. 2009). CSE has been used to identify cognitive requirements and uncover cognitive complexities, model work patterns and constraints, model cognitive aspects of tasks, and propose system design principles (Varga et al. 2015, Bisantz et al. 2003, D'Amico et al. 2005). With an emphasis on understanding decision making tasks within actual settings, CSE aims at reducing complexities in

proposed or existing systems while maintaining optimal (not removing) human cognitive requirements (Gersh et al. 2005).

As the use of CSE is in many fold, so are concepts for its application. Militello et al. (2009) present a concept map (see Figure 2.6) illustrating the various frameworks, methods, models, and principles used. In spite of the advantages brought by a richly diverse research area, CSE has suffered from a proliferation of terms describing what are otherwise similar approaches within CSE, and the inconsistent use of terms with related research communities e.g., Systems Engineering (Hoffman et al. 2002).

Critical Decision Method (CDM) and Cognitive Work Analysis (CWA) are explained next. The two are examples of CSE selected for their focus on critical (risk related) and unanticipated (uncertainty related) events respectively.

2.4.1.1 Critical Decision Method

Cognitive task analysis is defined as the extension of traditional task analysis techniques to yield information about the knowledge, thought processes and goal structures that underlie observable task performance (Chipman et al. 2000). The three main aspects of cognitive task analysis are data knowledge elicitation, data analysis, and data representation. As illustrated in Figure 2.6, CDM is one of several knowledge elicitation approaches under cognitive task analysis.

As a knowledge elicitation approach, CDM (Klein et al. 1989) aims at identifying how experts make decisions during critical incidents. First, the expert is asked to select and narrate a critical incident (from experience), highlighting timeline and decisions made. After narration, the interviewer probes the expert on key points, identifies critical decisions and seeks their justifications with the aim of understanding the expert's goals, expectancies and cues used. Responses shed light on the expert's mental models, experience and training. As a final step, the interviewer probes for the expert's views if the situation or their knowledge and experience had been different. Outputs of the process are a critical incident and the cognition used to address it presented as narratives, flowcharts, task steps and other forms of knowledge representations.

Critical decision method is summarised by the following four steps:

1. Sweep 1 - Incident identification
2. Sweep 3 - Timeline verification
3. Sweep 3 - Deepening

4. Sweep 4 - “What if” queries

Due to its dependence on expert knowledge and incident recollection, CDM is difficult to apply in situations where expert availability is limited, in novel situations where expertise has not been gained or incident recollection is difficult, or due to the lack of critical incidents. Alternative approaches addressing different aspects of the issues have been proposed, such as the use of observation instead of incident recollection, or “the Knowledge Audit” approach which allows the collection of multiple incidents when one critical example is unavailable (Crandall et al. 2006, Gutzwiller et al. 2016).

2.4.1.2 Cognitive Work Analysis

Cognitive work analysis (Jenkins et al. 2017, Vicente 1999) developed by Rasmussen et al. (1994) is based on the understanding that cognitive task analysis approaches fail to design for unanticipated events. They argue that tasks are event dependent acts that workers do, while work domains are a collection of both event-driven and event-independent tasks (anticipated and unanticipated). By shifting the focus from the tasks to the work domain, one can visualise the bigger picture (Vicente 1995).

Unlike CDM that purely focusses on knowledge elicitation, CWA is a framework (see Figure 2.6) that guides designer through the stages of analysis, design, and evaluation by focusing on constraints to information seeking which expose unanticipated events. The framework is divided into five phases, each employing a variety of tools and techniques, and focussing on different constraints in the work domain. Listed below are the five phases based on Vicente’s (1999) update of the original.

1. Work Domain Analysis
   Addresses constraints imposed by the physical context in which the worker operates.

2. Control Task Analysis
   Addresses constraints imposed by task situations to uncover ’what’ should be done.

3. Strategies Analysis
   Addresses constraints imposed by task situations to uncover ’how’ they should be done.

4. Social Organisation and Cooperation Analysis
   Addresses constraints imposed by organisational structures or specific actor roles and definitions.

5. Worker Competencies Analysis
   Addresses constraints possibly dictating the worker's behaviour within the situations.

The variety of techniques used in the CWA phases for data acquisition and representation are illustrated in Figure 2.7.

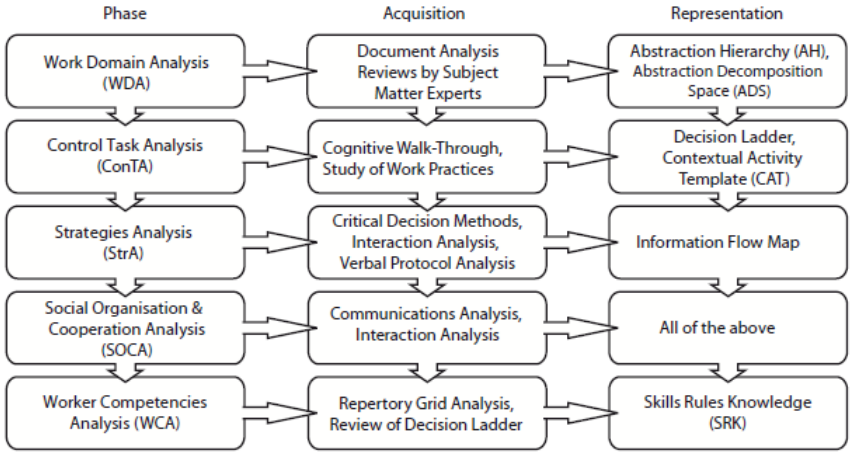


Figure 2.7: Cognitive Work Analysis phases (Jenkins et al. 2017)

Cognitive Work Analysis has been applied to a number of research projects. For example Roth et al. (2001) use it to specify levels of automation, human role, and display prototype of a ship's combat command center. Similarly, Varga et al. (2015) use it to analyse the constraints of distributed crewing in commercial flights.

While many lessons can be drawn from CWA, it falls short based on its Human-factors approach to cognition. In other words, it facilitates a fit between user and equipment e.g., interfaces, as seen in the two examples above. The approach is, therefore, a better fit for improving usability and not decision making. Cognitive Work Analysis has also been criticised as it promotes a focus on analysing the constraints in the environment, and avoiding the human on the basis that they may have flawed mental models - thus unreliable for requirements elicitation (Crandall et al. 2006, p. 250).

2.4.2 Traditional user-centricity

Unlike cognitive user-centric approaches that focus on eliciting and analysing knowledge and cognitive complexities, traditional user-centric approaches promote focussing on a *context of use*; which is defined as the characteristics of the users, tasks, and environment (ISO 9241-210 2010). For example, the context of use for incident detection activities differs from that of incident analysis activities as seen in Section 2.2.3.2. Though not

associated with cognitive elicitation and analysis, traditional approaches have proven effective in the analysis of users requirement to inform design. A few traditional user-centric examples from HCI and Requirements Engineering are detailed below.

2.4.2.1 Scenarios

Scenarios are stories describing people carrying out activities and their context. Scenario details vary based on the design requirements instantiating their deployment and they are used at various points in usability design. For example, problem scenarios may detail problem domains situated prior to technology introduction, while activity scenarios could be situated post-introduction; focussing on what users what to do, need to do, and events during interaction (Rosson and Carroll 2002).

Scenario use in security-related research has included overcoming issues of confidentiality and classified information and conveying the meaning of security properties in an accessible manner (D'Amico et al. 2005, Flechais et al. 2007).

Carroll (2000) presents five advantages of scenario-based design:

- Scenarios evoke refection in design
  Scenarios are intrinsically bound to context evoking the contextual reflection of design. This differs from design reviews or formative assessment that could be conducted devoid of context.

- Scenarios are at once concrete and flexible
  Design is a dynamic process that must focus on achieving the desired goal while being flexible to changes. Scenarios help manage this fluidity by being specific, while open for easy revision or elaboration.

- Any scenario has many possible views
  Design activity has the potential of producing multiple unwanted consequences. Scenarios afford multiple views of an interaction, diverse kinds and amounts of detailing helping manage the consequences of design ideas put forward.

- Scenarios can also be abstracted and categorised
  Scenarios help recognise, capture and reuse generalisations which address the challenge that technical knowledge often lags the needs of design.

- Scenarios promote work-orientation
  Scenarios are work-orientated design objects. They describe systems in terms of the work that users will try to do. A design process in which scenarios are em-

ployed as a central representation will inadvertently remain focused on the needs and concerns of users.

2.4.2.2 Personas

Introduced by Cooper (2004), personas are behavioural specifications of archetypical users aimed at preventing a generalised or biased views designers may have of users (elastic user). Personas are therefore nuanced representations of a target user type that should be addressed during design. As a representation of a target user group, their formulation is a result of thematic refinement of a user behaviour corpus grounded in empirical or hypothetical data (assumption persona) (Faily 2015, Pruitt and Adlin 2006).

Personas act as main characters in scenario-based approaches to design and are defined by their characteristics which typically include: activities, attitudes, aptitudes, motivations, and skills (Cooper et al. 2014). They provide feedback that enforces design coherence and serve as a communication tool that helps validate design rationale (Friess 2012).

Persona use in security design has included facilitating the elicitation and specification of requirements for secure and usable systems (Faily and Fléchais 2010a), promoting information security awareness (Ki-Aries and Faily 2017), and designing for security from an adversarial perspective (Steele and Jia 2008, Moeckel 2018).

The authenticity and use of personas have however been called to question, citing a lack of traceability between persona and source data (Chapman and Milham 2006). However, some of the arguments posed by the critics have no bearing. For example, the argument that two separate designers working on the same data should arrive at identical personas is an impossibility. The nature of qualitative research is not to produce exact replicable results, but provide consistency and integrity in the study design (Carcary 2009).

2.4.2.3 Goal-oriented approaches

According to Rolland et al. (1998), a goal is something a stakeholder hopes to achieve in the future. Goals are used in Goal-oriented requirements engineering (GORE) for eliciting, elaborating, structuring, specifying, analysing, negotiating, documenting, and modifying requirements (Lapouchnian 2005).

This approach to requirements engineering was motivated by inadequacies in traditional systems analysis approaches that focussed on data and process requirements for software systems overlooking the rationale/justification for the requirements. The understanding is that software systems are means of achieving user goals; the focus should

therefore not be confined to eliciting requirements for software systems, but the analysis and refinement of user goals that would suggest software systems requirements (functional and non-functional) (Lapouchnian 2005).

Though not a user-centered approach, GORE may be applied during activities preceding the specification of systems requirements (early requirements engineering); these include understanding the context, the stakeholders, their objectives and their relationships.

Several GORE approaches have been proposed, aimed at achieving different purposes. These include i* (Intension STrategic Actor Relations) that focusses on modelling and analysing stakeholder interests and how they might be addressed in various environments (University of Toronto 2011), and Knowledge Acquisition in autOmated Specification (KAOS) that focusses on analysing, specifying, and structuring goals and requirements using hierarchical analysis (Dardenne et al. 1993).

Below, some GORE concepts are highlighted, particularly focussing on those relevant to the dissertation's research theme. Detailed reviews on GORE concepts and approaches are presented by Lapouchnian (2005) and Horkoff and Yu (2011).

- Goal elicitation
  While goals drive user behaviour and represent their requirements, users, generally have difficulty articulating them. This is mostly because goals are implicit and not obvious; their elicitation is, therefore, better through the investigation of user operations and actions where intentional keywords hinting at goals may be identified (van Lamsweerde 2000).

- Goal refinement and analysis
  As expressions of intent, some goals are strategic, high-level and unattainable as requirements. Goal refinement aims at providing traceability links from these high-level goals to low-level requirements. This is done using the AND/OR goal decomposition where attainable sub-goals are identified (Dardenne et al. 1993).

- Obstacle analysis
  Goals are an ideal world view, however, the reality is goals may be unachievable due to anticipated (risk) or unanticipated (uncertainty) conditions. Originally proposed by Potts (1995) and refined by van Lamsweerde and Letier (2000), obstacle analysis aims at taking this into account through the identification and refinement of exceptional conditions in goal modelling.

- Contextual modelling

> Contextual goal modelling promotes the understanding that goals are not aspirations occurring in the absence of a context. As context influences goals, equally are its impact of requirements. This being the case, contextual differences must be taken into account during goal analysis for systems operating in dynamic conditions (Ali et al. 2010).

2.4.3 The automation conundrum

Unlike the previous sections that reviewed design approaches and implications to decision making before design, this section reviews the implications post-design. This is an area that was most likely not going to be covered as the research focusses on the early stages of design, however, automaton presents a special case as it both elevates and hinders decision making (Endsley 2017).

The International Society of Automation defines automation as the creation and application of technology to monitor and control the production and delivery of products and services. For security analysts, it would be fair to say that automation is the application of technology to monitor and control the delivery of cyber security services (see Section 2.2.3.2 for analyst activities). The need to automate cyber security activities and services prompts a few questions. Which areas of security decision making should be automated, to what extent, and what could the implications be?

According to Ritter et al. (2014), common techniques for allocating automation between users and technology are based on Fitts' allocation of functions known as MABA-MABA (Men Are Better At - Machines Are Better At). The problem with this approach is that attempts are made to automate almost everything that can be automated with little consideration on how contextually ideal this might be. For example, Gutzwiller et al. (2015) identifies that many existing cyber-defence tools fail to link information they provide to the goals of the users, making them unlikely to enhance decision making and performance.

The irony of automation is that although it alleviates the complex decisions users make through abstraction and simplifications, it may also result in over-reliance on automation that leads to automation induced uncertainty or out-of-the-loop unfamiliarity. Users become complacent, lose situational awareness, and their skills gradually degrade (Parasuraman and Manzey 2010). To put the problem into perspective - how may it be ensured that users are capable of understanding events and making correct decisions when manual system takeover is required during automated systems failure (Endsley 2017)?

The ironies of automation originally presented by Bainbridge (1983) are still prevalent in

current systems in spite of increased research and solutions thereof (Baxter et al. 2012). A commonly referenced solution is Parasuraman and colleagues' (2000) model on levels of automation and types of human interaction with automation. The model defines four system functions, namely *Information acquisition, Information analysis, Decision and action selection, and Action implementation*, where automation can be applied in accordance with a ten-level automation scale (Table 2.2).

A point of note on the implications of automation to decision making is the need to automate in accordance to user capabilities; thus keeping users in the loop and maintaining their awareness - which in turn improves their potential for informed decision making.

Automation level	Automation description
1	The computer offers no assistance: human must take all decision and actions
2	The computer offers a complete set of decision/action alternatives, or
3	Narrows the selection down to a few, or
4	Suggests one alternative, and
5	Executes that suggestion if the human approves, or
6	Allows the human a restricted time to veto before automatic execution, or
7	Executes automatically, then necessarily informs humans, and
8	Informs the human only if asked, or
9	Informs the human only if it, the computer, decides to
10	The computer decides everything and acts autonomously, ignoring the human

Table 2.2: Automation scale

2.4.4 Design summary

This section reviewed the literature on design with the aim of identifying suitable approaches for eliciting and specifying requirements for RBDM. The review suggests gaps in the current practice between the the cognitive user-centric approaches used for eliciting decision making requirements and the traditional user-centric approaches used for specifying requirements. This implies investigating how cognitive element may be considered during requirements specification.

2.5 Chapter summary

This chapter reviewed the state-of-the-art from three areas (risk, decision making, and design) contributing to design for cyber security RBDM as summarised below.

- From the literature on risk and security, it was identified that the distinction between risk and uncertainty has not been made explicitly clear - analysts' activities tend

to address risk with uncertainty implied. Consequentially, the literature presents a limited scope to analysts' decision making, often dwelling on threats associated with risk, while overlooking the effects of uncertainty. The findings suggest further investigations to identify the implications of risk and uncertainty to security analysts' practices and decision making. In addition to this, considerations must be made on how to effectively elicit security knowledge and overcome the analysts' unavailability problem due to sensitivity in the security domain.

- The literature on decision making presented a diverse range of theories and techniques that may be considered for facilitating design. Candidate techniques that are applied in this dissertation were identified and highlighted in Section 2.3.6. A lack of differentiation between decision making and awareness theories and approaches was also identified in the literature. A clear distinction is essential as awareness is a precursor to decision making that dwells on the strategies for situational understanding. Decision making on the other hand, dwells on the strategies deployed in identifying or weighing possible decision alternatives.

- The design literature reviewed dwelt on approaches for eliciting and specifying requirements with a focus on cognitive and traditional approaches to user-centricity. The review did not find evidence that the traditional approaches have the potential to support the elicitation of cognitive requirements for design. While the cognitive approaches reviewed are suitable for cognitive elicitation, they fall short in translating the findings into design specifications. The findings suggest conducting further investigations for adapting or adopting existing approaches.

As is evident above, each research areas presents unique problems that require further investigations or knowledge that should be built upon. In addition, there is a gap on how findings from the three areas may be integrated to facilitate the specification of requirements for systems deployed in cyber security RBDM.

Chapter 3

Research Approach

3.1 Introduction

This chapter discusses the research approach supporting the thesis from a philosophical and methodological perspective, it presents the rationale behind the adoption of the approaches and the related strategy adopted for this dissertation by considering the gaps between research on decision making and research on design.

Based on the research questions, designing for RBDM will involve synthesising knowledge from research approaches for eliciting and understanding decision making in cyber security (the problem domain), with research approaches for specifying design requirements for decision making in cyber security (the solution domain).

Review of the literature indicates that various cognitive approaches; awareness and decision making (see Section 2.3) are ideal in facilitating the elicitation of requirements for decision making in cyber security e.g., the theory of Situation Awareness, the Decision Ladder Template, and Distributed Cognition (Hibshi et al. 2016, Gerber et al. 2016, Botta et al. 2011, Gutzwiller et al. 2015). Cognitive approaches are, however, not ideal for specifying design requirements. This may be attributed to methodological gaps between techniques used to understand decision making and techniques used to specify design.

Decision making research follows a descriptive to prescriptive approach, this is the understanding of how decisions are made to then design approaches (models/techniques) that facilitate informed choice. Artefacts resulting from decision making research typically dwell on improving awareness and decision strategy, however, they are rarely presented in forms familiar to designers and do not properly translate to models capable of informing design (Blandford and Furniss 2005, Parush 2017).

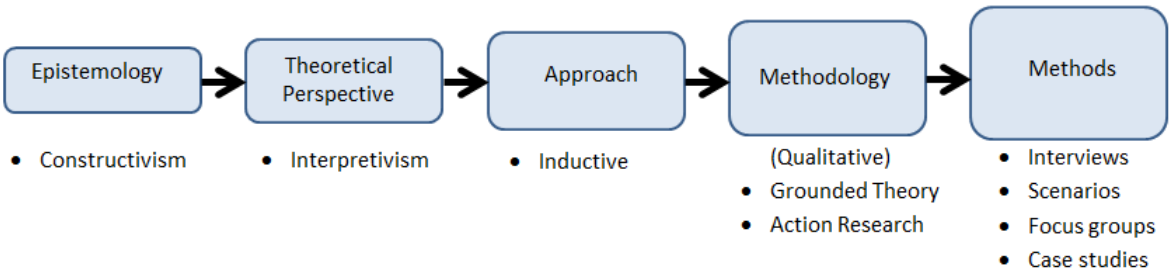


Figure 3.1: Research approach

In contrast, the literature indicates that traditional (non-cognitive) User-centered design approaches from HCI and Requirements Engineering (see 2.4.2) are ideal for the solution domain as they have been demonstrated to be suitable for informing design (Faily and Fléchais 2011, Flechais et al. 2007). Traditional approaches are, however, not developed for eliciting cognitive requirements, therefore, only provide sparse or invalid cognitive understanding (Gutzwiller et al. 2015).

Cheng and Atlee (2007) point out that successful design involves the adequate understanding and representation of user requirements. This implies that successful design for RBDM would require input from both the cognitive and traditional approaches. Decision making models are primarily aimed at understanding the problem domain, while design models aim at informing the solution domain. In a perfect world, this would mean that requirements identified in the former, serve as input to the latter. However, methodological differences present incompatibilities (Fischer 1991).

Based on this understanding, the research approach has to take the following into considerations:

1. Elicit RBDM requirements as dictated by the problem domain.
2. Construct output linking the cognitive and traditional approaches.

3.2 Philosophical perspective

Having identified the considerations for the research approach in Section 3.1 above, the selected research approach is outlined in Figure 3.1, highlighting the relationship between the research's philosophical perspective and methodological approach.

From a philosophical perspective, the research is grounded in the Constructivism epistemology; this is to say that RBDM will be investigated empirically, based on security analysts' views and understanding of risk. Constructivism posits that knowledge or meaning

is based on one's view, or dependent upon a social consensus. Knowledge is constructed and not discovered, hence contradicting but equally valid views of reality (knowledge) can exist (Guba and Lincoln 1994). According to Elkind (2005), Constructivism is *" the recognition that reality is a product of human intelligence interacting with experience in the real world. As soon as you include human mental activity in the process of knowing reality, you have accepted constructivism."* An alternative approach to Constructivism is Positivism which argues that knowledge is generated by scientific methods (not scientists' understanding) and there is a single correct method for generating knowledge; generally, through quantifiable interpretation. This philosophical stand does not align with this research as understanding and designing for decision-makers can be approached in multiple ways and there is no quantifiable truth.

The theoretical perspective adopted for this dissertation is Interpretivism which is closely aligned to Constructivism. Interpretivism aims at interpreting elements of a study in cognisance of the differences between people. The focus of interest lies in identifying what is specific, unique, and deviant as opposed to identifying averages and representative samples. Both Constructivism and Interpretivism emphasizes qualitative over quantitative analysis (Saunders et al. 2009).

The research aimed to develop meaning based on understanding and interpreting findings from the problem domain as opposed to testing the validity of a preconceived hypothesis. This suggests that the research follow an inductive approach rather than a deductive approach that begins with a hypothesis. The inductive approach does not aim to corroborate or falsify theory. Rather, through a process of gathering data, it attempts to establish patterns, consistencies and meanings (Gray 2016). Typically induction occurs during data elicitation and analysis where relationships in data are identified, findings are generalised, or theory generated. As a multistage research endeavour, the approach to this research is to apply induction as an ongoing process where each subsequent output is informed by the preceding output (see Figure 3.2). The approach is necessitated by the interdisciplinary nature of the research, where initial finding from the problem domain shall require additional interpretation and analysis to inform design.

Selecting an approach for research is unfortunately not a straightforward process due to the un-unified view of epistemological positions and related research strategies (Yeganeh and Su 2004, Lehaney and Vinten 1994, Knox 2004). In light of this, and to maintain consistency, the research takes the approach presented in Figure 3.1, which is adopted from Gray (2016).

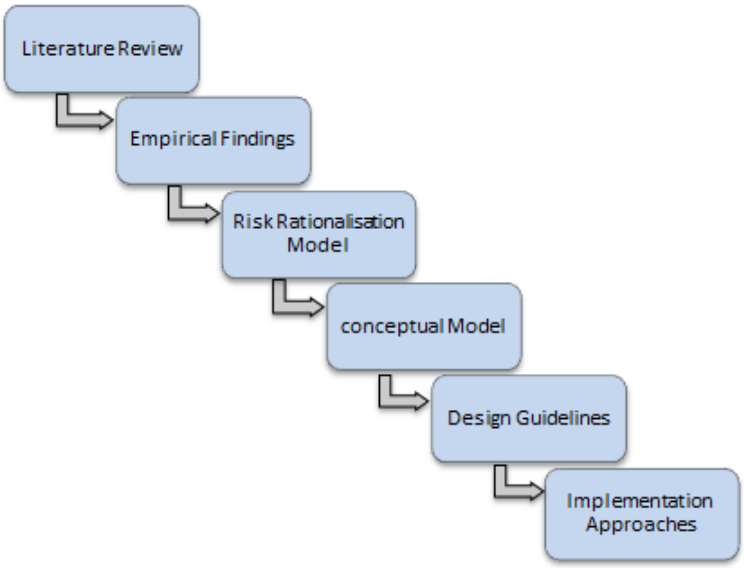


Figure 3.2: Application of Inductive Constructivism

3.3 Methodological approach

The theoretical perspective chosen for research influences the methodology which in turn influence the data collection and analysis approach (methods). This is however not to say that research methodologies should be categorised against specific philosophical perspectives as concrete relationships, what is important is the justification of a realistic methodological selection in relation to the philosophical perspective and research questions (Gray 2016, Knox 2004).

Two methodologies were adopted for this dissertation, these being, Grounded Theory and Action Research.

Grounded Theory was applied in Chapter 4 as part of early-stage empirical analysis aimed at identifying factors contributing to analysts' perception of risk. Data collected from interviews with the analysts was thematically analysed using Grounded theory, where findings emerged after three rounds of coding. Grounded Theory is qualitative and inductive, therefore, falls in line with the philosophical perspective adopted for the research. Further details on the methodology are provided in Section 3.3.1 below.

Action Research was applied in Chapter 8 as part of later-stage research, that was used as a vehicle for facilitating the validation of design guidelines proposed in the dissertation. As cumulative products of the overall research, the design guidelines were applied to a real-world organisation where a secure data handling policy was inductively designed following the stages of Action Research detailed in Section 3.3.2 below.

A variety of data collection and analysis methods were used at different parts of the research, all in line with the chosen philosophical perspective and qualitative nature of the research. Among the methods used are interviews, scenarios, focus groups, and case studies, selected based on suitability for the problem being addressed. Where necessary, the methods are described in greater detail in the applicable chapters.

3.3.1 Grounded Theory

Grounded Theory is a qualitative data analysis technique that aims to formulate, test and reformulate prepositions until a theory is developed. The approach refers to theory that is grounded in, or developed inductively from a set of data (Saunders et al. 2009). Originally limited to the inspection and analysis of qualitative data (Glaser and Strauss 1967), Corbin and Strauss (2008) among other things revised it to include both qualitative and quantitative data. See Heath and Cowley (2004) for a detailed comparison between the Glazer and Strauss approaches to Grounded Theory.

In Grounded Theory, collected data in various forms is broken into codes which serve as identifiers of key points. Concepts which are codes of similar content are then reassembled in new ways to derive new meaning. The Corbin and Strauss (2008) approach to Grounded Theory achieves this by subjecting elicited data to the steps of *Open*, *Axial*, and *Selective* coding. In the Open coding, codes are assigned to units of similar data that capture the intent behind the observations. During Axial coding, codes are grouped into categories and sub-categories, this aims to identify the relationship between the categories. Selective coding entails defining the Core Category (central phenomenon). The Core Category represents the main theme with the greatest explanatory relevance and highest potential for connecting the emergent categories. In addition to the three coding steps, Grounded Theory utilises the constant comparative method which refers to the simultaneous collection, coding and memoing of data, and the constant testing of emerging themes as codes are generated.

Grounded Theory is, therefore, an iterative data elicitation and analysis methodology. This quality influenced its selection over Thematic Analysis (Braun and Clarke 2006), where the steps for collecting and analysing data are linear; thus analysis can only begin after all data has been collected.

3.3.2 Action Research

Action research is a research strategy originally introduced in social science (Lewin 1946) that involves learning by doing, where identified problems are resolved through active intervention by the researchers and practitioners. Baskerville (1999) sparked its popularity in information systems research and it has more recently been used successfully in information security research (Flechais 2005, Faily 2011). Action Research is described as a collection of research approaches rather than a single methodology, characterised by four common points. These are an action and change orientation, problem-centricity, involvement of systematic and sometimes iterative stages, and collaboration among participants. The Baskerville (1999) version of Action Research used in this research consists of the following phases:

1. Diagnosing
   Identification of the primary problems motivating the organisation's desire for change.

2. Action planning
   Collaboration between researchers and practitioners to establish an action for relieving or improving the problem. Action plans clearly stipulate the target and approach for change.

3. Action taking:
   Implementation of the planned action which is the introduction of an active change causing intervention.

4. Evaluating
   Evaluation of outcome to determine whether the effects of the action were realised and relieved the problem.

5. Specifying learning
   An on-going phase considered throughout the project to reflect the knowledge gained, provide diagnosis where the change is unsuccessful, and the provision of insight for the scientific community.

3.4 Chapter Summary

In this chapter, findings from the literature review were summarised in line with the research questions to motivate the requirements for a suitable research approach. Based on this, the philosophical perspective and methodological approaches adopted for the thesis were presented; detailing Grounded Theory and Action Research as the primary data analysis and research validation approaches for the dissertation respectively.

Chapter 4

Risk Analysis Practices by Security Analysts

4.1 Introduction

This chapter presents factors influencing risk analysis practices deployed by cyber security risk-based decision makers. As part of the literature analysis on risk (Section 2.2), a need to further investigate the relationship between decision making and risk analysis practices deployed by security analysts was identified. The investigating addressed research aim 1: Identify factors influencing risk analysis practices deployed by cyber security risk-based decision-makers.

The chapter presents two studies on analysts' risk analysis practices. First a proactive risk analysis study investigating factors promoting risk understanding, then a reactive risk analysis study investigating decision making under constrained conditions that was motivated by the first study. Conducting investigations from both a proactive and reactive perspective assured a comprehensive coverage of risk analysis practices by analysts.

4.2 Proactive risk study

4.2.1 Approach

Proactive risk analysis (Li et al. 2010) focusses on activities that occur before an incident and dwell on identifying the likelihood of exploitation based on inherent system weaknesses. This study focussed on understanding analysts' approach to risk and uncertainty during vulnerability analysis - exemplifying proactive risk analysis.

A total of ten interviews were carried out with analysts at three UK based organisations. Interviews were semi-structured and held at the participant's place of work. Each in-

terview lasted for approximately an hour and was recorded and later transcribed. The transcripts were coded and analysed using NVivo 11 (Hutchison et al. 2010). Ethical considerations were made following Bournemouth University's research ethics guidelines. Using a participant information sheet, each participant was made aware of the purpose of the study and the ethical procedures to be followed beforehand. Written consent was also sought from the participants before interviews began using an agreement form. See Appendix .1.2 and .1.3 for the participant information sheet and participant agreement form respectively.

Questions directing the interviews were modelled based on possible situations of uncertainty during vulnerability analysis that would result in risk if suboptimal decisions were made. For example, the question "*what guidelines do you follow to help you manage risk?*" was asked during the early stages of the interview to give the researcher an understanding of the risk analysis practice. Questions following from this aimed at identifying what happens when the guidelines do not work or when novel situations were encountered. E.g. *"how do you identify false positives?* and *"what were the occasions when you had to accepted risk?"*. See Appendix .1.1 for a list of questions that directed the interviews.

Based on the decisions, procedures, and workflows described by the analysts during the interviews, risk understanding flows were modelled using DiCoT adaptations, depicting the distributed nature of risk information (Hollan et al. 2000, Rajkomar and Blandford 2012). The models were subsequently presented to the analysts for validation. In parallel, the data collected from the interviews was coded and qualitatively analysed using Grounded Theory (Corbin and Strauss 2008). While Distributed Cognition elucidated the distributed nature of risk information, Grounded Theory complemented the process by interrogating interview data to identify thematic patterns characterising the analysts' understanding of risk. Participants' quotes supporting the findings are presented throughout the chapter.

4.2.2 Participants

The three interviewed organisations, hereon organisation A, B, and C, were recommended through contacts and selected based on the requirements that they had security teams that carried out vulnerability analysis. Participants in the teams were drawn based on availability for interview.

Organisation A was a higher education institution with three permanent information security analysts supported by team members from other Information Technology (IT) service

departments, e.g., the Linux, Windows, and Oracle server teams. P1 and P2 (Participant) were a security analyst and security manager in the permanent security team, while P3 to P5 were analysts from the support teams. The professional experience of participants within Organisation A ranged from two to over seven years, and they were responsible for over 1000 servers.

Organisation B was an information security practice with a core team of information security analysts. P6 was the organisation technical director and P7 the head of group IT. P6 and P7 had eleven and two years of professional experience in the organisation respectively and were responsible for approximately 150 servers.

Organisation C was a public sector organisation; the three security analysts (P8 - P10) interviewed were primarily focused on external engagements. Their work entailed vulnerability analysis, information assurance, and penetration testing. Their professional experience at the organisation ranged from eighteen months to five years.

4.2.3 Findings

4.2.3.1 Distribution of risk information

Distributed between teams

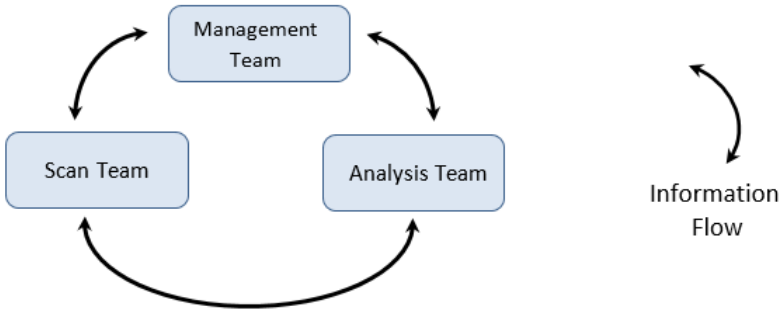


Figure 4.1: Distribution between teams

Interviews indicated that one form of gaining risk understanding was through the distribution of information for decision making between teams (Figure 4.1). It was identified that in most cases, analysts belonged to one of three teams (scan, analysis and management). The scan team was responsible for configuring the scan parameters and scanning the network infrastructure, it monitored false positives and passed all scan results to the analysis team. The analysis team was responsible for verifying the findings, and identifying and applying remediation. Feedback was given to the scan team on false positives, false negatives, and updates on vulnerability remediation. In situations of doubt, the anal-

ysis team sought advice and approval from the management team before taking action. The management team provided guidance to the other two teams, approved actions, sought justifications for decisions, and monitored activities. Members of this team had significant experience in one or both the other teams.

A common trend in the organisations was the use of collaboration and workflow management tools like the ServiceNow product suite (ServiceNow 2019) to support communication, job posting, and job status tracking.

"They notify me from the system, and when the change is happening, I get notified as well. It's when they log it, so the system itself notifies me when a change is going to happen" [P2].

Distributed through intelligence sources

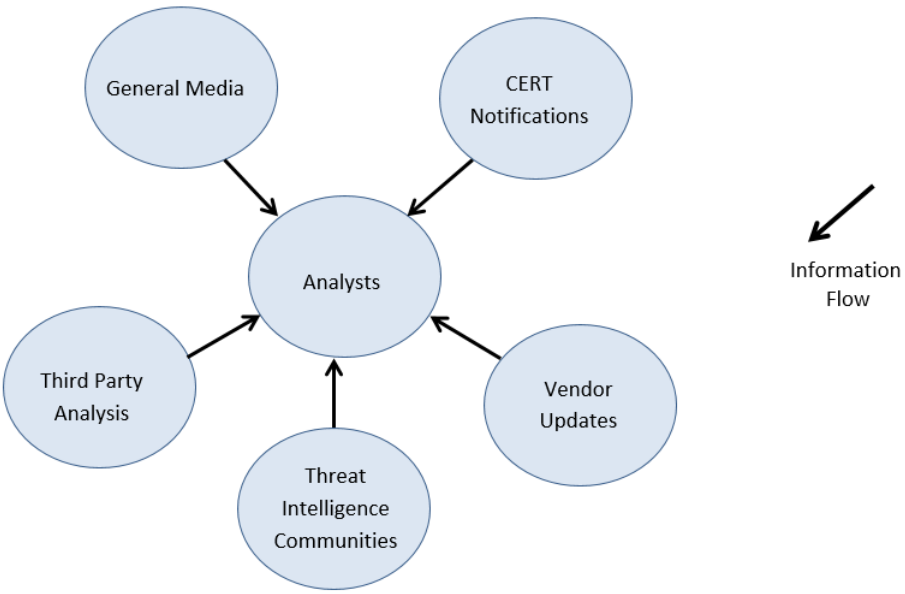


Figure 4.2: Distribution of intelligence

Risk understanding was also gained by the distribution of information through intelligence sources (Figure 4.2). Other than the analysis reports produced by vulnerability scanners, analysts highly depended on information produced by sources external to the organisations for awareness and decision making.

"There are CERTs that will send us notifications on malicious activity on the network if we sign up to them..." [P1].

While this is not an exhaustive list, the sources of intelligence included penetration test and vulnerability analysis findings from third parties, Computer Emergency Response Team (CERT) notifications, information from the general media, and updates from vendors and threat intelligence communities. False negatives resulting from network scans were usually discovered using external sources. The sources of intelligence findings closely relate to those reported by ENISA (2017) on the nature of threat intelligence platforms.

"...we identified new vulnerabilities so they were, therefore, no tests for them in Nessus...Pen testing teams have identified some of these by trying our system" [P7].

Distributed through tools and artefacts

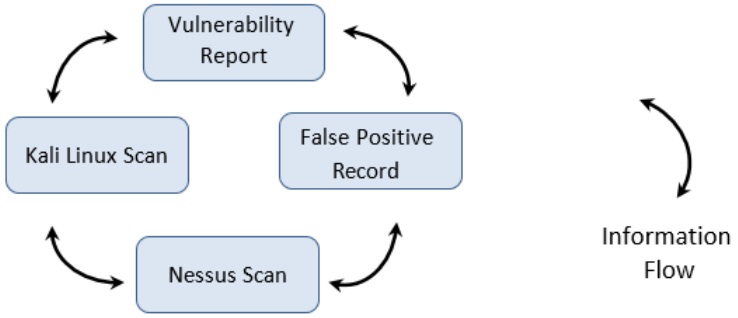


Figure 4.3: Distribution between tools and artefacts

Lastly, risk understanding was gained through the distribution of information between tools and artefacts which analysts used to identify and validate vulnerabilities on network resources (Figure 4.3). The analysts detailed using multiple tools for verifying identified vulnerabilities and possible false positives, suggesting limited confidence in tools. Artefacts used included manually maintained records; such as Excel files used to list known false positives.

"We manually scan for vulnerabilities using Kali Linux, and then we verify the findings using Nessus as a backup" [P8].

"Over time we have identified certain vulnerabilities where we do not agree with the rating in Nessus. We will then write exceptions in our system to change them. So when the XML report is presented to our system, it knows that rating is wrong" [P7].

"As Nessus doesn't link scans, I keep a record of the false positives in my Excel spreadsheet so if I see the vulnerability occur again, I know to ignore it" [P2].

Open Coding	Axial Coding	Selective Coding
Internal Awareness	Awareness	Remediation
External Awareness		
Standards and Guidelines		
Proactive Remediation	Remediation	
Reactive Remediation		
Feedback	Communication	
Information Sharing		
Third Party Dependency	Constraints	
Business Process Requirements		
Insufficient Privileges		
Project Management		
Obligations		
Assistive Tools	Tool Capabilities	
Vulnerability Analysis		
Vulnerability Scans		
Aptitude	Individual Capabilities	
Roles and Responsibilities		
Experience and Training		

Table 4.1: Grounded Theory analysis - Factors promoting risk understanding

Once false positive filtering was completed by analysts, a vulnerability report was produced for remedial action. The trend was to address the vulnerabilities marked as critical as early as possible, leaving the rest for later.

"If we got high or critical vulnerability that is found we immediately raise a ticket into our support desk and we will prioritise that to be fixed within 48 hours if possible...The rest of them we lump into one ticket which we work on over the rest of the month" [P7].

4.2.3.2 Factors influencing risk understanding

As a result of Grounded Theory analysis, four factors emerged that promoted risk understanding and five conditions that constrained risk decision making. Table 4.1 illustrates the results from the Grounded Theory analysis with the main findings grouped under Axial[1] coding. The core category that emerged from the analysis was *Remediation* as it had the greatest explanatory relevance and highest potential for connecting other categories. The relationship between interviews and themes identified is presented in Appendix .1.4.

Factors promoting risk understanding

Factors promoting risk understanding fostered a sense of rationality in the face of uncertainty. Just as their presence promoted understanding, their absence limited it. The factors identified were *Awareness*; promoted by the use of standards and guidelines and gleaned from sources internal or external to the organisations. *Communication*; the ex-

[1]See Section 3.3.1 for an explanation of the Grounded Theory steps.

change of information by the analysts for informed decision making. *Tool capabilities*; the effectiveness of tools used. And *Individual capabilities*; a combination of training, experience, and one's aptitude for inquiry and analysis. The following quotes illustrate conditions where limited individual capabilities were expressed.

"A lot of the decisions are based on the experience of people in that group and their knowledge of risk and the business... we are relying on expertise and awareness of those people" [P6].

"As far as I am concerned, we have to take the scan results as almost gospel... I do not have the awareness of all the systems, maybe if I had been here an awful lot longer...if I had the experience and the knowledge of the systems that were in place, I would say I know how that works and I know how that fits into the environment" [P2].

Conditions constraining risk decision making

Constrained conditions were results of contextual mismatches between business and security goals that were not carefully considered at the onset. The conflicts between the goals impeded the implementation of security objectives, thus promoting uncertainty. The constrained conditions were grouped based on similarities in goal conflicts as follows.

- Project Management
  Time, cost and human resource are vital components of successful projects (Schwalbe 2014). The project management goal conflict arose when resource allocations were not in line with the maintenance of security goals. Systems typically have an end of life where replacements are required due to advances in technology and improvements in security. When this point is reached, time and resources are required to upgrade systems and maintain security goals. Analysts expressed the constraints faced due to a lack of time and resources to undertake the actions.

  "We know we have a number of 2003 servers that need to migrate to the latest version of Windows server and the reason that does not happen overnight is because of a conflict of interest in terms of products, but also because of the services that sit on these" [P1].

- Third Party Dependency
  This conflict arose as a result of a third party's inability to provide adequate support for their products and services. Well established product and services suppliers such as Microsoft and Oracle usually support their services by making updates available routinely or on demand. Less established suppliers and open source projects prefer a collaborative approach to maintaining different parts of products and services. Analysts expressed that although the use of such collaborative prod-

ucts was essential, problems ensued when some collaborators stopped supporting the products.

"We have a product that uses Apache and there is a vulnerability that needs to be patched in Apache. Unfortunately, it is vendor supported, and the vendor does not support that version of Apache, so we have got to accept it, to be in line with the vendor application" [P4].

- Business Process Requirements
  A business process is defined as an activity or set of activities that accomplish specific organisational goals. This conflict was identified when analysts' risk decision making was constrained due to the requirements of essential business processes. For example, an analyst reported that System developers requested new tools that seemed secure at first instance; however, the overall security implications when considered contextually were unclear.

  "The developer team are using software which they use for their internal collaboration and they want to use video, but we are unsure how they are going to use the video...we are going to review it in six months and if we find that they are using it in a way that is a risk to the business...we would shut it down despite the fact that it is a good tool to them" [P7].

- Insufficient Privileges
  Risk analysis and remediation requires privileged access to devices and services, the lack of these privileges resulted in the insufficient privileges goal conflict. For example, an analyst expressed concerns about the limited knowledge and access they had on the internal working of a proprietary security tools they used.

  "We use Qualys for our external servers and website, but Qualys tend to talk back to its cloud service (vendor run)...If you have a Qualys system on your network, it belongs to them so you cannot change the system configuration" [P7].

- Obligations
  The Obligation goal conflict was identified when there were legal, standard or contractual obligation for data protection, versus the business objective to share data. For instance, an organisation may implement the security goal to encrypt all transmissions of personally identifiable data as one way of conforming with the data protection act (Great Britain 1998). However, conflicts arose when the data had to be shared with entities lacking encryption capabilities.

  "We do have challenges around client capabilities. So if we want to send an encrypted message and they do not have PGP or an encrypted Dropbox, then we have to come to an agreement on how to share that information" [P6].

4.2.3.3 Consolidated findings

To conclude, the analysts' decision making during vulnerability analysis was consolidated (Illustrated in Figure 4.4). Decision making began by identifying whether or not there was a likelihood of risk. In the event that the likelihood had been identified (e.g., outdated software), the risk source was verified by checking for vulnerabilities and the need for response validated (e.g., identification of critical vulnerability). Where response was warranted, probable conflicts were resolved and mitigation strategies identified, tested and applied where successful. If tests were unsuccessful, or where suitable mitigation strategies could not be identified, or conflicts resolved, the risk was tolerated and monitored. In the alternative event that risk likelihood was not apparent, the possibility of risk introduction was considered. For example, the *Insufficient Privileges* constraint referred to the Qualys system as a seemingly unlikely risk source, though risk introduction was possible based on its proprietary nature and unknown internal workings.

4.2.4 Study implications

The findings indicate that risk understanding is a matter of consolidated effort between analysts and artefacts, facilitated by the communication of information to improve awareness. For analysts, experience and training were essential, however, one's eagerness for improved awareness and aptitude for inquiry and analyses were most important. This was evident in the analysts' determination to question findings on vulnerability, use second sets of tools for analysis, and the identification of alternative intelligence sources to understand situations. The goal conflict situations highlight the importance of considering context when defining business and security goals to avoid later stage constraints during decision making. Analysts' strategies for resolving conflicts are investigated in the next section.

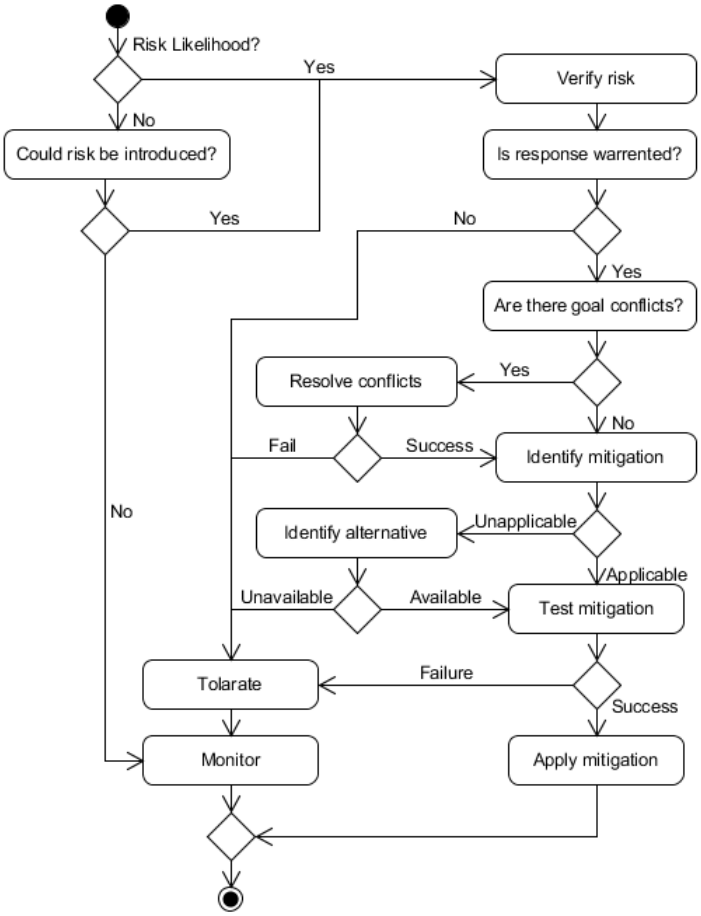


Figure 4.4: Decision making during vulnerability analysis

4.3 Reactive risk study

4.3.1 Approach

Reactive risk analysis includes real-time and posterior risk analysis, focusing on activities that address the whys and hows of incidences during and after occurrence (Li et al. 2010). This study focussed on understanding the analysts' approach to risk and uncertainty under constrained conditions - exemplifying reactive risk analysis.

While seeking approaches to overcoming the limited access to analysts, a data elicitation opportunity emerged to work with a group of 30 security practitioners undertaking a cyber defence capabilities workshop in Tokyo - Japan. Participants (PT 1 - 30) were drawn from 11 different Japan-based sectors including transport, steal, buildings, gas and manufacturing. The participants had roles in security or its facilitation and experience ranging from 1 to 20 years. Bournemouth University's research ethics procedures were considered throughout the data elicitation exercise. This included making the participants aware of the study's aim, the participant's freedoms during the study, and the signing of a con-

sent form before the study began (Japanese translation of Appendix .1.2 and .1.3).

The elicitation exercise lasted approximately 2 hours. First, the researcher made a PowerPoint presentation of a hypothetical scenario with conflicting goals which was simultaneously interpreted to Japanese by a translator. Having understood the scenario, the participants were asked to discuss how they would approach the conflicts in the scenario and were each given a form with the Japanese written version of the scenario and space for writing their answers.

As the participants were non-English speakers, the translator[2] also assisted in translating the participant's written responses from Japanese to English (Squires 2009). Translated responses were analysed at a later date and coded in NVivo 11, where Grounded Theory was used to identify thematic patterns depicting the analysts' approach to risk and uncertainty under constrained conditions.

4.3.2 Scenario

The scenario was inspired by the "Obligation goal conflict" identified in the Proactive risk analysis study. A scenario was used to avoid the complexities associated with abstract security questions and the sensitive nature of actual security operations in the participants' organisations.

> *You are a security analyst at a shipping company based in Tokyo. Your organisation needs to send urgent confidential information to new business partners in Osaka, however, the partners do not have secure and encrypted communication channels approved by your organisation's information security policy. As time is running short, the business manager asks for your advice on the issue.*

4.3.3 Findings

4.3.3.1 Approach to constrained conditions

As a result of the Grounded Theory analysis, thirteen themes emerged from Open coding. These were then grouped into four themes as part of Axial coding, namely Goals, Concerns, Assessment, and Decisions (see Table 4.2). Only the first two steps of Grounded

[2]The translator was a Japanese secretary with regular English translation assignments, a first degree, and twelve years experience working in the USA. A Japanese cyber security professor assisted in cases where security terminology was not understood by the translator. See Appendix .1.6 for sample participant responses in Japanese.

Open Coding	Axial Coding
Minimise Risk	Goals
Provide Guidance	
Secure Transfer within Time-frame	
Concerns	Concerns
Analysing Current Procedures	Assessment
Investigating Alternatives	
Analysing Threat Trends	
Monitoring	
Time-frame Extension	Decision
Transfer Cancellation	
Alternative Physical Options	
Alternative Electronic Options	
Negotiate Lesser Security	

Table 4.2: Grounded Theory analysis - Decision approach under constrained conditions

Theory were applied (open and axial coding) as the final step (selective coding) aims at identifying a core category to expose a central phenomenon. Unlike the first study, this would not be required when working with hypothetical scenarios. We detail the findings of Grounded Theory analysis and quotes from participants below.

- Goals
  To address the circumstances of the scenario, analysts established goals as a measure of satisfactory problem resolution. Goals were, however, varying, indicating differences in problem interpretation and understanding. For example, for some, the goal in the scenario was to minimise risk, while for others, it was to ensure the secure transfer of confidential information within a specific time-frame. The varying goals hinted on differences in resulting decisions.

  "Minimize impacts on management strategies." [PT17].

  "Have our manager to acknowledge risks (risks associated with information leakage)" [PT24].

  "Build secure transmission paths, and if impossible determine whether transmission using e-mails or websites is right or wrong." [PT3].

  "Suggest the best way to transmit confidential / sensitive information within the time limit." [PT12].

- Concerns
  Concerns were areas the analysts felt required clarification before decisions could be made. For example, enquiries were made on the urgency of the information transfer, the risks associated with possible information leakage, and the business partner's security capabilities.

  "It is fine if there is no information leakage, or if it is one-time-information-leakage?" [PT22].

  "Although we do not have encrypted communication channels which have been authorized, we might have other encrypted communication channels. Not clear urgency and necessity of online transmission." [PT18].

- Assessment
  Assessments were activities carried out to identify the best way forward. Assessments included analysing current security practices for effectiveness, assessing past security incidents to gain an appreciation of past security trends, monitoring the threat landscape, and investigating the feasibility of information transfer alternatives.

  "Conduct interviews, identify the history of information security policies. Confirm possibilities whether we are able to contact with other parties." [PT29].

  "...the information security policies for our organization and the ones for the Osaka BP." [PT18].

- Decisions
  Final decisions made included extending the transfer deadline, proposing the use of lesser secure information transfer alternative that were within the partner's capabilities, the use of alternative electronic transfer mechanisms such as video conferencing and fax, the use of alternative physical transfer options such as the Shinkansen (bullet train), or opting not to transfer.

  "Negotiate with BP (obtain an authorization for the transmission with lower security level)." [PT3].

"Propose to extend deadlines under HQ's security policies." [PT4].

"Facsimiles and Shinkansen are the alternative transmission options other than websites or e-mails." [PT11].

"...TV conference, introduce alternative options (Detailed data must be omitted)" [PT19].

"It would be suitable to deliver information to Osaka by my own (or subordinates)." [PT26].

4.3.4 Study implications

The findings indicate that although analysts seek clarifications when in doubt, this does not necessarily result in goal clarification. Sometimes analysts contemplate how to achieve perceived goals, instead of aiming to clarify them.

The findings highlight the role culture plays on analysts' perception of risk and decision making. For example, the bullet train was deemed as a suitable information transfer alternative in Japan, however, it may not be considered a viable option in other parts of the world. Similarly, PT26 suggested that they would prefer to physically transfer the information to Osaka on their own or use subordinate, hinting at a culture of commitment and uncertainty avoidance. Research by Hofstede et al. (2010) detail the influence of culture on decision making. According to their findings, cultural influences my be categorised into several dimensions. For example, the Japanese are more likely to make decisions through group cohesion and avoid uncertainty, whereas, the English have an individualistic approach to decision making and welcome uncertainty.

Beautement et al. (2009) introduced the term compliance budget, by which they posit that security compliance is a finite resource and the lengths at which one is willing to comply depends on the perceived reward to the individual. Compliance shall be maintained as long as its cost does not exceed the compliance threshold which is determined by individual benefit. While the benefit in our study is directed to the organisation and not the individual (analysts), the findings indicate that when constrained, analysts are willing to treat security as a tradable resource hinting at a possible compliance threshold. For example, the analysts enquire on permissible information leakage levels, or the decision PT3 makes to negotiate transmission at lower security levels. However, examining analysts from a compliance perspective is not fitting as their role is not about compliance,

but the enforcement and maintenance of security. As an alternative, the term *Relevance Scope* is introduced to describe the analysts' compliance. Relevance Scope is defined as a minimum level for the continued pursuit of a security goal.

The differences between the Compliance Budget and Relevance Scope are illustrated by using the graphs in Figure 4.5 adapted from Beautement et al. (2009), where the two propositions are plotted using the effectiveness of a security policy versus the perceived individual cost. The Compliance Budget is driven by the perceived individual cost and specific to user behaviour. For example, a policy statement (depicted by a circle on the graph) to backup work data on a weekly basis may seemingly cost an individual very little, and therefore complied with as it remains below the compliance threshold. Conversely, the Relevance Scope is driven by the effectiveness of security by taking risk into account and is specific to security enforcement. For example, some staff members may slack and forget to back up their data though viewed as a manageable cost in their compliance budget. However, based on the data's value, the analysts would ensure the policy is abided with, as the associated risk levels surpass the minimal level for the continued pursuit of a security goal (Relevance Scope),

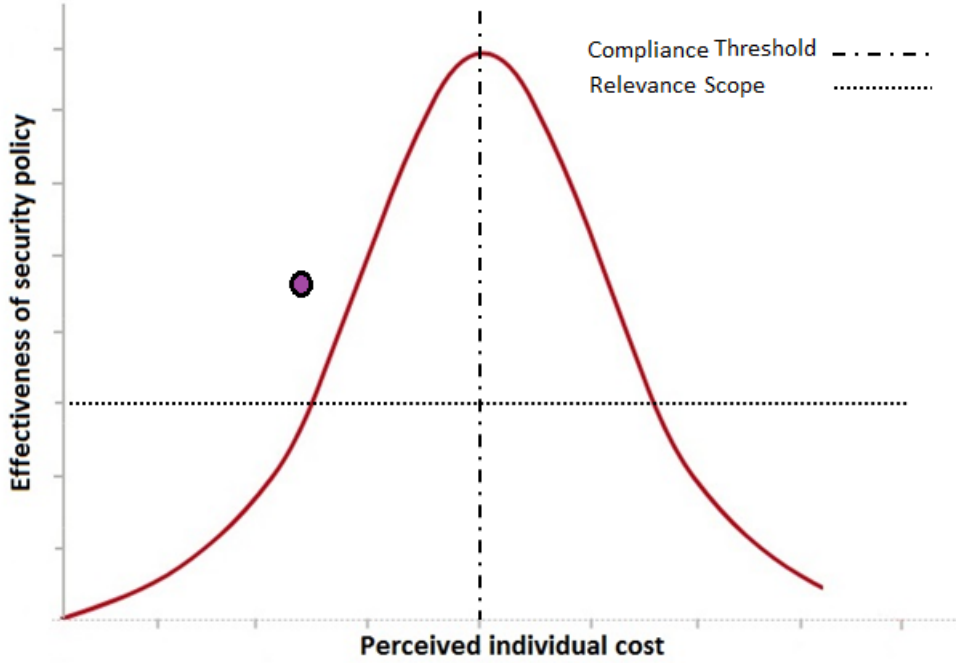


Figure 4.5: Compliance budget versus Relevance scope

4.4 Chapter summary

In this chapter, factors influencing the risk analysis practices deployed by cyber security risk-based decision makers were investigated. Factors promoting risk understanding and strategies analysts' use to resolve conflict situations were identified. Findings also hinted on the role information, goals, perception and culture play in security decision making, and the security enforcement behaviour, termed the *Relevance scope* was identified. In the following chapter, the knowledge drawn from this chapter and the literature is used to develop a normative model for facilitating the transparent fine-grained communication of security decision making.

Chapter 5

A Normative Model for Rationalising Decision Making about Risk

5.1 Introduction

This chapter presents a normative model for communicating and tracing the rationalisation of risk by cyber security decision makers. This work builds on findings from Chapter 4 and literature on security and decision making.

The chapter is the first of two addressing research aim 2: To propose approaches for adapting cyber security decision making techniques to design.

Research on expert decision making during risk and uncertainty has indicated that experts e.g., security analysts, take decision making shortcuts when moving from ambiguity to certainty. This line of research has been pioneered by Klein's (1999) work on naturalistic decision making, where it was identified that experienced firefighters use situational familiarity for quick decision making as opposed to weighing all available alternatives - a type of heuristics. Similar expert-decision findings are presented by Wong and colleagues (2014, 2015) on criminal intelligence analysts, and Hibshi et al. (2016) on cyber security analysts. While these findings are informative, a comprehensive process for eliciting design requirements for systems supporting RBDM, would have to explain more than the expertise-based shortcuts by elaborating on the decision making steps during risk and uncertainty.

Normative models are particularity useful for this as they act as blueprints upon which awareness and decision making may be traced and communicated [1]. Early work by Rasmussen (1974) on the Decision ladder template has played a key role in identifying the

[1] see Section 2.3.1 for details on the normative perspective.

generic steps to decision making, whereas OODA (Boyd 1996) and Situation Awareness (Endsley 2015) played key roles in exemplifying the generic steps to awareness. The work in this chapter expands on these by presenting a normative model grounded in security decision making findings, that illustrate a detailed view to risk rationalisation.

5.2 Establishing the normative model

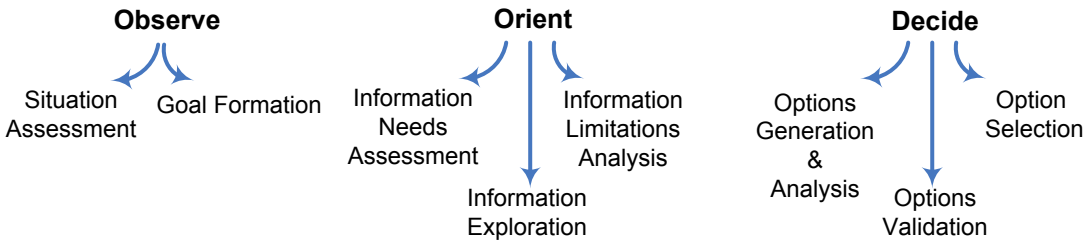


Figure 5.1: Adapting OODA

Illustrated in Figure 5.1, OODA was used as a modelling baseline, selected for its simplicity and easy adaptability[2]. To develop a model that captures security risk rationalisation with fine-grained details, OODA steps were instantiated with comparable risk rationalisation finding from the conducted empirical studies and literature. Sub-categories were then created under each OODA step where the instantiated steps had noticeable variations. For example, findings on one's ability to recognise insufficient information and findings on one's ability to recognise excess information were grouped under OODA's Orient as two separate risk rationalisation categories. Once categorisation was complete, suitable titles were assigned to the new steps and ordered in accordance with the researcher's understanding, thus forming the model. The following additional considerations influenced model design:

- OODA's final step ACT was not included as it is a product and not a part of the rationalisation process.
- Design followed an incremental and iterative process where adaptations were continuously made based on new insight.
- Unlike the single starting point presented in OODA or other awareness and decision making models, our findings indicated that security decision making had two alter-

[2]see Section 2.3.4.2.

native starting points - one for proactive and the other for reactive analysis. Details are provided in the following section.

- Based on the amount of detail the model captures, presenting it in one diagram would have been difficult. It was, therefore, sub-divided into two complementary elements, one illustrating the process and the other detailing the steps.

The model is presented in the section below, before validating it in two studies; the first validates the model's sequence using cognitive walkthroughs in a focus group and the second validates the model's application by eliciting analysts' views on automating aspects of risk rationalisation during security analysis.

5.3 Model design

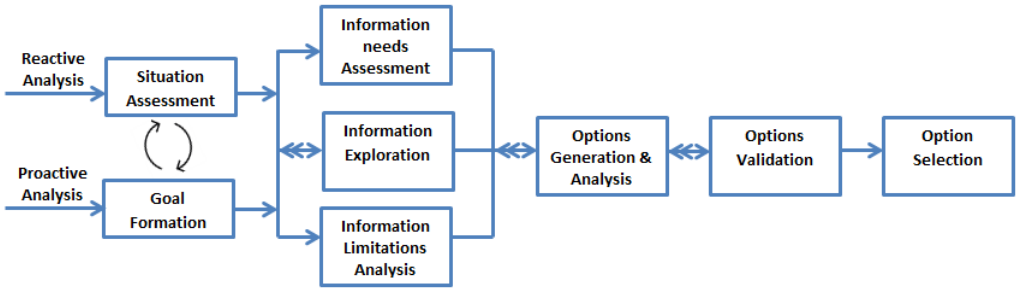


Figure 5.2: Risk rationalisation flow

The normative model consists of eight steps to risk rationalisation and consists of two complementary elements; the Flow and Actions collectively referred to as the Risk Rationalisation Process (RRP).

5.3.1 Risk Rationalisation Flow

The first element is a Risk Rationalisation Flow (RRF) highlighting sequences and iterations during risk rationalisation. Illustrated in Figure 5.2, RRF indicates two alternative starting points; reactive risk analysis beginning with Situation Assessment and continues to Goal Formation, while proactive risk analysis presents an inverse flow starting with Goal Formation and continuing to Situation Assessment. The difference is based on the understanding that security strategies precede incidents in proactive analysis, goal formation, therefore, begins before assessment, while the inverse is true in reactive analysis where goals are set after incidents.

The second part of RRF consists of the three information related steps, these are; Information Needs Assessment, Information Exploration, and Information Limitations Analysis (detailed in sections 5.3.3.3, 5.3.3.4, and 5.3.3.5, respectively). Their adjacent positioning in Figure 5.2 indicates that the steps may overlap and occur in varying order.

The final three steps occurring in sequential order relate to options. These are; Options Generation and Analysis, Option Validation, and Option Selection (detailed in sections 5.3.3.6, 5.3.3.7, and 5.3.3.8, respectively). Risk rationalisation is an iterative process which is illustrated in RRF by the reverse arrows at each point of possible iteration.

5.3.2 Risk Rationalisation Actions

The second element of RRP consists of the risk rationalisation actions illustrated in Figure 5.3. The actions address the lack of fine-grained detail in normative models by providing context-related meta-cognitive questions at each rationalisation step. Metacognition is defined as awareness or analysis of one's own thinking processes, this may be expounded upon as the knowledge of knowledge (what one knows about their thinking), and the regulation of knowledge (how one uses that knowledge to manage thinking) (Schraw and Moshman 1995). For example, to understand the rationale behind the characterisation of a situation, the question "how may a situation be understood?" is posed. The question is posed retrospectively, hence meta-cognition. The risk rationalisation actions also present procedures for clarifying the questions. In the case of "how may a situation be understood?" the procedure could be through data correlation, which is the piecing together of disparate data sets to derive meaning. By using the rationalisation steps, meta-cognitive questions, and procedures, RRP aims at understanding the rationale behind decision making irrespective of the decision maker's expertise.

5.3.3 Step in the Risk Rationalisation Process

The eight RRP steps below are detailed below.

5.3.3.1 Situation Assessment

Situation Assessment corresponds to OODA's Observe. During this step, the aim is to understand how the decision-maker identifies factors aiding in situation understanding and not the actual analysis of the situation. The meta-cognitive question "how may the situational be understood?" is presented and expanded into four possible procedures:

- *Knowledge of a situation*: This is experienced-based recognition through situation familiarity and the knowledge of normal states. For example, analysts with expe-

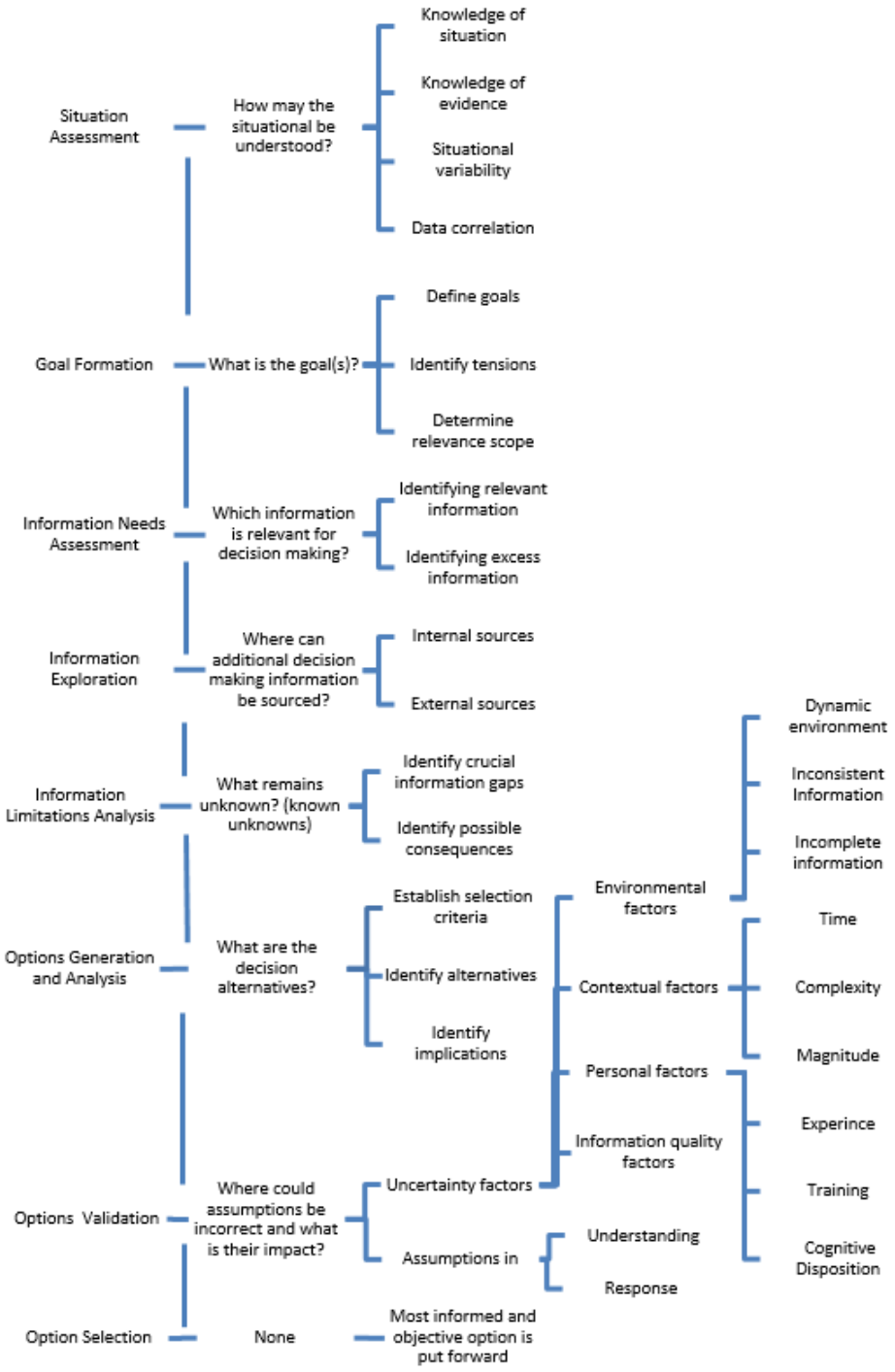


Figure 5.3: Risk rationalisation actions

rience of a network's activities could have a rough idea on how many failed logins are generated every hour. Deviations would consequently trigger suspicion, albeit, its susceptibility to judgement biases (see Section 2.3.2.3 for Judgement biases).

- *Knowledge of evidence*: This is experienced/training-based recognition by recognising information affordances in an environment to achieve greater awareness (Norman 1999). The reasoning is inductive through the identification of informa-

tion affordances; this is in contrast to deductive reasoning used in the step above. In other words, knowledge of evidence is not grounded on a hypothesis.

- *Situational variability*: This is the recognition of the dynamic elements of a situation such as state and context. Situational variability involves understanding the present state and aiming to understand possible alternatives by projecting future states. Endsley (1995) gives the example of knowing how a threat aircraft would attack based on positioning. In cyber security, this could be understanding the alternative security implications new users and services could introduce on a network.

- *Data correlation*: This is the ability to recognise the disparate pieces of data that must collaborate to achieve greater awareness. For example, the use of data from multiple tools to validate findings.

5.3.3.2 Goal Formation

Goal Formation is a step also corresponding to OODA's Observe. The objective is to understand the strategies used to establish decision goals, identify tensions that may restrict goals from coming to fruition, and the determination of the relevance scope within which a decision is made. The Relevance Scope was defined as a minimum level for the continued pursuit of a security goal (see Section 4.3.4). For example, analysts interviewed in the proactive risk analysis study (Section 4.2) expressed that the inner workings of some of the proprietary security products they used were unknown to them. However, based on the product's benefit, they found uncovering the potential risk inessential.

5.3.3.3 Information needs Assessment

Information needs Assessment is one of three steps corresponding to OODA's Orient. The objective is to understand how the decision-maker identifies information relevant for decision making and the filtering of excess information. The decision-maker's assessment is based on information credibility determined by factors identified during Situation Assessment and the Relevance Scope identified during Goal Formation. For example, the identification and treatment of false positives as extraneous information, while recognising their effect on overall decision making. During the proactive risk analysis study (Chapter 4), it was identified that Linux servers had an ongoing false positive related to backporting (RedHat 2017). As a false positive, analysts recognised the importance of flagging it. While the action had no impact on their present work, it expedited future analysis and decision making.

5.3.3.4 Information Exploration

During Information Exploration, it is recognised that decisions are determined by information availability and when information is unavailable, possible alternatives are explored. The focus is therefore placed on understanding the strategies for identifying the alternative sources of information. To the decision-maker, the exploration of additional sources of information is usually subject to available time. Information sources may be subject matter experts within the analysts' environment, for example, legal officer, public relations manager, or external experts such as CERT analysts.

5.3.3.5 Information Limitations Analysis

Information Limitations Analysis is driven by the question, what remains unknown? This is presented with the aim of understanding how the decision-maker identifies critical information gaps and the conclusion drawn from the knowledge. Information gaps refer to the known-unknowns critical for informed decision making which includes gaps requiring further information exploration, or gaps resulting from weak evidence and requiring further collaboration with available data to build confidence. For example, it would be advantageous for an analyst to recognise that an attack vector has been identified although the motive and capabilities of the attacker remain unknown. Recognition of the missing information such as the motive for an attack promotes preparation and investigations (Rashid et al. 2016).

5.3.3.6 Options Generation and Analysis

Options Generation and Analysis is the first of three steps corresponding to OODA's Decide. The aim of the step is to identify and understand the reasoning behind options considered by the decision-maker. Based on the cumulative understanding from the previous steps, the decision-maker establishes an option selection criterion and identifies qualifying options for decision formulation and their implications. For example, analysts who felt their goal was to minimise risk during the reactive risk analysis study (Section 4.3), would most likely not have quick information transmission as a primary factor in their selection criteria. Options Generation and Analysis also involves verifying if the possible options are sub-optimal. This is where the identification of potential unwanted effects of the options becomes crucial.

By this point, a decision-maker's limited understanding may inadvertently introduce meta-risk (decision risk). Meta-risk is the risk resulting from one's decision making on potential risk and can be in two forms. This are the risk of understanding e.g., forming incorrect goals due to a lack of understanding and the risk of response e.g., increasing threat

exposure resulting from the implications of a selected response option.

5.3.3.7 Options Validation

Options Validation focusses on uncertainty by verifying if there were elements of uncertainty hindering the decision making process and how they were managed. Option Validation also aims at examining the potential impact of failed risk understanding and risk response. Factors causing decision uncertainty are groped into the four categories listed below:

- **Environmental factors**
  The environment is the situation within which decisions are made. Environmental factors includes:
  - Dynamic environments: Continuously changing environment.
  - Inconsistent information: Continuously changing information in the environment.
  - Incomplete information: Inadequate information in the environment.
- **Contextual factors**
  Context characterises a situation within which a decision is made (Dey 2001). This includes:
  - Time limitations: Inadequate time for decision making.
  - Situation complexity: A situation difficult to understand because of one or many other factors.
  - Problem magnitude: A situation with multiple factors to consider.
- **Personal factors**
  These are attitudes, aptitudes, skills, and capabilities a decision-maker may possess that could influence decision making. These include:
  - Experience: Knowledge or skill from doing or seeing.
  - Training: Learned skills required for a particular job or activity.
  - Cognitive disposition: Limiting mental models, biases, and heuristics (see Chapter 2.3.2).
- **Information quality factors**
  These are; accuracy, current, relevant, specific, understandable, comprehensive, unbiased, and comparable. A detailed explanation on these factors is presented in Wang et al. (2005).

5.3.3.8 Option Selection

Option Selection is the third of three steps corresponding to OODA's Act. As a final step, the most informed and objective option is put forward as the basis for a decision. The decision should not come as a surprise where the rationale is traceable.

5.4 Model Conclusion

In this section, RRP was presented detailing the steps to risk rationalisation. Key points from the model include an illustration of the two complementary elements of RRP. The first was the Rationalisation Flow which illustrated the process to risk rationalisation and highlighted the difference between proactive and reactive risk rationalisation. The second was the Rationalisation Actions providing guidance for communicating and tracing steps to risk rationalisation which included procedures that provided fine-grained details at each rationalisation step.

The model stressed the importance of information during risk rationalisation by presenting three information orientation steps, it illustrated the role of goals and subsequent decision options, and it illustrated the importance of recognising uncertainty as an element separate from risk which requires similar analysis. Four groups of uncertainty worth considering during risk rationalisation were presented, these related to the decision-makers' environment, context, information, and information quality. Lastly, meta-risk was introduced as the risk of decision making on potential risk which is categorised as the risk of understanding and the risk of response.

In summary, the model highlights four main areas in risk rationalisation, these being understanding, goals, uncertainty, and response.

5.5 Sequence validation

5.5.1 Objective

This section presents a study where the Risk Rationalisation Process was validated using Cognitive Walkthroughs (Rieman et al. 1995) during a focus group session (Flick 2014). The aim was to validate the sequence and steps of RRP and not the model's ability to communicate risk rationalisation. This is covered in Section 5.6.

5.5.2 Participants

Three participants (P1-3) were recommended through contacts; the three were security analysts from organisations within the UK. P1 and P2 worked as part of a cyber security team monitoring events within their organisation and possessed 1 to 3 years of professional experience in security. P3 worked for a counter-terrorism and intelligence unit and possessed over 24 years of relevant experience.

5.5.3 Approach

The focus group was held at Bournemouth University, where each participant was provided with a copy of RRP and given a brief tutorial on its application. Participants were then presented with the hypothetical scenario below about a data breach, incorporating tensions related to possible decisions and uncertainty due to insufficient information. The participants were asked to walk-through RRP, comparing the model's steps with steps they would actually take addressing the scenario. Participants jotted down their views, and in addition, P3 ran a second walk-through based on his experience in counter-terrorism. On completion, focus group discussions began with participants presenting their critiques of the model's sequence and steps. The session ran for approximately 40 minutes, and the researcher moderated discussions and took notes. Bournemouth University follows similar ethical procedures for interviews and focus groups. As such, the participant information sheet and consent form (Appendix .1.2 and .1.3)) approved for interviews in sections 4.2 and 4.3 were also used for this study.

5.5.4 Scenario

The scenario required the analysts to decide whether to make a breach on a university's network known to affected parties in advance, after remediation, or not at all. In addition, they had to take into account that some of the breached data was already on the dark web. The scenario was inspired by events that occurred during an attack on JANET, the network used by the UK research and education community (Buller 2016).

> *A University's CERT has uncovered a breach in the University's IT network, where hackers have infiltrated the student database and posted their personal details on the dark web. While the incident seems at its infancy, the University has to decide on disclosing the breach immediately, disclosing the breach after successful containment, or avoid disclosing the breach altogether.*

5.5.5 Findings

Having gone through RRP and the scenario, analysts felt the sequence and steps presented were justified, although the analysts might only have taken some of the three information related steps (Information Needs Assessment, Information Exploration, and Information Limitations Analysis). The findings were expected as normative models do not aim to illustrate experienced-based decision, but how decisions should be made with respect to rational choice. Opinions were, however, divided on whether Option Validation was an independent step or part of Option Generation and Analysis. P1 and P2 felt that options are validated as they are generated and the two are not independent of each other. We concluded that the two were independent steps as lesser experienced decision makers would have to generate options for a decision before validating them. Simultaneous validation would require substantial levels of experience, the understanding the RPD model is based upon (see Section 2.3.3.2). Having validated the steps and sequence, the next goal was to validate RRP's capacity for communicating the rationalisation of risk.

5.6 Model validation

5.6.1 Objective

To demonstrate the application of RRP, a study was conducted with nine Information Systems (IS) personnel from a variety of organisations in Tokyo - Japan. The participants were engaged as part of continued collaboration with Japanese security practitioners undertaking cyber defence capabilities workshops (introduced in Section 4.3). The study's aim was to elicit the participants' views on automating aspects of risk rationalisation during security analysis. A focus on automation meant the model's validation could be done simultaneously with the exploration of approaches for better applying automation to security decision making[3].

Under real settings, the knowledge gleaned from this study would form the basis for nuanced requirements for security automation that are grounded in user understanding as opposed to default automation levels for all; which typically result in unusable systems (Chiasson et al. 2007). Demographic factors such as experience, roles, and industry could also be used in representative and longitudinal studies to uncover risk rationalisation norms and deviations thereof. The findings could hint at hidden biases and unveil the need for system adaptations and training.

Findings from this study do not aim at providing statistical accuracy as the work did not

[3]See Section 2.4.3 for a discussion on the ironies of automation and their implication to decision making.

have a representative sample size. Rather, the aim is to illustrate how RRP may be applied to communicate the rationalisation of risk (proof of concept).

5.6.2 Participants

Illustrated in Table 5.1, two of the nine participants (PT1-9) had security-specific roles working in Computer Security Incident Response Teams (CSIRT), while the rest had security as a part of other IS responsibilities. The participants had work experience ranging from one to ten years and were all selected based on availability. For illustrative purposes, the four participants with a maximum of two years experience are referred to as Novice (PT1-4), and the remaining five with a minimum of six years are referred to as Experienced (PT5-9).

Participant	Industry	Role	Experience (Years)
1	IT	IS Support	1
2	Electricity	CSIRT Analyst	1
3	Printing	CSIRT Analyst	1
4	Electricity	IS Support	2
5	Electricity	IS Support	6
6	IT	IS Support	8
7	Oil	IS Support	9
8	IT & Communication	Engineer	9
9	Chemical	Systems Operations	10

Table 5.1: Automation study participants

5.6.3 Approach

Like the validation exercise in Section 5.5, participants were trained on RRP and provided with a cybersecurity decision making scenario containing elements of risk and uncertainty. Using the scenario, participants were asked to indicate whether or not they would use automation during the different step of risk rationalisation and to provide justifications for their answers. For example, based on one's understanding, would they opt to automate the Situation Assessment step relating to situational understanding, or opt to automate the Options Generation and Analysis step relating to the identification of options and their implications?

The study sought to elicit the participants' general opinion on automation, not views based on the effectiveness of existing tools. The RRP steps considered were from Situation Assessment to Options Validation. Option Selection was omitted as the automation of this step would imply a system is the final decision maker and not the human.

Participants were briefed on the ethical procedures to be followed and written consent was sought before the study began (Japanese translation of Appendix .1.2 and .1.3). The study ran for approximately one hour, where participants provided written responses in Japanese, which were later translated to English[4]. Translated data was imported to Microsoft Excel where the participant's selection and justifications were analysed by the researcher.

5.6.4 Scenario

The scenario was inspired by findings on analysts' abilities to infer hacking activities based on certain types of network traffic (Werlinger et al. 2010).

> *You are a security analyst at a shipping company based in Tokyo. You have been monitoring the network traffic at the Osaka regional office and have noticed suspicious Twitter and Internet Relay Chat (IRC) traffic. There is the possibility that this could be an incident in progress. Following the RRP model steps, which parts of your security analysis would you automate to facilitate understanding?*

5.6.5 Findings

5.6.5.1 All respondents

The first part of the findings represent all respondents (novices and experienced). For this part, focus was on the risk rationalisation steps with the highest and lowest outcome. Illustrated in Figure 5.4, Situation Assessment had the highest outcome, with seven of the nine participants opting for automation the step. Participants felt that systems were more efficient in detecting situational changes as compared to humans. Comments for the choice included:

"Systems have a better understanding of network traffic and monitoring for signs of risk" [PT7].

"We register the strings to be checked in advance and issue an alert..." [PT1].

Information needs Assessment had the lowest outcome with none of the participants opting to automate, seconded by Option Validation with only one participant opting for

[4]We maintained the translator from the reactive analysis study (Section 4.3) as they had gained an understanding of our work and could provide better contextual translations.

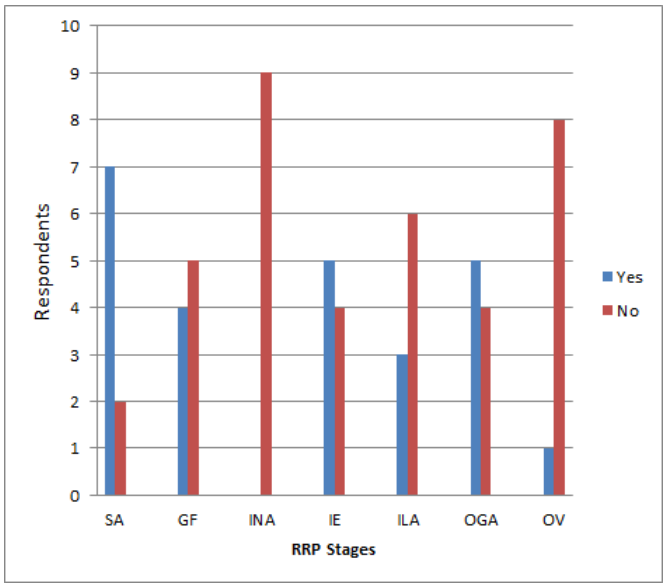


Figure 5.4: Automating security analysis (all respondents)

automation. For Information needs Assessment, the reasoning was that humans are better at determining information requirements for decision making, thus automation would not be as effective. However, participants felt that automating the validation of options was beneficial, though it would require large and ever increasing amounts of data. Comments promoting the two choices included:

"When determining the necessary or unnecessary information, one's experience or wider perspective would be required" [PT6].

"It is ambiguous for a system to determine unnecessary information" [PT9].

"New information might emerge fluidly; thus, automation would be impossible" [PT6].

"Although mechanical correlations could be derived by automation; automation in causation could be difficult" [PT9].

5.6.5.2 Novice versus Experienced

The second part of analysis aimed at identifying if there were substantial differences in the novice versus the experienced choice. Illustrated in Figure 5.5, differences were observed in Information Limitations Analysis where none of the experienced opted to automate, while three of the four novices opted for it. Like the Information needs Assessment finding above, the experienced felt humans were better at determining information requirements for decision making. Comments leading to the contrasting choices included:

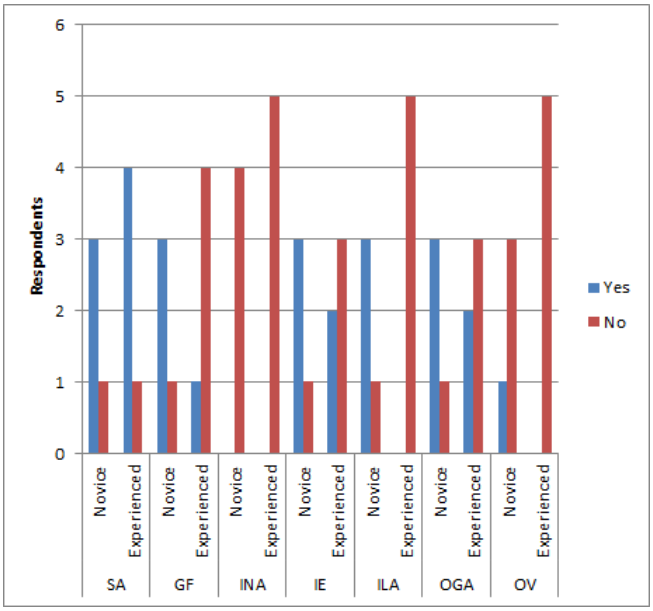


Figure 5.5: Automating security analysis (novice vs experienced)

"Since information acquisition is uncertain, automation would be impossible" [PT7].

"If information is limited, we would be able to determine such information using conditional branching" [PT1].

As an overall, the results indicate that the experienced were lesser inclined to automate with Situation Assessment as their only selection higher than the novice's choices. It would be reasonable to expect that more experienced practitioners would have a better understanding of when to rely on their judgement and when not to.

5.6.6 Study implications

The study presented a proof of concept on the application of RRP. It illustrated how the risk rationalisation steps during security analysis could be considered for automation based on user requirements, therefore leveraging human and system decision making capabilities.

As expressed above, the aim is not to draw too much from the quantitative aspects of the study due to the limited sample size, however, the findings indicate which risk rationalisation steps were preferred for automation. The findings also reveal that opinions *within* the two groups were mostly similar, while opinions *between* the groups were mostly different, indicting the analysts' understanding of the model. By using the experienced and novices as two independent and contrasting study variables (MacKenzie 2013), it is believed the

soundness of RRP as a nuanced approach for communicating risk rationalisation has been illustrated.

5.7 Chapter summary

In this chapter, RRP was presented as a normative model for rationalising decision making about risk. Its use was described and two studies validating its sequence and application were presented. The model is not the proposition of a new approach to decision making, but rather, one that complements existing approaches but adding a level of granularity appropriate for risk rationalisation in RBDM.

The model aims to serve two purposes, the first as a tool facilitating the analyses of security decisions (communication and traceability), and the second as a baseline upon which design requirements for RBDM are elicited. This chapter achieved the first, the second is expanded upon in the following chapter, by presenting a conceptual model for RBDM based on the four main areas identified in risk rationalisation. These are understanding, goals, uncertainty, and response.

Chapter 6

Conceptual Model for Risk-based Decision Making

6.1 Introduction

This chapter presents a conceptual model for designing for RBDM illustrating the various concepts in cyber security decision making and their relationship. The model is grounded in findings from previous the chapters but particularly builds on areas identified in RRP. While RRP took a cognitive view to understanding risk and uncertainty in cyber security decision making, the conceptual model shifts to a design view linking decision making findings in risk rationalisation to the design domain. In turn, the chapter illustrate how RBDM concepts may be reasoned about in design.

The chapter is the second of two addressing research aim 2: To propose approaches for adapting cyber security decision making techniques to design.

6.1.1 Conceptual models

In systems design, conceptual models are an abstract representation of a system (social or technical) presented in text or diagrammatic forms. The role conceptual models play includes enhancing the understanding of the system they represent, promoting the efficient conveyance of system details, and providing a reference point for system designers to gather system requirements. Conceptual models also aid in identifying system-specific concepts, entities, and entity relationships that could otherwise be overlooked during design (Johnson and Henderson 2002).

Risk Forms	RRP Steps	Step's Procedures
Risk of understanding	Situation Assessment	All
	Information Needs Assessment	All
	Information Exploration	All
	Information Limitations Analysis	All
	Options Validation	Personal factors
Goal risk	Goal Formation	All
Uncertainty risk	Options Validation	All
Risk of response	Option Generation & Analysis	All

Table 6.1: Risk forms in RBDM

6.1.1.1 Risk forms

This chapter presents an integrated RBDM conceptual model highlighting the risk forms that should be considered when designing for RBDM. The risk forms are used as a vehicle to ease the elicitation of requirements driven by the understanding that it is sometimes easier to elicit requirements by aiming to identify what is missing (consequences of decisions), than focussing on desired abilities (Faily and Fléchais 2016). This being the case, the risk forms highlight the consequences of missing requirements in a RBDM process.

To ensure that a complete set of requirements are captured, the risk forms were elicited from risk rationalisation practices in cyber security decision making (RRP). Table 6.1 illustrates how the RRP steps and procedures informed the identification of the risk forms. All steps translated to a single risk form with exception to Options Validation (Section 5.3.3.7) which translated to the risk of understanding and risk from uncertainty. This is because personal factors under Options Validation may translate to the risk of one's limited understanding or the risk of an information provider's limited understanding - which is a source of uncertainty.

6.1.1.2 Sub-models

The integrated RBDM conceptual model focusses on three of the four risk forms highlighted in Table 6.1, namely, risk in understanding, goals risk, and uncertainty risk. For each risk form, a sub-model expanding on the integrated model's details is presented, these are: Personal-risk model, Goal-risk model, and Contextual-risk model. The fourth risk form - the risk of response - is presented in Chapter 7 as its relationship is modelled at a higher level.

The models are designed using UML Class diagrams (Rumbaugh et al. 1999), selected for their widespread use in systems design and their ability to represent the proposed concepts. As an overall, design of the conceptual models draws inspiration from the IRIS meta-model (Integrating Requirements and Information Security), a model focused on specifying security and usability requirements during the early stages of system design (Faily and Fléchais 2010b).

6.1.1.3 Running example

For each model, examples illustrations are presented using adaptations of events surrounding a Distributed-Denial-of-Service (DDoS) attack on the Australian Bureau of Statistics in 2016. The scenario was identified as part of the on-going literature review during the progression of the research. While alternative security scenarios such as the attack on the Singapore Health Services were considered (Ministry of Communications and Informations 2019), the DDoS attack on the Australian Bureau of Statistics was selected as it portrayed the role decision making may play in causing and exacerbating security incidents. There also were up-to-date academic publications on the event (Ceric and Holland 2019) and reports from involved industrial entities (IBM Australia 2016, Vocus Communications 2016, Nextgen Group 2016). The event also provided a reasonable level of complexity for illustrating the various concepts the researcher proposes. A brief overview of the incident adopted from MacGibbon (2016) is provided below.

6.1.2 Australian Bureau of Statistics DDoS incident

The 2016 Australian national census was conducted on 9 August 2016. Unlike previous censuses in 2006 and 2011, this was fully run online. The Australian Bureau of Statistics contracted IBM to run the systems; selected for its successful delivery of the two previous censuses which were partially ran online. IBM approached the project by setting up a data centre for running the census website and agreed to provide a minimum of 98% website availability for accessing, completing and submitting census forms. Denial of service attacks were identified as the main security concerns, to which IBM sub-contracted two Internet Service Providers (ISP) (NextGen and Telstra), providing alternative public access to the website. In addition, a DDoS mitigation strategy for traffic originating from outside Australia (geoblocking) was agreed upon - to be implemented at the ISPs. On census night, malicious DDoS attacks were successfully launched against the census website resulting in its partial shutdown, where the first attack was at around 3GB/s and lasted 11 minutes. Reasons for the successful attacks include but are not limited to the following decisions and actions.

- Geoblocking only addressed traffic originating from outside Australia with no clear strategy for domestic traffic in place.
- Geoblocking was tested for only 10 minutes though it was identified that attacks could last an average of 16 hours.
- The ISP NextGen did not have geoblocking enabled.
- Though two ISPs were contracted, the two had the same upstream provider (Vocus) that had also failed in implementing geoblocking, resulting in a single point of failure.
- An attempt to restore systems during a fourth attack led to router failure, compounding network issues.

6.2 Integrated model

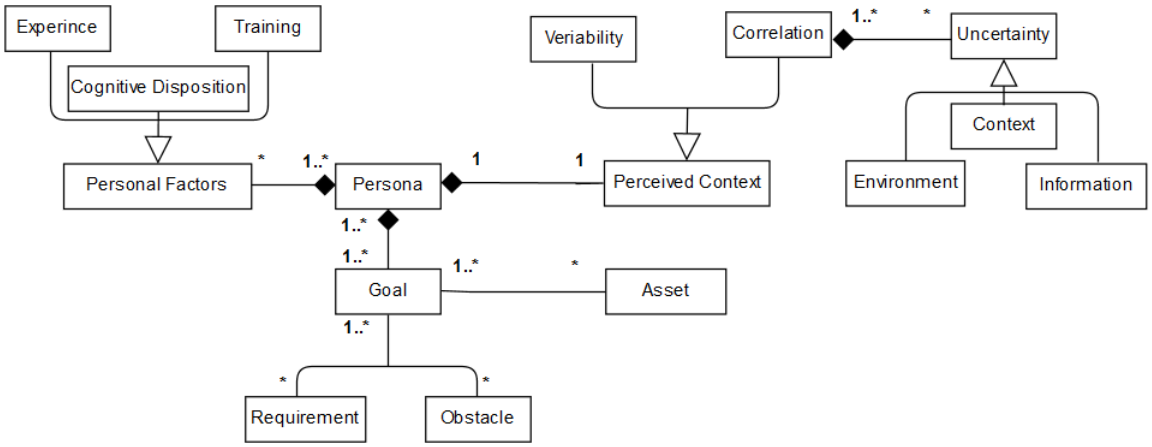


Figure 6.1: RBDM conceptual model

The conceptual model for RBDM illustrated in Figure 6.1 serves as an overview illustrating the relationships between entities in the three identified risk forms. An explantation for the model and link to the risk forms is as follows: At the centre of the model is the persona who is the decision-maker. The persona may have personal factors that influence or fail to assist decision making and possibly resulting in risk (Section 6.3: Personal-risk). The persona's decisions are driven by goals that must be satisfied. As our personas are specifically decision makers, decision goals that reflect the desired system properties will always be present, however, situations may arise where the goals are unattainable (Section 6.5: Goal-risk). To make informed decisions, decision-makers can only rationalise what they perceive; which is facilitated and validated by available information. As perception is sometimes not a true reflection of the actual context (Klein et al. 2007), it results in contextual risk (Section 6.4: Contextual-risk). Similarly, the level of confidence that may

be placed on information facilitating the understanding of situations may also be limited (Section 6.4.1.4: Uncertainty). Detailed explanations for each sub-model are below.

6.3 Personal-risk model

6.3.1 Defining Personal-risk

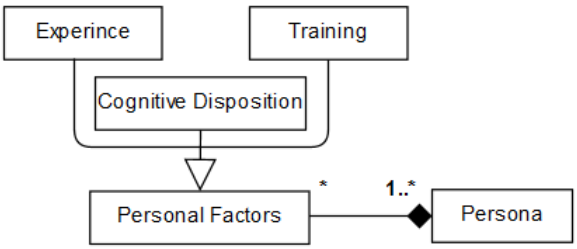


Figure 6.2: Personal-risk model

Illustrated in Figure 6.2, the Personal-risk sub-model dwells on modelling decision risks resulting from personal factors. Personal factors are a collection of attitudes, aptitudes, skills, and capabilities one may possess that could influence decision making. These are specific to the decision-maker (persona) and were detailed in RRP as experience, training and a cognitive disposition (see Section 5.3.3.7). A persona may have several factors whose presence or lack of, may contribute to risk. While it is unlikely that one may have absolutely no personal limitations, we opt to say a persona may have zero-to-many personal factors to indicate that the limitations may not be related to the decision in question. On the other hand, similar factors may apply to one or more personas. For example, a lack of training in an area critical for a decision may affect all lacking training.

6.3.2 Personal-risk example

Using the Australian Bureau of Statistics incident example in Figure 6.3, an examination of the analysts at the ISP's providing public access to the census site might have indicated that some did not have the required training or experience to correctly configure the geoblocking DDoS mitigation strategy. Overconfidence (bias) might also have clouded the ISP analyst's judgement, as the two previous censuses in 2006 and 2011 had run smoothly, albeit a lower number of online users (Ceric and Holland 2019).

Equipped with knowledge from such analysis, designers may begin to identify requirements for addressing the analysts' limitations.

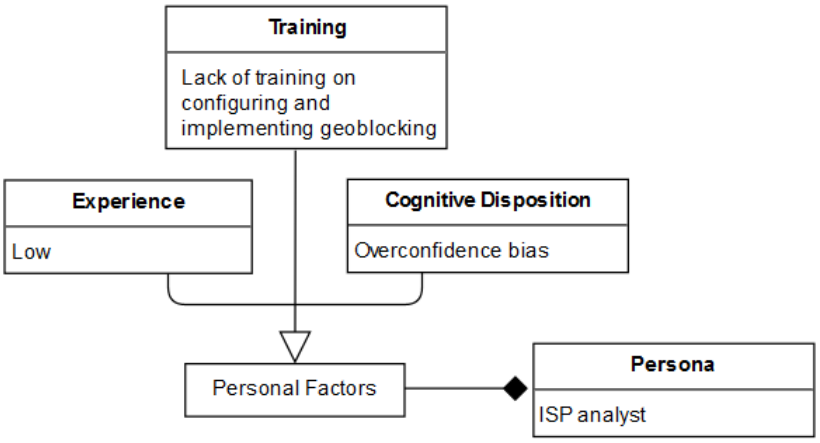


Figure 6.3: Personal-risk model example

6.4 Contextual-risk model

6.4.1 Defining Contextual-risk

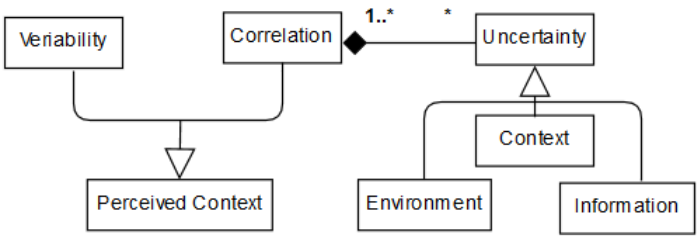


Figure 6.4: Contextual-risk model

The Contextual-risk sub-model dwells on modelling decision risks resulting from the perception of a situation. Illustrated in Figure 6.4, the model's main focus is the Perceived Context which is a composition of Correlation and Variability that were explained in RRP's Situation Assessment step (Section 5.3.3.1) and further detailed below.

The term perceived is used to indicate that the context is a product of a decision-makers view, differentiating it from the actual context that is independent of the decision-maker. In RRP, the actual context was explained as the characteristics of a situation within which a decision is made (see contextual factors in Section 5.3.3.7).

The understanding that a perceived context is independent of an actual context has been expressed in various scholarly articles. For example, Wong and Varga (2012) discuss the data keyhole problem, explained as an information analysis limitation where one only sees a small part of a large dataset due to computational or display constraints. Another example may be found in Klein and colleagues' (2007) data-frame theory, where a frame is the portion of perception that is internal to the perceiver and accepts information as it

becomes available. What is common in the Keyhole and Data frame theories, is that, like the perceived context, they both are a decision-maker's limited view of an actual context.

6.4.1.1 Variability

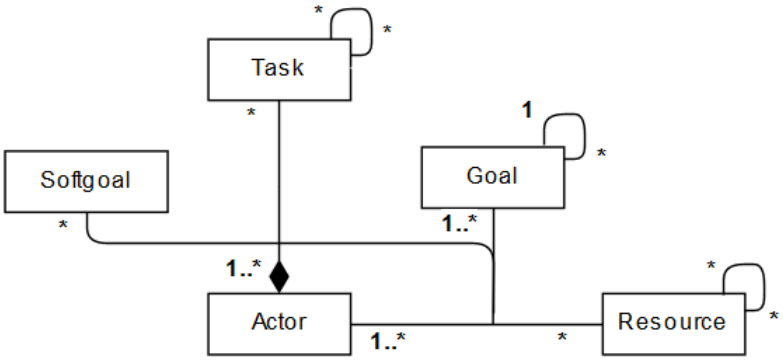


Figure 6.5: Contextual-risk model (Variability)

Variability is the understanding of the dynamism of a situation, or in other words, the projection of alternative states. Here, the contextual risk lies in the failure to identify plausible situational alternatives in the problem domain. To design for Variability (Lapouchnian 2005), actors, their goals (actor goals), tasks, resources, and softgoals are used to model contextual variations.

According to the i* framework (University of Toronto 2011, Yu 1997), an actor is an entity that has strategic goals and intentionality within a system or organisational setting. Goals represent the actor's strategic interests that have clearly defined satisfaction criteria. Softgoals are goals that do not have clearly defined satisfaction criteria; they are therefore satificed as opposed to satisfied and are often used to define quality. Tasks are specific processes actors perform and resources are physical or informational entities used by the actors.

As illustrated in Figure 6.5, modelling of variability is centered on a minimum of one actor, with at least one goal as an expression of intentionality. For example, a malicious actor may have the goal to reduce access to a census site. The actor may have zero or many dependent tasks and softgoals. For example, the task of hiring a botnet with the softgoal of achieving a quick attack. Similarly, the actor may have zero or many associated resources, e.g., cryptocurrency to hire a botnet. Unlike the tasks and the softgoals, resources are only used by the actor but not dependent on the actor.

6.4.1.2 Variability example

Figure 6.6 illustrates the Context-risk example for Variability. A few options a malicious actor might consider to reduce access to the census site are modelled. By analysing these options, it becomes clear that the DDoS geoblocking mitigation strategy which only considers international traffic was not suitable as the sole mitigation option as attacks could equally have originated from within the country (Australia).

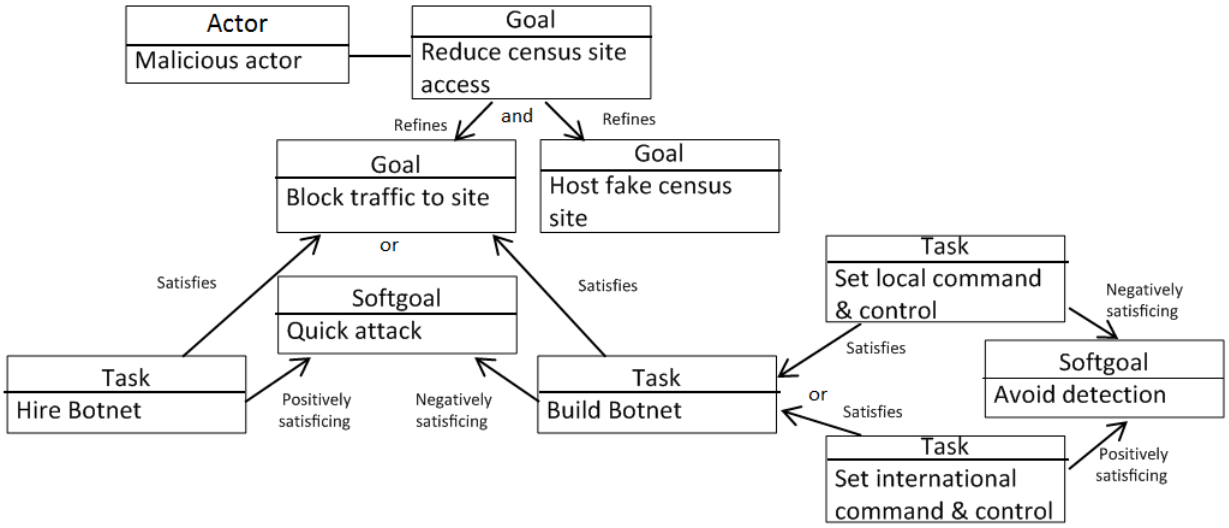


Figure 6.6: Contextual-risk model example (Variability)

6.4.1.3 Correlation

Correlation relates to recognising the disparate pieces of data that may be used collaboratively to achieve greater awareness. The contextual risk lies in the inability to identify or piece useful data. At the lowest level, data is either held by an actor or a resource, e.g., an Excel file as a resource, not the organisation owning the file. Thus, modelling takes the form of data flows between actors and resources. At a minimum, Correlation involves one actor representing the data seeker (decision-maker), while additional actors and resources represent the data sources (see Figure 6.7).

6.4.1.4 Uncertainty

As previously indicated, Correlation relates to uncertainty. In RRP, uncertainty was explained as a composition of factors relating to context (actual not perceived), the environment, information quality, and the persona - who in this case is the information provider (see Section 5.3.3.7). Uncertainty is modelled by appending the uncertainty factors to each identified data source, thereby, hinting on the level of confidence that can be placed

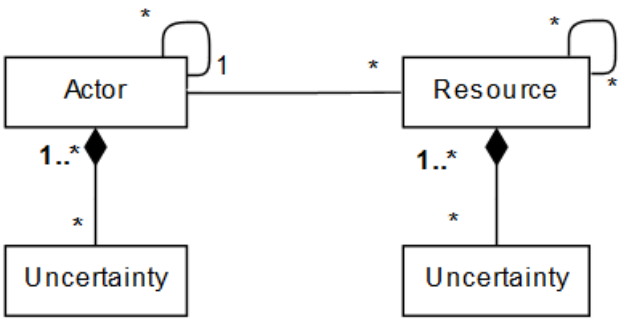


Figure 6.7: Contextual-risk model (Correlation)

on the data and promoting heedful decision making (Cohen and Freeman 1996). For example, uncertainty on the Excel file mentioned above may relate to information quality, e.g., inaccurate or outdated data. There is also the possibility that uncertainty relating to the sourced data is unknown, thus, the zero or many representation for uncertainty in Figure 6.7. As an overall, uncertainty can only be modelled when data sources have been identified.

Note that uncertainty is not modelled with Variability as the process is presumptive. It would, therefore, be difficult to validate the type of uncertainty in question.

6.4.1.5 Correlation and Uncertainty example

Having identified potential alternatives during Variability modelling, decision-makers may use this information to identify suitable sources of information to achieve greater awareness and informed decision making. Continuing with the Census example, possible data sources could be an investigator monitoring attack discussions on the dark web, an analyst monitoring cryptocurrency movement, or traffic pattern logs at the ISP. Once these have been identified, the type of uncertainty for each data source is appended as illustrated in Figure 6.8.

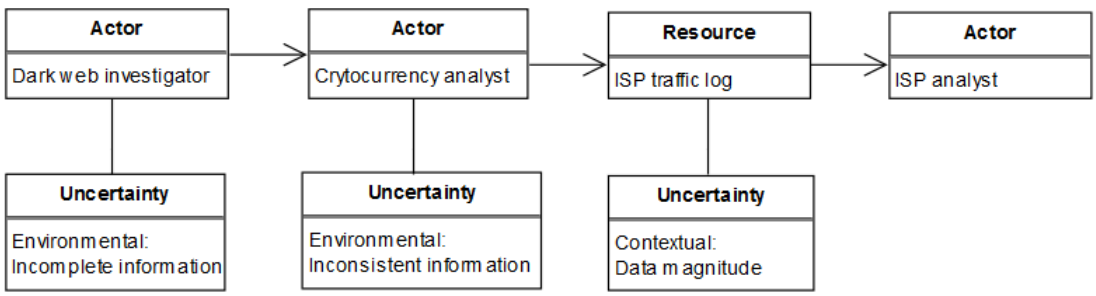


Figure 6.8: Contextual-risk model example (Correlation and Uncertainty)

6.5 Goal-risk model

6.5.1 Defining Goal-risk

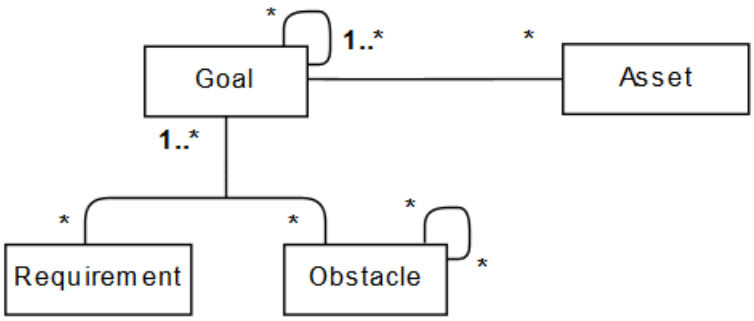


Figure 6.9: Goal-risk model

Illustrated in Figure 6.9, the Goal-risk sub-model dwells on modelling decision risks relating to goals satisfaction (see Section 5.3.3.2). Unlike the actor goals discussed in the contextual-risk sub-model that aim at understanding actor intentions, the goals here are used as an approach for refining requirements (Dardenne et al. 1993) and are specifically the goals of decision-makers and not actors in general.

To satisfy goals, refinement follows one of two approaches. The first approach focuses on refining the goals themselves from a high unachievable level to attainable low-level goals or requirements. The KAOS (Dardenne et al. 1993) definition for requirements is borrowed, which defines requirements as refined goals under the responsibility of a single agent. Agents may be humans, devices, programs, etc. (van Lamsweerde and Letier 2000). For example, the goal of having multiple ISPs as a backup to Internet outages may be satisfied by the requirement to issue contracts to several ISPs - a responsibility assigned to a specific person.

As goals are the main focus, modelling entails a minimum of one goal, refined to zero or many sub-goals and/or requirements.

The second approach focusses on obstacles restricting the satisfaction of goals[1]. Like goals, obstacles are refined to sub-obstacles, which are then addressed by identifying new goals or requirements that prevent the obstacles from occurring. In KAOS, obstacles are defined as undesired conditions that prevent associated goals from being achieved (van Lamsweerde and Letier 2000). For example, the goal of contracting multiple ISPs may be obstructed by budgetary constraints which could then be refined as a budget reallocation requirement.

[1]For examples, see conditions constraining risk decision making in Section 4.2.

Obstacles are modelled with a minimum of one goal, but may be refined to zero or many other obstacles and/or requirements.

As an overall, goals in security decision making are typically associated with assets where the aim is to maintain the asset's security properties. Assets may be associated with one or many goals, but goals may not have a direct association with assets, e.g., sub-goal. Assets are defined as entities of value to an organisation (ISO 2013).

6.5.2 Goal-risk example

The Goal-risk example in Figure 6.10, illustrates how risks relating to IBM's goal of providing sufficient public access to the census site could have been considered. First, the main goal is refined into achievable sub-goals with the hope of determining requirements. Public website access includes determining the possible number of site users per given time and determining the throughput required to serve the users. On the other end, site unavailability is an obstacle to achieving the desired access level. This may be refined as a low throughput obstacle resulting in router failure, or refined as the requirement to contract a secondary ISP that is independent of the first to avoid a single point of failure.

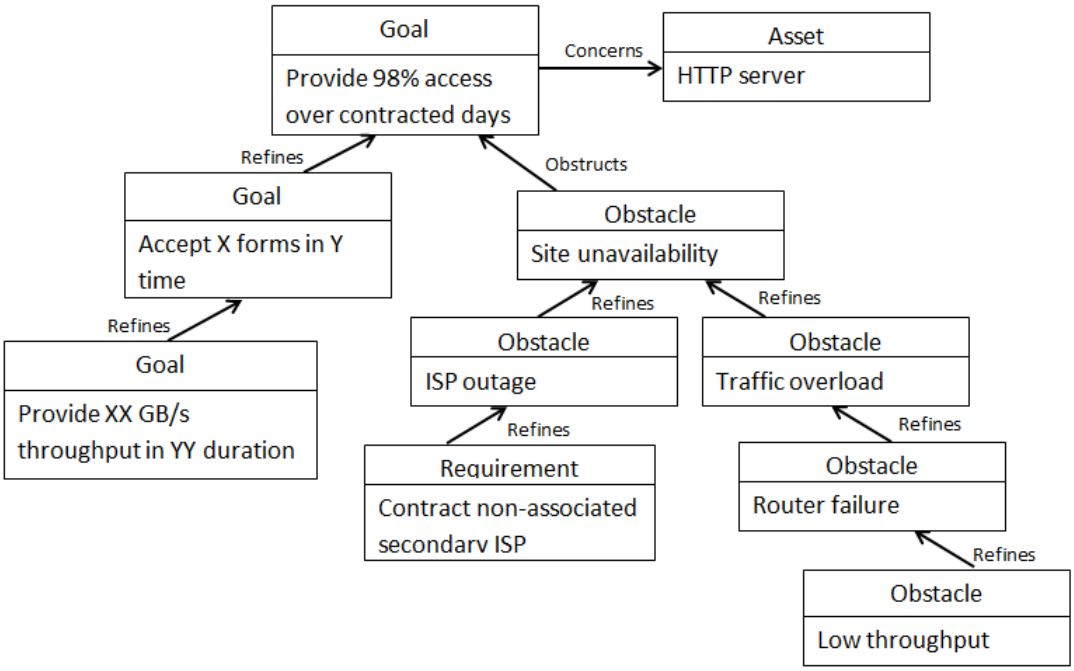


Figure 6.10: Goal-risk model example

6.6 Chapter summary

In this chapter, a conceptual model for designing for RBDM aimed at enhancing designer understanding by highlighting the various concepts in cyber security RBDM was presented. Sub-models relating to risk forms were presented, each with a sample illustration based on a DDoS attack on the Australian Bureau of Statistics.

The conceptual model is a step towards adapting previously identified decision making finding to the design domain, and more generally, it illustrates how RBDM concepts may be reasoned about in design.

In the following chapter, the conceptual model is instantiated by presenting design guidelines, guiding the specification of requirements for systems deployed in cyber security RBDM.

Chapter 7

Conceptual Model Instantiation

7.1 Introduction

This chapter presents design guidelines and suggested implementation techniques, guiding the specification of requirements for systems deployed in cyber security RBDM. The guidelines are a cumulation of work presented in this dissertation and an instantiation of the conceptual model presented in Chapter 6; they aim to facilitate the requirements specification activities between system designers and security analysts as exemplar decision makers addressing situations of risk and uncertainty.

The chapter addresses research aim 3: To propose approaches supporting the specification of design requirements for systems facilitating cyber security risk-based decision making.

The rationale for selecting the guidelines is first presented, before presenting the guidelines and their implementation techniques.

7.2 Rationale for design guidelines

In Section 6.1, it was indicated that the conceptual model comprehensively covers the requirements that should be considered during design for RBDM. This was achieved by grounding the model in risk rationalisation practices in cyber security and RRP. An exception in the conceptual model was the risk of response which was excluded as it is modelled at a high-level modelling. As instantiations of the conceptual model, the guidelines address areas covered by the conceptual model and also take the risk of response into account.

The relationship between the risk of response and other concepts is highlighted in Figure

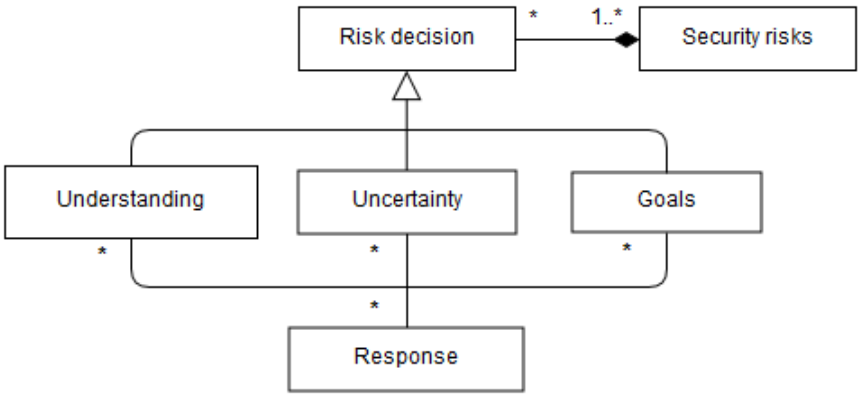


Figure 7.1: High-level RBDM conceptual model

7.1. As seen in Chapter 6, risk decisions are a composition of understanding, uncertainty, goal, and related risks. Response, however, is a product and not a part of the risk decision. Consequently, the risk of response can only be considered after the other risks have been analysed. It is this higher level relationship that made the risk of response ill-suited during the presentation of the conceptual model in Chapter 6. The risk of response is defined as the risk resulting from the implications of a selected risk response (course of action). During decision making, multiple courses of action could be considered, where selection is based on risks and expected outcomes (see Section 5.3.3.6).

The next point considered to derive a comprehensive set of guidelines was that risk is not only in the decisions made, but that the decisions are in response to one or many risks in a domain. In cyber security, the domain-risk is the security-risk (threat, vulnerability, and likelihood). While the ”security-risk” is acknowledged as a way of characterising the domain, it is not include in the guidelines as this would be moving towards the formulation of guidelines for risk and threat assessment e.g., AEGIS (Appropriate and effective Guidance for Information Security) (Flechais 2005). In other words, the objective of the research is to facilitate the identification of requirements for cyber security RBDM, which differs from the identification of approaches that facilitate the elicitation of security requirements.

Based on this understanding, the guidelines are drawn from the four risk forms in RBDM. Illustrated in Figure 7.2, the risk of understanding is further refined to sub-areas drawing on knowledge from the conceptual model in Chapter 6. Consequently, the guidelines are based on the risk forms and the sub-areas. These total six guidelines (G1-6), aimed at comprehensively supporting the specification of requirements for RBDM. The guidelines are presented in detail below.

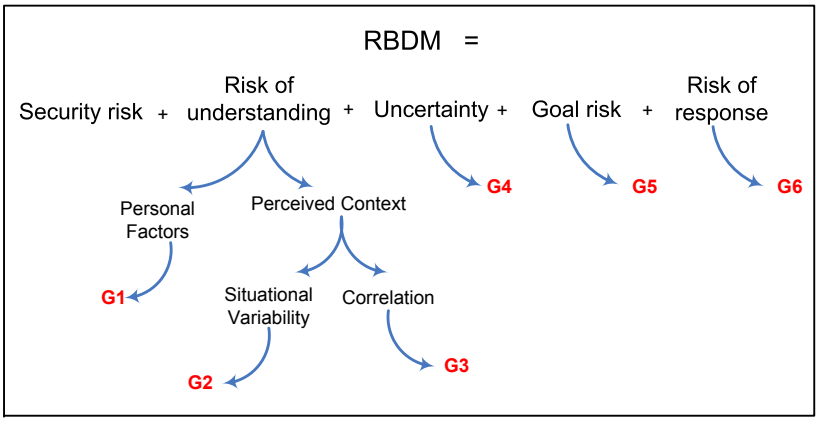


Figure 7.2: Deriving the design guidelines

7.3 Design guidelines

Design Guidelines	Suggested Implementation Techniques
1. Behavioural Characterisation	Personas
2. Dynamic Contextualisation	Agent oriented Goal modelling
3. Distributed Rationalisation	Distributed Cognition Models
4. Uncertainty Characterisation	Distributed Cognition Models
5. Goal Facilitation	Goal and obstacle modelling
6. Requirements Validation	Integrated validation of specified requirements

Table 7.1: Design guidelines

Table 7.1 presents an overview of the design guidelines and suggested implementation techniques. While the guidelines specify the concepts to be considered when specifying requirements, the implementation techniques guide the modelling of the concepts through the use of techniques from design and decision-making research. The term “suggested” is used for the implementation techniques to indicate that applicable techniques are not limited to the proposed.

A strict order for applying the guidelines is not specified, other than the requirement that Guideline 4 (Uncertainty Characterisation) follows from Guideline 3 (Distributed Rationalisation) due to the way the are modelled. However, it is believed that following the numbering would prove helpful.

The significance of each guideline is presented including possible consequences of non-conformity. The supporting implementation techniques are then explained providing the

rationale for use and variations to implementation where applicable.

7.3.1 Guideline 1: Behavioural characterisation

7.3.1.1 Guideline

The behavioural characteristics of risk decision-makers must be understood in order to identify decision delimiting personal factors, where delimiters are those that directly or indirectly affect the decisions in question.

This guideline instantiates the Personal-risk model (Section 6.3) and its significance lies in its focus on understanding the cognitive requirements of users in systems where humans are the final decision makers (Roth et al. 2001). Consequences of nonconforming to the guideline may include the failure in identifying required training and experience levels, or the inability to address the effects of cognitive limitations held by the decision-makers (Kahneman 2002 2011).

7.3.1.2 Implementation technique

The guideline is implemented using personas which were introduced in Section 2.4.2.2. Personas are descriptive models of users (Cooper et al. 2014) selected for their ability to represent archetypical user behaviour. The technique avoids the modelling of stereotypical decision-makers that would be difficult to represent in large groups, but focusses on representing the essential characteristics of selected groups. For example, analysts in a large organisation might have a variety of training requirements, however, modelling the analysts by roles, e.g., intelligence gathering or threat analysis would produce a manageable set of behaviour variables from which personas are constructed and behavioural requirements elicited.

Uncovering cognitive constructs such as mental models and biases requires the use of cognitive elicitation technique when eliciting persona characteristics. Based on the circumstance, either contrived (controlled environment) or naturalistic (natural environment) knowledge elicitation techniques could be used each presenting advantages and disadvantages (Shadbolt and Smart 2015, McGeorge and Rugg 1992). For examples, contrived methods such as card sorting may be limited by their designer's imagination. On the other hand, naturalistic elicitation methods such as shadowing (observation) or CDM (Klein et al. 1989) discussed in Section 2.4.1 do not have this limitation, however, there is an information sensitivity risk as data collected is not hypothetical and participants may have limited recollection when using CDM.

Given the limitations, the essence is using cognitive elicitation technique suitable for the situation in question. Identifying behaviour variables recommended by Cooper et al. (2014) (activities, attitudes, aptitudes, motivations, and skills) should also prove useful when eliciting cognitive constructs.

7.3.2 Guideline 2: Dynamic contextualisation

7.3.2.1 Guideline

Design activities should aim at contextualising the dynamism of a situation in order to identify situational variations that influence the formulation or direction of decisions. The guideline instantiates the Contextual-risk model on Variability which details the contextualisation of dynamic situations (Section 6.4.1.1).

The significance of this guideline lies in recognising that risk may be reduced where risky situations are anticipated and prepared for (Endsley 1995, Franke and Brynielsson 2014). Nonconforming to the guideline would likely result in an inability to anticipate situational alternatives and the impact they may have on the selection or direction of a course of action.

7.3.2.2 Implementation technique

As indicated during Variability modelling (Section 6.4.1.1), dynamic contexts can be modelled using actors, goals, resources, softgoals, and tasks. Implementing the guideline may be through the use of narrative scenarios (introduced in Section 2.4.2.1) or agent-oriented goal modelling techniques (introduced in Section 2.4.2.3). Scenarios are easily understood as they are presented in natural language but can be verbose when documenting multiple contextual variations. On the other hand, agent-oriented goal modelling techniques require a level of expertise for the model to be understood, but a wider range of contextual variations may be represented easily. Applicable agent-oriented goal modelling techniques include the i* framework (University of Toronto 2011, Yu 1997) and its derivatives such as Tropos (Fuxman et al. 2000) and GRL (Goal-oriented Requirement Language) (University of Toronto 2000).

7.3.3 Guideline 3: Distributed rationalisation

7.3.3.1 Guideline

As risk decision making is information-driven, design activities should aim at identifying information sources that reduce levels of risk and uncertainty. To achieve this, the information sourced from dynamic contextualisation above, may serve one of two purposes.

First to clarify the risky situation, and second, to aid the decision makers selection of a course of action. This refers to the difference between understanding a situation versus understanding how to address it.

The guideline instantiates the Contextual-risk model on Correlation (Section 6.4.1.3). The significance of the guideline lies in recognising the value of information as a tool for rationalising risk (Groenewald et al. 2017, Gutzwiller et al. 2016, D'Amico et al. 2005, Fisher and Kingma 2001). Consequences of non-conformity include the failure to adequately characterise risky situations and an inability to identify appropriate courses of action.

7.3.3.2 Implementation technique

For implementation, the requirement is to map out information distribution and collaboration, where actors and resources are used as representative artefacts (discussed in Section 6.4.1.3). To this end, the proposal is to use adaptations of DiCoT for implementation (introduced in Section 2.3.5.1) (Blandford and Furniss 2005). Based on the theory of Distributed Cognition (Hollan et al. 2000), DiCoT provides representational models for analysing information flows among actors in a system among other things. For compatibility, DiCoT is adapted by adding resource representations to its information flows. Other useful representations from DiCoT's information flow model include the representation of information channels and decision hubs, which in this case are the decision makers.

7.3.4 Guideline 4: Uncertainty characterisation

7.3.4.1 Guideline

For every risky situation identified, design activities should aim at identifying the level of confidence that may be placed on information sources by characterising the nature of uncertainty.

This guideline instantiates the Contextual-risk model on Uncertainty which details uncertainty characterisation (Section 6.4.1.4). The guideline is significant to risk decision making as it enforces the understanding that risk and uncertainty are separate but crucial entities that should equally be considered during design for RBDM. Overlooking the guideline could result in an inability to determine the limitations of sourced information (Toma et al. 2012, Cohen and Freeman 1996).

7.3.4.2 Implementation technique

As discussed in Section 6.4.1.4, uncertainty first requires the modelling of information sources (Guideline 3). Based on this, the approach is implemented by appending uncer-

tainty information tags to DiCoT information flow models.

7.3.5 Guideline 5: Goal facilitation

7.3.5.1 Guideline

Design activities should aim at verifying the feasibility of decision-makers goals and the facilitation of their achievement. The guideline involves considering the obstacles to goal achievement and the refinement of high-level goals. Goal formation varies based on context (Guideline 2); capturing a wide range of likely goals is, therefore, necessary to ensure systems supporting RBDM are fit for purpose overall anticipated situations.

The guideline instantiates the Goal-risk model (Section 6.5) and is significant to risk decision making as decisions are enactments of goals, thus goal correctness and feasibility is critical for outcome (see Section 4.3). Consequences of non-observance include an inability in capturing appropriate goals and in identifying goal impeding conflicts and obstacles.

7.3.5.2 Implementation technique

For implementation, KAOS goal modelling is recommended (Dardenne et al. 1993). Introduced in Section 2.4.2.3, KAOS is a method where goals are desired system properties and unlike the agent-oriented goal modelling approaches recommended for Guideline 3, KAOS focuses on modelling system goals rather than user intent (social goals), where a system is not limited to software but can be extended to the environment; e.g., an organisational system.

Conversely, the goals modelled in this research are decision-makers goals and not system goals. It would, therefore, seem reasonable to implement these using the agent-oriented goal modelling techniques (i* and derivates), however, using KAOS is recommended, first because it satisfies the required modelling concepts proposed in the Goal-risk model (Section 6.5) (assets, requirements and obstacles). Secondly, while agent-oriented goal modelling techniques support the refinement of goals, they do not support the refinement of obstacles. This is supported by KAOS (van Lamsweerde and Letier 2000) and it is one of the modelling requirements specified for goals in Section 6.5.

7.3.6 Guideline 6: Requirements validation

7.3.6.1 Guideline

Implementation of the guidelines should ideally produce a set of requirements. As the requirements are the product of different techniques and analyses, validating consistency and compatibility across the specified requirements is recommended (Pohl 1994, Pohl and Rupp 2015).

This guideline is an instantiation of the risk of response. Indicated in Section 7.2 above, the risk of response is risk resulting from the implications of selected response options and is considered after other risks have been analysed. For design, this equals identifying the effectiveness of the specified requirements to decision facilitation as their implication on actual decisions can only be determined after implementation.

Implications of nonconformity include an inability in understanding the effectiveness or ineffectiveness of specified requirements in facilitating decision making.

7.3.6.2 Implementation technique

Unlike the previous guideline, requirements validation does not require modelling techniques for implementation but an adherence to known requirements validation techniques. For example, Pohl and Rupp (2015) propose the following six requirements validation principles which help ensure the specification of correct requirements.

- Involvement of the correct stakeholders
  The identification and selection of correct stakeholders for requirements audit.
- Separating the identification and the correction of errors
  The separation of error identification and error fixing tasks.
- Validation from different views
  Validating requirements from multiple perspectives.
- Adequate change of documentation type
  The use of different document types such as natural language or models to improve requirement understandability and expressiveness.
- Construction of development artefacts
  The development of artefacts to test requirements e.g., test cases.
- Repeated validation
  Validating throughout the design process.

Designers can therefore consider adopting these principles or other suitable requirements validation approaches during the implementation of the guideline.

7.4 Chapter summary

In this Chapter, the conceptual model presented in Chapter 6 was instantiated by presenting guidelines and suggested implementation techniques guiding the specification of requirements for systems deployed in cyber security RBDM. The selection and completeness of the proposed guidelines was argued, and in turn, the difference between decision risks and security risks were illustrated. Theoretically, this implies that the guidelines should be applicable to RBDM domains outside cyber security.

While the proposed implementation techniques are in themselves not new, the guidelines' contribution to knowledge is an illustration of the adoption and adaptation of existing design and decision making techniques to facilitate the specification of requirements for systems deployed in cyber security RBDM. By doing this, the presented work addresses the research question motivating the thesis: What system design techniques should be taken into consideration to facilitate cyber security decision making during situations of risk and uncertainty?

In the following chapter, the guidelines are validated through application to a real-world case study where RBDM requirements were elicited to inform the design of a secure data handling policy.

Chapter 8

Case Study: Informing the Design of a Secure Data Handling Policy

8.1 Introduction

This chapter reports on the results of a validation case study where the design guidelines for systems deployed in cyber security RBDM were applied to inform an approach used to specify the requirements of a secure data handling policy for a charity supporting traumatised parents. The case study was conducted following the Acton Research methodology which validated the guidelines' effectiveness in informing the study approachand the study approach effectiveness in facilitating the design of an intervention in the research environment.

Summative validation is conducted to ensure that the overall output of a research project meets requirements. For this project, the requirement was to validate that the proposed guidelines would adequately facilitate the elicitation of design requirements for RBDM. Several validation approaches were considered which included studies with security analysts making decisions in the financial sector, studies with security analysts making decision in the increasingly popular use of drones in medical care (Kim et al. 2017), and the application of the guidelines to inform the requirements of a security-by-design tool (Faily 2019b). Based on participant and information availability, the researcher opted to conduct the validation work with a psychotherapy charity that was aiming to ensure the secure handling of their client files. The anonymised name Samaritan shall be used in reference to the charity.

The chapter introduces the research environment and problems motivating Samaritan's need for change, before detailing an action plan and its implementation where an intervention was designed following an Action Research approach. The chapter concludes by

validating the intervention and the research approach, before presenting lessons learnt.

8.2 Description of study

Samaritan's main role was to provide non-paying counselling services to psychologically traumatised parents of abused children. The charity stored, processed, and disseminated client data during consultation service, and for police and local council reporting requirements. The data included the clients' personal identifiable details, medical history, history of abuse, and legal history.

Samaritan's counselling services involved a team of supervisors (experienced counsellors), of which their manager was one, and a team of supporting counsellors (lesser-experienced). In addition to them, Samaritan had recently contracted two IT analysts responsible for overseeing all IT issues including security. The IT analysts were privy to client data.

8.3 Diagnosis

To understand the circumstances promoting Samaritan's desire for change, two initial meetings were set, each lasting approximately one hour and audio recorded. The first was at Bournemouth University between the researcher and Samaritan's manager - who presented an overview of the charity's operations and problems. The second was at the charity with the manager and a supervisor; here the researcher had the opportunity to appreciate the work environment, discuss the problems facing the charity and establish an action plan.

Based on the meetings, the following concerns were uncovered.

8.3.1 Automation of processes

As a relatively newly founded charity, Samaritan was at a stage where their business processes and the handling of data were mostly manual. While this had not been a problem in the first few years, a steady increase in clients meant several processes required full or increased automation to improve efficiency. For example, Samaritan had registered 55 new families over the 2018/19 period and was expecting higher annual increases. Processes under consideration included data storage, processing, and dissemination.

8.3.2 Part-time Counsellors

As a charity that provides free consultations, Samaritan depended on donations for the running of its services. Samaritan therefore aimed at keeping its running costs at a minimum where all counsellors worked on a voluntary and temporary basis, with the freedom to work for other charities and organisations. The temporal nature of the counsellors' work made it difficult to ensure they understood Samaritan's secure data handling expectations. A couple of policies around risk were in place, however, none with a focus on secure data handling.

8.3.3 IT staff

While IT/security staff typically take a lead in the design, development, and implementation of security artefacts e.g., security policies. Samaritan's two IT analysts were both relatively new and were also on a part-time basis. Consequently, they did not have the knowledge of Samaritan's data handling activities to enforce rules, nor did they have time to comprehensively study organisational activities and decision making processes to establish secure data handling procedures.

8.3.4 GDPR concerns

At the time of the study, it had been a little over a year since the enforcement of the General Data Protection Regulation GDPR, the then-new European framework for data protection laws. Samaritan had not tested for GDPR compliance, however, they recognised that a secure data handling process was a step towards it. Security enforcement falls in line with GDPR's 6th principle where it is recommended that process should be in place for ensuring data integrity and confidentiality. While GDPR states the requirements, it is up to an organisation to identify implementation techniques such as following ISO 27001 that proves a level of commitment to cyber security.

8.4 Action planning

Based on the concerns identified during diagnosis, the researcher proposed the design of a secure data handling policy that would act as a reference point for addressing the concerns. A RBDM design approach was deemed useful as the issues in the study environment were not only limited to security, but the need to understand decision making strategies and its facilitation were also identified. For example, what information sources were the counsellors using in their decision making about clients, how could the information affect their perception of the clients and consequently affect the treatment of data?

Following this, the policy was going to focus on data security and also consider decision making requirements such as the desired characteristics of a decision-maker. The researcher was to take the lead eliciting requirements for the design of the secure data handling policy with the following considerations.

8.4.1 Scope

To identify areas of risk in client data handling, it was agreed that the study would focus on counselling decision making and work processes. Findings thereof would inform requirements for the design of a secure data handling policy aiding the counsellors and facilitating IT security expectations.

In addition to the clients' data, Samaritan also held data on the charity's staff and trustees. These were agreed to be out of scope.

8.4.2 Data collection

8.4.2.1 Interviews

To ensure a free presentation of work practices and decision making, it was agreed that data would be collected using one to one interviews. Two supervisors, two counsellors and one IT analyst were selected by the manager for the interviews. The different roles aided the elicitation of requirements from multiple perspectives (Pohl and Rupp 2015).

Interviews were to be conducted over a two week period with details illustrated in Table 8.1. The manager's availability was assured during the interview days or via email throughout the course of the study.

Date	Location	Interviewee	Duration
13/06/19	Samaritan's Office	Supervisor	Approximately 1 hour
18/06/19	Samaritan's Office	Supervisor	Approximately 30 minutes
18/06/19	Samaritan's Office	Counsellor	Approximately 1 hour
19/06/19	Samaritan's Office	IT analyst	Approximately 30 minutes
20/06/19	Samaritan's Office	Counsellor	Approximately 30 minutes

Table 8.1: Data elicitation interview schedule

8.4.2.2 Interviews procedure

Based on the two initial interviews, it was identified that eliciting relevant work process data that was capable of revealing risk decision making strategies was going to be a challenge. This was because the primary risk based decision-makers were the counsellors and not the IT staff accustomed to expressing risk from a security perspective. The counsellors' idea of risk mainly related to client well-being.

To address the problem, inspiration was dawn from an approach used to analyse the efficiency of algorithms by testing their performance on best, average, and worst cases (Heineman et al. 2016, p. 14). The approach yields possible risks and uncertainties to algorithm performance under presented conditions. Similarly, the counsellors could be asked to detail probable best, optimal, and worst (BOW) cases on issues relating to client data handling and decision making; thereby, revealing data handling risks and uncertainties in their work practices.

Interviews therefore aimed at understanding BOW cases on the security (confidentiality, integrity, availability) of client data during access, storage, processing, and dissemination activities, and on the availability of information facilitating decision making on client data.

With consent received, audio recordings were to be made in all interviews.

8.4.2.3 Available resources

In addition to the interviews, documents used during the work processes and policies guiding staff conduct were to be made available to the researcher. For confidentiality, blank documents or templates were to be provided where applicable. Below is a list of the policies relating to the counselling services that were made available.

- Confidentiality policy
  Describing organisation confidentially expectations and practices during Samaritan's service delivery (directed at clients and employees).
- Privacy policy
  Describing the use of personal data (directed at clients and donors).
- Risk Assessment register
  Used to register organisation-wide risks and response actions (directed at employees).
- Lone working policy
  Describing general risk considerations for employees working alone and without

close or direct supervision (directed at employees).

- Counselling policy
  Describing general expectations relating to ethics, trust and confidentiality during counselling services (directed at employees).

- Safeguarding policy
  Describing the procedures for addressing signs of possible child abuse (directed at employees).

8.4.3 Data analysis - applying RBDM design guidelines

Having set the interviews, the application of the design guidelines was planned to follow a series of phases as illustrated in Table 8.2. For each phase, the table presents the activity carried out and the technique used, it presents input data sources and expected outputs, and lastly, it presents the tools used in support of the phase and guideline.

Functionality offered by the tools used is as follows; NVivo: for qualitative data analysis (Hutchison et al. 2010). Microsoft Visio: for diagram design. jUCMNav: a graphical editor for modelling, analysis and transformations with the user requirements notations (Amyot 2017). CAIRIS: an open-source platform for building security and usability into software that supports various usability, security, and Requirements Engineering techniques (Faily 2018 2019a).

Phase	Activity	Technique	Input	Output	Tool Support
1	Interviews analysis	Thematic analysis	BOW cases interviews	Thematic categories	NVivo
2	Behavioural characterisation	Persona	Phase 1 output	Behavioural considerations	NVivo & CAIRIS
3	Dynamic contextualisation	GRL	Phase 1 output	Dynamic considerations	jUCMNav
4	Distributed rationalisation	DiCoT	Phase 1 output & sourced documents	Correlation considerations	Microsoft Visio
5	Uncertainty characterisation	DiCoT	Phase 1 & 4 output	Uncertainty verification	Microsoft Visio
6	Goal facilitation	KAOS	Phase 1 & 4 output	Goal satisfaction considerations	CAIRIS
1-6	Requirements validation	Varying	Phase 1-6	Validated requirements	N/A

Table 8.2: Application of design guidelines

Phases

- Phase 1: Interview analysis
  An initial interview analysis phase was incorporated to the guideline to serve as a source of refined data for the guidelines. Interview data was to be analysed thematically and coded with the guideline titles denoting categories. For example, codes relating to obstacles and conflicts in decision goals would be codded under the goal facilitation guideline.

- Phase 2: Behaviour characterisation
  The second phase involves identifying required characteristics the counsellor should possess as risk-based decision makers in the study environment. From the interview data, persona(s) would be developed to capture the required decision making characteristics specified by the guideline as minimum training, experience, and behaviour traits. Modelling would follow the behaviour variables recommended by Cooper et al. (2014) (see Section 7.3.1).

- Phase 3: Dynamic contextualisation
  Using interview data, situational variations that could result in risk were to be considered in the third phase, where mitigations to risks would inform secure data handling policy statements. However, the dynamic contextualisation guideline does not specify what the situational variants could be as they are determined by the study environment (see Section 7.3.2). As the focus is on data handling procedures, variants could relate to data access, processing, storage, and dissemination. For each variant, the guideline recommends considering the actors, their goals, their softgoals, tasks and resources.

- Phase 4 & 5: Distributed rationalisation and Uncertainty characterisation.
  As the uncertainty characterisation guideline (see Section 7.3.4) is dependent on the distributed rationalisation guideline (see Section 7.3.3), the fourth and fifth phases were implemented simultaneously. The phase would involve using both interview data and documents provided by the charity to identify information sources facilitating decision making; results of which would inform, information sourcing policy requirements. The distributed rationalisation guideline states that information sources shall be in the form of actors and resources. The level of confidence that may be placed on every information source identified would then be determined by enquiry during the interviews or through document reviews. As a generic modelling tool, Microsoft Visio was selected for the two phases as the technique used is mostly developed by the researcher and not supporting by specific tools.

- Phase 6: Goal facilitation
  For the sixth phase, conflicts and obstacles in the counsellors' decisions and activities were to be considered; mitigations of which would inform policy statements. Conflicts and obstacles under consideration would be those limiting decision making, thus input would be decision facilitators identified in phase four and the interview data.

- Requirements validation
  The final phase is an ongoing requirements validation from the first to last phase.

8.4.4 Output and Validation

Samaritan's manager was informed that the design process would first require the modelling of design artefacts before requirements could be specified. It was agreed that these and any concerns would be discussed via email as the study progressed.

One validation meeting was agreed upon at study completion. Validation was going to consider:

- The necessity of policy statements
- Omitted policy statements
- Validity of the risks addressed in the policy statements
- Clarity of policy statements
- Repetitions in the statements
- Repetitions relating to other Samaritan policies

8.5 Action taking

8.5.1 Thematic categorisation

Category	Subcategory	Interview Sources	Codes
Behavioural characterisation	Activities	4	15
	Attitudes	4	21
	Skills	3	16
	Motivations	2	6
	Aptitude	3	3
Dynamic contextualisation	Storage	3	20
	Dissemination	3	15
	Access	4	6
	Processing	0	0
Distributed rationalisation	Artefacts	2	4
	Actors	4	9
Goal facilitation	Obstacles	0	0
	Conflicts	0	0

Table 8.3: Thematic analysis of interview data

After receiving approval for audio recordings, each interview was recorded and transcribed. Thematic analysis (Saldana 2015) was then conducted on the interview data using Nvivo. Coding was only conducted on the four interviews with the counsellors and supervisors. The interview with the IT analyst was omitted as they had limited knowledge

of the organisation and their interview had only focussed on their expectations. Coding was to the four predefined categories representing the design guidelines illustrated in Table 8.3.

The approach was beneficial as it meant analysis work during the application of each guideline would solely focus on relevant coded data as opposed to the entire corpus. This, in turn, speeded data analysis.

As a result of the thematic analysis, two observations were made. First, it was identified that there were no data processing risks as codes did not emerge relating to this. This was an accurate representation of operations at Samaritan, as the only data processed was numerical for council reporting purposes.

Second, there were no codes for Goal facilitation. Analysis of the data did not produce substantial conflicts or obstacles relating to data handling - which are the two codes under goal facilitation. Further details on the finding are provided in Section 8.5.5 below.

8.5.2 Behavioural characterisation

The behavioural characterisation guideline was applied to identify characteristics required for counsellors to ably make secure data handling decisions.

Using the thematically analysed interview data as an input (Activities, Attitudes, Skills, Motivations, and Aptitude), a persona - Mary Hughes was modelled in CAIRIS representing an archetypical counsellor with the desired training and cognitive disposition.

The initial plan was to model two personas; one representing a supervisor and the other a councillor, however, experience was the only clear difference between the two, making a second persona unnecessary.

Modelling the persona and deriving policy requirements was based on desired behaviour attributes or the mitigation of undesired attributes.

For example, an interviewee said *"As therapists, we are members of the BACP, I go there to see a lot on ethics"*. This represents a desired behaviour attribute and was coded as a skill (skills improved by membership). The attribute informed the requirement for professionalism and the following policy statement was specified: *Counsellors shall be registered with the British Association for Counselling and Psychotherapy (BACP) or sim-*

ilar professional bodies.

An example of an undesired behaviour attribute may be seen in the following interview quote: *"Our relationship is based on trust, if I go snooping around on social media, it would affect my judgment with my clients"*. This was coded as an attitude. The attribute informed the requirement for trust and is reflected in the following specified policy statement: *Seeking and sharing information from, or with sources such as social media is strictly prohibited*.

Figure 8.1 is an illustrative example of Mary as modelled in CAIRIS. A complete persona description is found under Appendix .2.1.

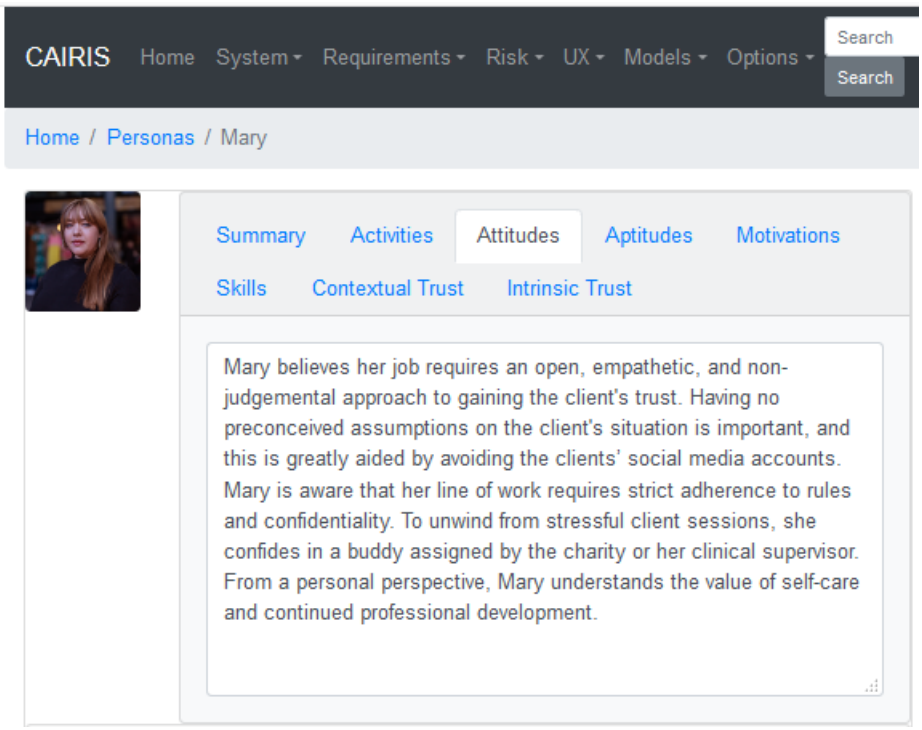


Figure 8.1: Persona - Counsellor

Findings from behavioural characterisation guideline contributed to Section - 2 'Counsellors' of the policy. See Appendix .2.2.

8.5.3 Dynamic contextualisation

The dynamic contextualisation guideline was applied to identify situational variations that could cause risks in the counsellors' data handling decisions and activities.

The thematically analysed interview data used for this guideline was coded in accor-

dance with data handling activities (storage, dissemination, and access) to capture the dynamism of the environment. As indicated in Section 8.5.1, there were no codes for data processing due to the nature of the charity's operations.

8.5.3.1 Resources

To apply the guideline, resources Samaritan used to store data for the provision of counselling services were first identified. These were paper-based files and folder, mobile phones, computers, electronic backup devices, and filing cabinets. The following interview quotes are examples of where resources were elicited:

"Her laptop has the Excel form and a Word document that helps her track the active files."

"Sometimes people send a long text back, saying these things have happened but there are no names, just the first name and ID number."

As vital parts of Samaritan's data handling activities, the requirement to protect the resources was identified. In essence, the resources are assets, as they are entities of value to the charity. Findings informed Section - 1 of the policy on securing assets (see Appendix .2.2).

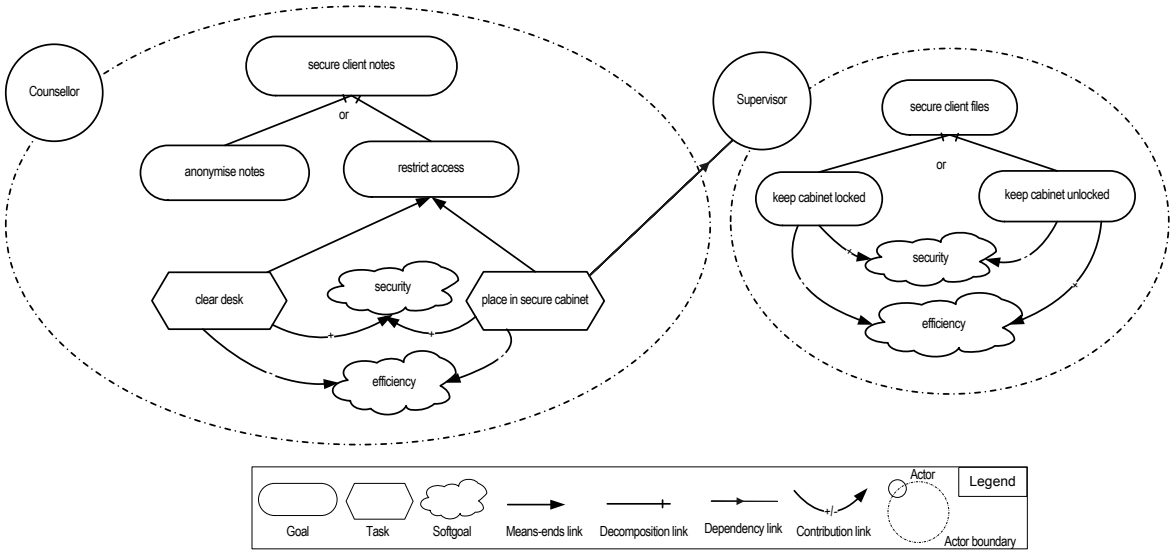


Figure 8.2: Contextualising client data handling

8.5.3.2 Contextualisation

After resource identification, GRL (introduced in Section 7.3.2.2) supported by jUCMNav was used to model alternative data handling situations. Based on the analysis of activities from the interviews, three contextual models were designed; the first for storage and access of paper-based files, the second for storage and access of electronic files, and the third for data dissemination.

Figure 8.2 is the secure storage model for paper-based files. It indicates that the counsellors could either anonymise notes or restrict their access. By restricting access, the counsellor would have to clear their desk and ensure the notes were placed in a secure cabinet. However, the security actions reduce the counsellor's efficiency and could easily be ignored. In addition, the counsellor had to wait for the supervisor to unlock the cabinet increasing the reasons for circumventing security procedures.

Requirements were specified based on desired events in the model or as mitigations to risks identified. For example, the model in 8.2 indicates the need for a clean desk policy statement and highlights the risk of non-conformity to security procedures resulting from reduced work efficiency.

The main risks identified in the contextual models are summarised in Table 8.4.

Findings from implementing the dynamic contextualisation guideline contributed to Sections 4, 5, and 6 of the policy. See Appendix .2.2.

Process	Risk
Data storage	Paper-based file
Data storage	Backup devices
Data storage	Mobile phones in office & transit
Data access	Unlocked filing cabinets
Data access	Unlocked offices
Data access	Weak access protection on computers
Data access	Confidential messages in phones
Data access	Dated physical of logical dates
Data access	Exposed confidential client notes
Data access	Data lost due to single point of failure
Data dissemination	Data provided to unauthorised entities

Table 8.4: Dynamic contextualisation risk summary

8.5.4 Distributed rationalisation and Uncertainty characterisation

The distributed rationalisation and the uncertainty characterisation guidelines were applied to the study to serve three purposes. First, to identify information sources facilitating the counsellors' decision making; second, to verify the level of confidence that could be placed on the information sources; and third, to identify the authorised personnel and entities confidential client data could be shared with.

Based on the output of the thematically analysed interviews, two sources of information facilitating the counsellors' decision making were identified.

The first were policies and guidelines internally or externally sourced. Samaritan's policies and guidelines relevant for secure data handling are listed in Section 8.4.2.3. Externally sourced guidelines include those from the British Association for Counselling and Psychotherapy, and similar professional bodies.

The second source of information facilitating the counsellors' decision making consisted of various personnel. These included the supervisors, buddies; who were experienced colleagues assigned by Samaritan to provide advice and emotional support to fellow counsellors, and clinical supervisors. Each counsellor was paired with a clinical supervisor for guidance and they were experienced external psychotherapist trained at level 6.

The counsellors could seek guidance from the three, but the sharing of personal identifiable information was restricted to the supervisors and buddies.

Policies presented by Samaritan were reviewed for reliability and it was identified that the Privacy policy contained inconsistencies on client and donor instructions which could affect the counsellors provision of guidance. The findings were reported and accepted by the stakeholders in the final validation meeting.

Using adaptations of DiCoT, the distribution of decision facilitating information for the counsellor was modelled, highlighting authorised information flows, actors, resources, and identified uncertainty (see Figure 8.3). A second model was also produced for the supervisors as they shared information with additional entities such as the police. Table 8.5 presents a summary of the distributed rationalisation elements identified.

Based on the analysis, a requirement to highlight authorised sources and recipients of information was identified. Resultant were policy statements contributing to Section - 3 of the policy, on information sourcing and sharing. See Appendix .2.2.

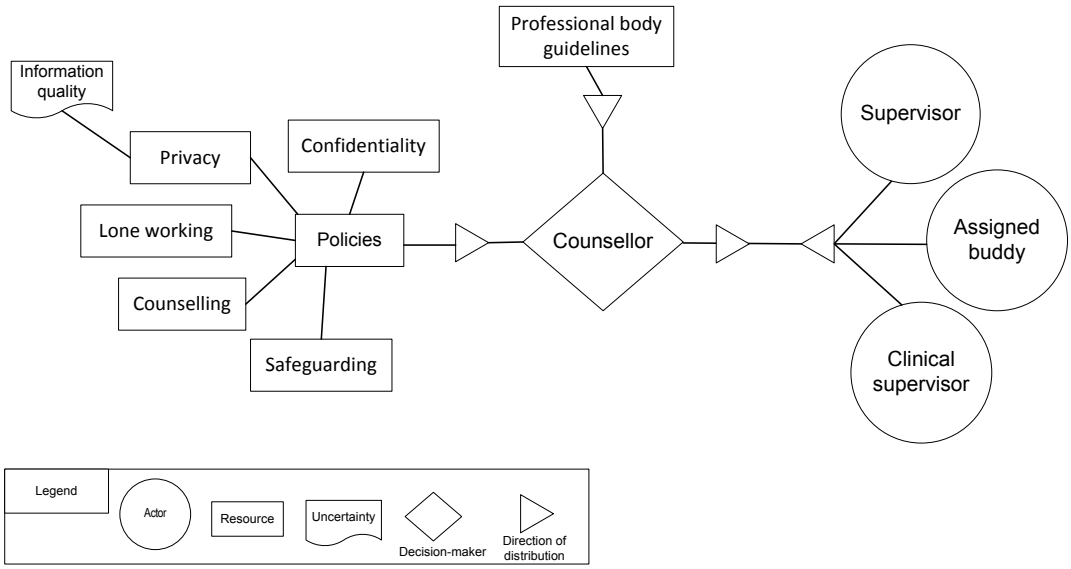


Figure 8.3: Distribution of decision facilitating information

Element types	Elements
Decision makers	Counsellor
	Supervisor
Actors	Assigned buddy
	Supervisor
	Clinical supervisor
	Manager
	Police
	Multi-Agency Safeguarding Hub
Resources	Samaritan policies and guidelines
	Professional body guidelines

Table 8.5: Distributed rationalisation elements summary

8.5.5 Goal facilitation

Application of the goal facilitation guideline aimed at identifying obstacles and conflicts preventing the counsellors from handling client data securely.

As alluded to in Section 8.5.1, substantial obstacles or conflicts to secure data handling decisions were not identified during the interviews or thematic analysis. The few that were found were the negation of situations by the researcher while testing various possibilities using BOW cases.

For example, it was inquired on what would happen if a buddy or supervisor were unavail-

able to offer advice during uncertain situations. For the most part, the obstacle situations were unlikely due to the fact that most data-related decisions at Samaritan were not time-bound and could simply be resolved by waiting. Evidence in the exchange below.

Researcher: *Assuming the supervisors were not around, what would you do?*
Counsellor: *I would telephone my clinical supervisor.*
Researcher: *What if the clinical supervisor is not picking up?*
Counsellor: *I would leave her a message.*

Using KAOS and CAIRIS as a supporting tool, hypothetical obstacle and conflict situations were modelled to analyse situations like the exchange between the researcher and counsellor above. A sample is illustrated in Figure 8.4. Substantial findings did not emerge from the analysis, therefore policy requirements were not drawn from the goal facilitation phase.

8.5.6 Requirements validation

The final design guideline for RBDM relates to requirements validation. In Section 7.3.6 it was stated that this involves identifying the effectiveness of the specified requirements. Similarly, Action Research recommends an evaluation phase that includes determining whether the theoretical effects of the action were realised. As the two achieve the same purpose, the following evaluation section accounts for both.

8.6 Evaluation

This section is divided into two parts. The first part (Section 8.6.1), validates the intervention to prove the effectiveness of the study approach; this includes validating the policy and identifying contributions made to the charity. The second part (Section 8.6.2), validates the study approach to prove the effectiveness of the guidelines.

8.6.1 Validation of intervention

This section validates the intervention to prove the effectiveness of the study approach.

8.6.1.1 Validation

A validation meeting was held for 2 hours on 24 July 2019 at Samaritan's office with the manager and one supervisor. Validation discussions were on the policy resulting from the study and the persona. Though not initially agreed, the researcher felt the persona would prove useful in explaining the policy design process. Both artefacts were emailed

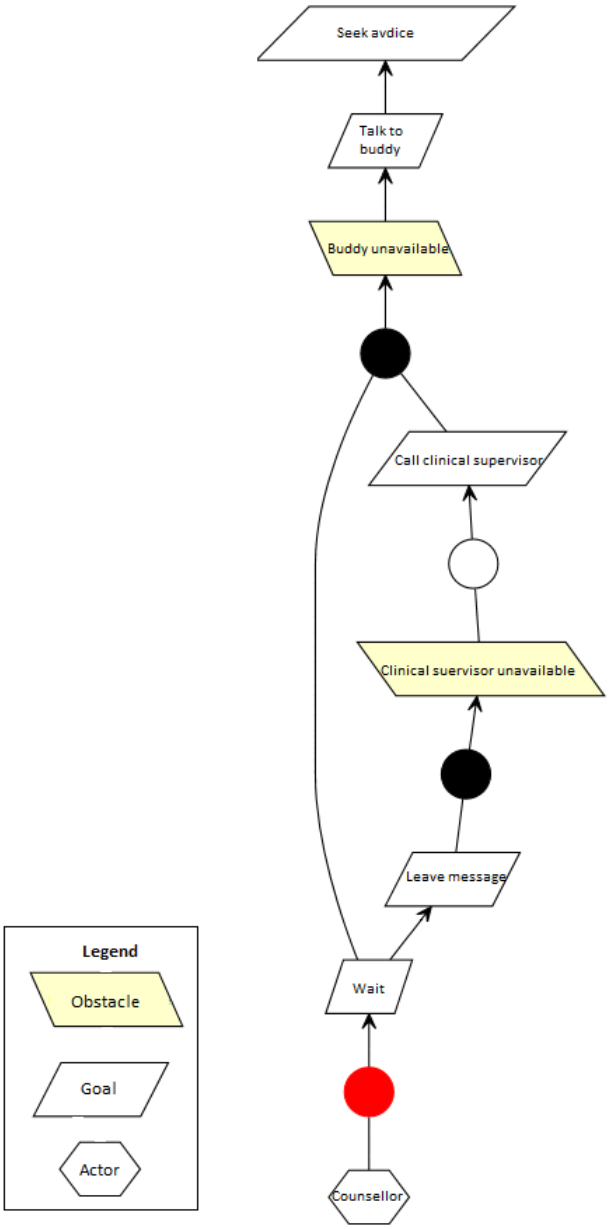


Figure 8.4: Benign obstacles

to Samaritan a day earlier.

Validation was ran as indicated in Section 8.4.4. For the most part, the stakeholders were satisfied with the policy statements but made the following observations and corrections. 1: In the policy, the counsellors' job title was corrected from psychotherapy counsellor to counsellor, a psychotherapy counsellors is a specialised role with higher qualification than those required by Samaritan. 2: Entities that facilitated the counsellors' decision making were not limited to the British Association for Counselling and Psychotherapy but included similar professional bodies. 3: The supervisors' distribution of client information had to include the Multi-Agency Safeguarding Hub (MASH) - which is the single point of

contact for reporting safeguarding concerns. 4: Due to limited time and resources, the manager observed that the policy statement where counsellors would commit to regular refreshers on related security and privacy policies was difficult to achieve. The counsellors had different levels of experience and worked on different days. This implied creating a comprehensive training plan that would take the obstacles into account. The finding indicated that although goal and conflict analysis (Section 8.5.5) did not yield results during requirements elicitation and specification, it could prove useful during policy implementation.

8.6.1.2 Contributions

A central theme in Action research is the contribution of an intervention causing change to the study environment (Baskerville 1999). The study accomplished this by presenting a policy that considered the four problems discussed during Diagnosis (Section 8.3), examples of each are highlighted as follows:

- Automation of processes
  Critical assets to be secured and security procedures to be taken into account were highlighted in the proposed policy in response to the charity's need to automate processes. In addition, the risk of a single point was identified as Samaritan kept its operations and backup devices in a single location. The practice would cause risks to automated services and avoidance measures were highlighted in the policy.

- Part-time counsellors knowledge
  As a central reference point for secure data handling, the proposed policy highlights desired security practices and authorised sources and recipients of confidential information. This knowledge would prove useful for the security inexperienced counsellors.

- IT staff experience
  The policy is a central document highlighting secure data handling expectations at the charity. It, therefore, aids the IT staff's understanding thereby facilitating security administration activities.

- GDPR concerns
  The design and implementation of the policy is a step towards proving compliance with principle six of GDPR which addresses data integrity and confidentiality.

In addition to the above, Samaritan's manager expressed their interest in incorporating the produced persona to their counsellor induction programme.

8.6.2 Validation of approach

This section validates the study approach to prove the effectiveness of the guidelines.

8.6.2.1 Best Optimal and Worst cases

An early adoption to the Samaritan case study was the use of BOW cases to elicit the counsellors' risk decision making strategies. The approach was simple but it helped the counsellors think outside their usual boundaries. For example, an interviewee pointed out that a fire hazard was a worst-case scenario based on their knowledge that Samaritan's paper files and computers were kept in one office.

The benefit of using BOW cases was also evident when an interviewee said they didn't know who to contact in the event a client had a mental or emotional breakdown. While the case initially seemed unrelated to data handling and security, it later became clear that the unauthorised sharing of a client's location would be a breach of confidentiality. The finding prompted the need to define authorised information recipients in the secure data handling policy.

Counsellor: *"I am thinking around client safety. If there were mental health issues and the client was in a really really bad way and it was unsafe for them to leave, we would need a contact. . . I think it would be useful in the contract, where the client said who to contact. I don't think we have that."*

8.6.2.2 Thematic analysis

While not a part of the guidelines, the use of thematically analysed data eased the design process considerably by linking each guideline to appropriate data. The coding process also helped the researcher's familiarisation with the data and the visualisation of possible risks and mitigation requirements. However, the use of thematic analysis is not a set part of the guidelines as other analysis techniques such as Grounded Theory could equally be used.

8.6.2.3 Design guidelines

Using the design guidelines to inform the study approach proved beneficial as they dictated which areas the researcher would focus on at each stage of the study to elicit appropriate requirements. This is evident in the output, where each guideline applied contributed to a different section of the proposed policy.

Implementing the guidelines as outlined in Table 8.2 also proved useful as output from early phases fed to later phases. For examples, a data dissemination model designed during Dynamic contextualisation (Section 8.5.3) later provided insight for Distributed rationalisation models (Section 8.5.4).

8.7 Specifying learning

The case study provides the following lessons.

8.7.1 Guideline applicability

By applying the guidelines, it was identified that while essential, not all guidelines may be applicable in a study.

8.7.2 Eliciting risk decision strategies

The security knowledge eliciting problem was discussed earlier in Section 2.2.3.3. Similar knowledge elicitation problems were identified in this study. Though decision-makers may have an understanding of risk, their strategies for addressing it are sometimes second nature and difficult to express making elicitation difficult. There still is a requirement for improved knowledge elicitation techniques in security (Ollis 2019).

8.7.3 Modelling uncertainty through Distributed Cognition

Work in the case study illustrated that uncertainty can be modelled by adapting DiCoT, a structured approach for analysing systems in terms of Distributed Cognition. The approach was introduced in Section 6.4.1.4 with the case study illustrating its application.

8.7.4 Tool support

The application of the guideline required several tools as indicated in Table 8.2. The modest size of the study made the tools and models manageable, however, a lack of a centralised tool managing the models could prove difficult in larger projects (Seffah and Metzker 2004).

8.8 Chapter summary

In this chapter, a case study was presented where the design guidelines for systems deployed in cyber security RBDM were applied to devise a research approach used to

inform the requirements of a secure data handling policy. In addition to the guidelines, a key contribution was the presentation of an approach where uncertainty may be modelled using Distributed Cognition.

While the main study participants were not security decision-makers, they proved relevant for the validation work as the risky decisions analysed in the study were from the security domain. Resulting from this is the secure data handling policy which facilitates both the counsellors' and IT/Security analysts' decision making.

The study validated the guidelines as cumulative findings of the dissertation. This illustrates the adoption and adaptation of existing design and decision making techniques to facilitate the specification of requirements for systems deployed in cyber security RBDM.

Chapter 9

Conclusion

This chapter presents the significant findings from the dissertation. It evaluate the success of the thesis in addressing the research question and the success of the contributions in satisfying the research aims. The chapter then presents the challenges and limitations experienced during the research and discusses future work. The chapter concludes by re-emphasizing the relevance and value of the research contribution.

9.1 Key research findings

This section summarizes significant findings from the dissertation.

9.1.1 The nature of risk in cyber security

A central theme in this dissertation is the idea of risk in cyber security, how it is understood and addressed. As part of the literature review, different views or understanding of risk were identified. Based on this, the research has uncovered the nuances of risk in cyber security.

For example, Chapter 4 analysed the proactive risk analysis activities deployed by security analysts. These are activities conducted before an incident has occurred dwelling on identifying the likelihood of exploitation based on inherent system weaknesses. Results from the study motivated a second study, on reactive risk analysis focussing on activities post-incident such as understanding the motivation for an attack. Based on the understanding gained, the decision making difference between the two risk analysis approaches were explained in Chapter 5. These were decision instantiated either by situation assessment or goal formation as a risk rationalisation strategy.

An alternative approach to considering risk in cyber security was the Relevance scope. Studies in Chapter 4 indicated that there is a level of risk security decision-makers are

willing to disregard before taking action. The Relevance scope was defined as a minimum level (requirement) for the continued pursuit of a security goal. Comparisons were drawn with the compliance budget, which states that the lengths at which one is willing to comply with security depends on the perceived reward to the individual.

From Chapter 5 it was identified that risk in security is not limited to the possibility of exploitation (explicit security risk), but may also result from decision making on potential risk (meta-risk). Meta-risk is implicit and was categorized as the risk in understanding, and the risk in response; both playing central roles in the direction of the research.

A few risk variations identified are illustrated in Table 9.1.

Term	**Variations**	
Risk	Explicit (in domain)	Implicit (in decision)
Risk	Dynamic (from environmental)	Static (from design)
Risk	Objective (measurable)	Perceived (feeling)
Risk outcome	Negative	Positive
Risk analysis	Proactive	Reactive
Meta-risk	In understanding	In response

Table 9.1: Risk variations

9.1.2 Independence of uncertainty

While uncertainty is an factor independent from risk, there is little clarity on how it should be considered during design. The dissertation first considers this in Chapter 5 by categorising uncertainty causing factors as: environmental, contextual, personal, and information quality. Having established this, Chapter 6, illustrated how these factors may be used to model uncertainty where they were appended to distributed information models as a way of expressing the level of confidence that may be placed in the information.

Uncertainty modelling is made possible because the proposed approach is to draw a distinction between the likelihood of risk and the uncertainty of information which were covered in the proposed guidelines 1 and 4 respectively (see Chapter 7). In other words, information about risk and information for decision making need not be the same. The first defines the problem, while the latter facilitates the decision, uncertainty was investigated the latter.

9.1.3 Distribution of decision making

The third area of note is the role Distributed Cognition plays in risk rationalisation and decision making. The researcher's initial understanding was that situation awareness (Endsley 1995) was vital to decision making, however, findings indicate that Distributed Cognition plays an equally important role. For example, the study in Chapter 4 indicated that the analysts achieved their awareness through the distribution of information between organisations, artefacts, and teams. The findings motivated the proposal of Principle 3 on Distributed rationalisation covered in Chapters 6 and 7. The principle's importance was validated in Chapter 8, where its use aided identifying authorised sources and recipients of security sensitive information for Samaritan's secure data handling policy.

9.2 Evaluation

This section reviews how the research findings and contributions address the research aims and overall research question.

9.2.1 Summarised findings from the research question

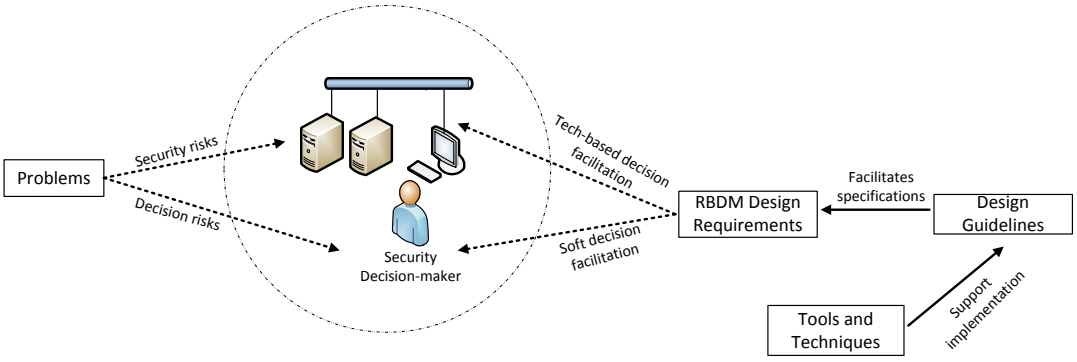


Figure 9.1: Thesis in context

In summary, this research is an implementation of inductive constructivism where each finding informs the next step of the research.

The principal claim of the thesis is *the presentation of complementary elements supporting the specification of design requirements for systems deployed in cyber security* RBDM. While the design guidelines are a cumulation of the findings, we say the thesis is a collection of complementary elements as each finding is a contribution in its own right.

Figure 9.1 puts the thesis in context by highlighting the problems which are decision risks, in security environments. The objective of the thesis was to therefore propose mitigation approaches that would facilitate decision making, motivating the research question; *What system design techniques should be taken into consideration to facilitate cyber security decision making during situations of risk and uncertainty?*

The research question was addressed by dividing it into the three research aims detailed in Sections 9.2.2, 9.2.3, and 9.2.4 below. In summary, the main contribution is the proposal of design guidelines guiding the specification of requirements for systems deployed in cyber security RBDM. Guidelines are proposed over design requirements as they are independent of problem environments and are applicable to different scenarios, while requirements are problem centric.

9.2.2 Aim 1

- To identify factors influencing risk analysis practices deployed by cyber security risk-based decision makers.

The research aim was motivated by the lack of clear distinction on how security analysts address risk and uncertainty. In most cases the literature detailed activities and decision relating to risk in cyber security with uncertainty implied but not explicitly defined.

The aim was addressed in Chapter 4 where a study on proactive and reactive risk analysis was conducted with security analysts. To this end, strategies for addressing risk were identified which included awareness, communication, and individualistic attributes such as experience and training. For most analysts, uncertainty was in the form of constraints that restricted them from carry out their duties. It was established that the constraints were the results of conditions where security and business goals were not contextually analysed or understood during planning, resulting in goal conflicts.

Based on the findings, a focus on awareness to reduce risk, and a focus on the resolution of conflicts and obstacles to address uncertainty were identified as areas requiring attention in subsequent investigations.

Contributions from the study were the identification of factors contributing to security analysts' risk practices and understanding.

9.2.3 Aim 2

- To propose approaches for adapting cyber security decision making techniques to design.

The research aim was motivated by the requirements to understand human cognition and decision making research approaches with the aim of identifying how they could be used to facilitate design.

Based on the literature, several approaches were reviewed and OODA was selected as a baseline for adapting decision making strategies to design. This was based on its simple and adaptable design which is in contrast to Situation Awareness (Endsley 1995), that for example discusses spatial awareness which is not applicable outside the aviation domain. Adaptation work and analysis were conducted in Chapters 5 and 6. Chapter 5 focused on designing a normative model (RRP) based on OODA representing cyber security decision making, and in Chapter 6 the knowledge gained from the normative model was used to design a conceptual model highlighting concepts and relationships required to design for RBDM.

As a foundation model for a large part of the research RRP was validated in various ways, however, the lack of access to cyber security participants in the UK motivated conducting some validation studies in Japan. The conceptual model was validated using a scenario based on an actual attack on the Australian Bureau of Statistics.

Scenario played a central role in validation due to the limitations of knowledge elicitation methods and the sensitivity of information in cyber security. A possible threat to validity was that the scenarios could be limited by the researchers understanding. This was however avoided by first running the scenarios with available experts.

Contributions from the investigations are a normative model for communicating and tracing risk rationalisation by cyber security decision-makers, and a conceptual model illustrating the various concepts and relationships in cyber security decision making .

To address research aim 2, the approach used to adapt cyber security decision making to design is illustrated in Figure 9.2.

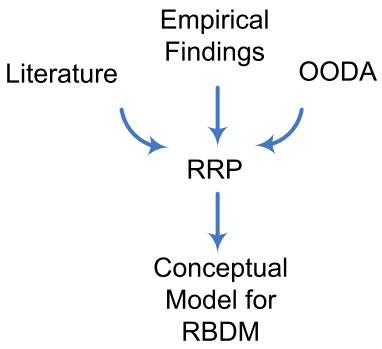


Figure 9.2: Bridging decision making and design

9.2.4 Aim 3

- To propose approaches supporting the specification of design requirements for systems facilitating cyber security Risk-based Decision Making.

The research aim was motivated by the lack of evidence that traditional design approaches could support the elicitation of cognitive decision making requirements and the shortfalls in cognitive approaches (CSE) when translating findings to design specifications.

The aim was addressed in Chapter 7 by building on insight gained from the conceptual model proposed in Chapter 6. The conceptual model highlighted the concepts and relationships required for specifying design requirements for RBDM; which were then used to draw design guidelines supported by representative modelling techniques.

As the guidelines are inductively constructed through research progression, the rationale for their selection is justified by progressive validations at each stage of the research. However, this is not to say alternative guidelines are not feasible as is the nature of qualitative research.

The guidelines were validated by informing an approach used to specify the requirements for a secure data handling policy in Chapter 8.

Having implemented and validated the guidelines, the research has illustrated how to effectively embed RBDM within cyber security system design, thereby addressing the research question.

9.2.5 Application of contributions

This section details the intended approach for disseminating and applying the contributions arising from the research, and it defines the target audience.

9.2.5.1 Application and target audience

The guidelines were developed to facilitate the capture of systems requirements for systems deployed in cyber security RBDM. The target audience are therefore system designers and requirements engineers that focus on the human aspects of cyber security, where risk-based decision-makers are the target system users. It is envisaged that the requirements will be applied during the requirements elicitation and specification stages of Requirements Engineering as illustrated in Chapter 8. Application of the guidelines is however not limited to cyber security, a point highlighted in Section 7.2. In cyber security the domain-risk is the security-risk (threat, vulnerability, and likelihood), however, the risk may differ in other domains. The application of the guidelines in other domains (outside cyber security) will be considered and evaluated as part of future work.

9.2.5.2 Accessibility

While the guidelines and other contribution in this dissertation would prove valuable when designing for RBDM, their effectiveness may only be proven by their availability to the target audience. Illustrated in Section 1.5, contributions arising from thesis work have been disseminated through peer-reviewed publications which have thus far including findings from chapters 4, 5, and 6. Findings from the remaining two chapters will also be submitted to peer-reviewed forums for publication.

As the research sponsor, Defence Science and Technology Laboratory (dstl) also plans to disseminate contributions arising from the thesis, where the researcher shall be invited to present findings to officials in the defence sector. Collaboration opportunities shall be explored on how findings may facilitate design for decision making in defence.

9.3 Challenges and limitations

Like other research undertakings, this work was not without its limitations and challenges. A critical challenge was the low number of UK based security analysts willing to participate in the research. As reported in chapters 4 and 5, the challenge was resolved by working with analysts from outside the UK. While helpful, working with analysts from outside the UK reduced the possibility for follow-up studies. For example, personas characterizing analysts' behaviour were designed based on the studies in Japan, however,

validating the personas was not possible due to logistical issue, thus the personas were not included in the dissertation.

A limitation resulting from researching in two different countries is the difference in culture. As indicated by Hofstede et al. (2010) and referenced in Section 4.3.4, culture influences the way decisions are made and culture is different from country to country. The research findings are, therefore, only generalisable to a certain degree. For example, findings in Section 4.3.4 suggests that the Japan based analysts' preferred avoiding uncertainty and making risky decisions. This may, however, not correspond to the analysts' decision making in the UK.

A second limitation of the research is that the participants were selected based on availability which could have affected who provided the data and what data they provided. However, the fact that the data was collected from a cross-section of analysts from different focus areas, different experience levels, and different industries provides a degree of assurance that the data was not from a narrow sub-set.

A final limitation of the research is that the proposed guidelines have only been validated by the researcher. As indicated in Section 9.2.5.2 above, this may be considered during the collaboration work with dstl that aims to evaluate the applicability of the guidelines in other domains.

9.4 Future work

This section proposes directions for future work based on findings from the dissertation. Directions for future work mentioned in the sections above e.g., the applications of the guidelines to other domains and the validation of the guidelines by third parties are not repeated.

9.4.1 Design requirements for groups Risk-based Decision Making

To maintain a manageable scope, the approach taken by this research was to limit investigations to the understanding and approach taken by individual decision-makers when addressing risk and uncertainty. The scope, therefore, leaves room for investigations on RBDM requirements for group decision making. This also includes verifying if the proposed guidelines may adequately facilitate the requirements specification process for group RBDM.

9.4.2 Consequences modelling

Based on the research, it has been identified that as a sector, cyber security tends to focus on security risks caused by threats and that it pays less attention to the risks caused by uninformed decision making (consequences). For examples, Chapter 4 illustrated the consequences (conflicts) of misalignment between security and business goals. Future work could investigate techniques for mapping security goals and business goals while taking the decision-makers awarenesses and degree of freedom (the level of freedom or authority to make a decision) into consideration.

9.5 Concluding summary

The research was motivated by the understanding the security analysts face the challenge of making decisions during situations of risk and uncertainty. While perfect decisions are difficult to achieve during these conditions, an optimal decision could be attained by considering the various factors that contribute to risk and uncertainty. The research therefore investigated the decision activities of security analysts and proposed guidelines that facilitate the elicitation and specifications of requirements for systems (soft and technical) deployed in cyber security, which in turn facilitate Risk-based Decision Making.

Bibliography

Adams, J., 1995. *Risk*. London [England] : Bristol, PA: UCL Press. [Cited on page 10.]

Adams, J., 2012. ISO 31000: Dr Rorschach meets Humpty Dumpty. URL `http://www.john-adams.co.uk/2012/02/22/iso-31000/`. [Cited on page 10.]

Adnan, M., Just, M., Baillie, L. and Kayacik, H. G., 2015. Investigating the work practices of network security professionals. *Information and Computer Security*, 23 (3), 347–367. [Cited on page 14.]

Ali, R., Dalpiaz, F. and Giorgini, P., 2010. A goal-based framework for contextual requirements modeling and analysis. *Requirements Engineering*, 15 (4), 439–458. [Cited on page 33.]

Amyot, D., 2017. jUCMNav. URL `http://jucmnav.softwareengineering.ca/foswiki/ProjetSEG`. [Cited on page 100.]

Azuma, R., Daily, M. and Furmanski, C., 2006. A review of time critical decision making models and human cognitive processes. *Aerospace Conference, 2006 IEEE*, IEEE, 9–pp. [Cited on page 19.]

Bainbridge, L., 1983. Ironies of automation. *Automatica*, 19 (6), 775–779. [Cited on page 33.]

Baskerville, R. L., 1999. Investigating information systems with action research. *Communications of the AIS*, 2 (19), 4. [Cited on pages 41 and 111.]

Baxter, G., Rooksby, J., Wang, Y. and Khajeh-Hosseini, A., 2012. The ironies of automation: still going strong at 30? *Proceedings of the 30th European Conference on Cognitive Ergonomics*, ACM, 65–71. [Cited on page 34.]

Beautement, A., Sasse, M. A. and Wonham, M., 2009. The compliance budget: managing security behaviour in organisations. *Proceedings of the 2008 workshop on New security paradigms*, ACM, 47–58. [Cited on pages 55 and 56.]

Bell, D. E., Raiffa, H. and Tversky, A., 1988. Descriptive, normative, and prescriptive interactions in decision making. *Decision making: Descriptive, normative, and prescriptive interactions*, 1, 9–32. [Cited on pages 15 and 16.]

Bernoulli, D., 1954. Exposition of a new theory on the measurement of risk. *Econometrica: Journal of the Econometric Society*, 23–36. [Cited on page 10.]

Bisantz, A. M., Roth, E., Brickman, B., Gosbee, L. L., Hettinger, L. and McKinney, J., 2003. Integrating cognitive analyses in a large-scale system design process. *International Journal of Human-Computer Studies*, 58 (2), 177–206. [Cited on page 26.]

Blandford, A. and Furniss, D., 2005. DiCoT: a methodology for applying distributed cognition to the design of teamworking systems. *International Workshop on Design, Specification, and Verification of Interactive Systems*, Springer, 26–38. [Cited on pages 24, 36, and 91.]

Botta, D., Muldner, K., Hawkey, K. and Beznosov, K., 2011. Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology & Work*, 13 (2), 121–134. [Cited on pages 24 and 36.]

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S. and Fisher, B., 2007. Towards understanding IT security professionals and their tools. *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS)*, ACM, 100–111. [Cited on page 14.]

Boyd, J., 1996. The essence of winning and losing. *Unpublished lecture notes*, 12 (23), 123–125. [Cited on pages xiv, 22, 23, and 59.]

Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3 (2), 77–101. [Cited on page 40.]

Bridges, R. A., Iannacone, M. D., Goodall, J. R. and Beaver, J. M., 2018. How do information security workers use host data? A summary of interviews with security analysts. *CoRR*, abs/1812.02867. [Cited on page 14.]

Buchan, A. and Taylor, J., 2016. A Qualitative Exploration of Factors Affecting Group Cohesion and Team Play in Multiplayer Online Battle Arenas (MOBAs). *The Computer Games Journal*, 5 (1-2), 65–89. [Cited on page 8.]

Buller, K., 2016. What the recent JANET attack tells us about Social Media Risk - Cyber security updates - PwC UK blogs. URL `https://pwc.blogs.com/cyber_security_updates/2016/02/what-the-recent-janet-attack-tells-us-about-social-media-risk-.html`. [Cited on page 67.]

Busby, J., 2001. Error and distributed cognition in design. *Design studies*, 22 (3), 233–254. [Cited on page 23.]

Campbell, S. G., O'Rourke, P. and Bunting, M. F., 2015. Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59 (1), 721–725. [Cited on pages xiv, 12, and 13.]

Carcary, M., 2009. The Research Audit Trial–Enhancing Trustworthiness in Qualitative Inquiry. *Electronic Journal of Business Research Methods*, 7 (1). [Cited on page 31.]

Carroll, J., 2000. Five reasons for scenario-based design. *Interacting with Computers*, 13 (1), 43–60. [Cited on page 30.]

Carroll, J. M., Anderson, N. S., Olson, J. R. and others, 1987. *Mental models in human-computer interaction: Research issues about what the user of software knows*. 12, National Academies. [Cited on page 16.]

Ceric, A. and Holland, P., 2019. The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology & People*, 32 (1), 171–188. [Cited on pages 76 and 78.]

Champion, M. A., Rajivan, P., Cooke, N. J. and Jariwala, S., 2012. Team-based cyber defense analysis. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, New Orleans, LA, USA: IEEE, 218–221. [Cited on page 8.]

Chapman, C. N. and Milham, R. P., 2006. The personas' new clothes: methodological and practical arguments against a popular method. *Proceedings of the human factors and ergonomics society annual meeting*, SAGE Publications Sage CA: Los Angeles, CA, volume 50, 634–636. [Cited on page 31.]

Cheng, B. H. and Atlee, J. M., 2007. Research directions in requirements engineering. *2007 Future of Software Engineering*, IEEE Computer Society, 285–303. [Cited on page 37.]

Chiasson, S., van Oorschot, P. C. and Biddle, R., 2007. Even experts deserve usable security: Design guidelines for security management systems. *SOUPS Workshop on Usable IT Security Management (USM)*, Citeseer, 1–4. [Cited on pages 12 and 68.]

Chipman, S. F., Schraagen, J. M. and Shalin, V. L., 2000. Introduction to cognitive task analysis. *Cognitive task analysis*, Mahwah, NJ: Lawrence Erlbaum Associates, 3–23. [Cited on page 27.]

Cohen, M. S. and Freeman, J. T., 1996. Thinking naturally about uncertainty. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, SAGE Publications Sage CA: Los Angeles, CA, volume 40, 179–183. [Cited on pages 82 and 91.]

Cooper, A., 2004. *The inmates are running the asylum*. Indianapolis, IN: Sams. [Cited on page 31.]

Cooper, A., Reimann, R., Cronin, D. and Noessel, C., 2014. *About face: The essentials of interaction design*. John Wiley & Sons. [Cited on pages 31, 89, 90, and 101.]

Corbin, J. M. and Strauss, A. L., 2008. *Basics of qualitative research: techniques and procedures for developing grounded theory*. Los Angeles, Calif: Sage Publications, Inc, 3rd ed edition. [Cited on pages 40 and 43.]

Crandall, B., Klein, G. A. and Hoffman, R. R., 2006. *Working minds: A practitioner's guide to cognitive task analysis*. Mit Press. [Cited on pages 2, 28, and 29.]

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B. and Roth, E., 2005. Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the human factors and ergonomics society annual meeting*, SAGE Publications Sage CA: Los Angeles, CA, volume 49, 229–233. [Cited on pages 13, 14, 15, 26, 30, and 91.]

Dardenne, A., van Lamsweerde, A. and Fickas, S., 1993. Goal-directed requirements acquisition. *Science of Computer Programming*, 20 (1-2), 3–50. [Cited on pages 32, 83, and 92.]

Davies, R., 2017. Shipping firm Clarksons braces for data leak after refusing to pay hacker. *The Guardian*. URL `https://www.theguardian.com/technology/2017/nov/29/shipping-charksons-data-hacker-cyber-attack`. [Cited on page 1.]

Dey, A. K., 2001. Understanding and using context. *Personal and ubiquitous computing*, 5 (1), 4–7. [Cited on page 65.]

Dezfuli, H., Stamatelatos, M., Maggio, G., Everett, C., Youngblood, R., Rutledge, P., Benjamin, A., Williams, R., Smith, C. and Guarro, S., 2010. *NASA Risk-Informed Decision Making Handbook*, volume NASA/SP -2010- 576- Version1.0. Washington, DC: NASA Office of Safety and Mission Assurance. [Cited on page 11.]

Elkind, D., 2005. Response to Objectivism and Education. *The Educational Forum*, 69 (4), 328–334. [Cited on page 38.]

Endsley, M. R., 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 37 (1), 32–64. [Cited on pages xiv, 16, 21, 63, 90, 117, and 119.]

Endsley, M. R., 2015. Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*, 9 (1), 4–32. [Cited on page 59.]

Endsley, M. R., 2017. From Here to Autonomy: Lessons Learned From Human–Automation Research. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 59 (1), 5–27. [Cited on page 33.]

Endsley, M. R., 2018. Combating Information Attacks in the Age of the Internet: New Challenges for Cognitive Engineering. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 60 (8), 1081–1094. [Cited on page 17.]

ENISA, 2017. Exploring the opportunities and limitations of current Threat Intelligence Platforms. Technical Report 1.0, European Union Agency For Network and Information Security. [Cited on page 46.]

Ersdal, G. and Aven, T., 2008. Risk informed decision-making and its ethical basis. *Reliability Engineering & System Safety*, 93 (2), 197–205. [Cited on page 11.]

Fagan, M. and Khan, M. M. H., 2016. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, Denver, CO: USENIX Association, 59–75. [Cited on page 10.]

Faily, S., 2011. *A framework of usable and secure system design*. Ph.D. thesis. [Cited on page 41.]

Faily, S., 2015. Engaging Stakeholders during Late Stage Security Design with Assumption Personas. *Information and Computer Security*, 23 (4), 435–446. [Cited on page 31.]

Faily, S., 2018. *Designing Usable and Secure Software with IRIS and CAIRIS*. OCLC: 1034541387. [Cited on pages 2 and 100.]

Faily, S., 2019a. CAIRIS. URL `https://cairis.org/`. [Cited on page 100.]

Faily, S., 2019b. HuaHana - enabling agile teams to create digital products and services with security and privacy designed in. URL `https://www.huahana.com/`. [Cited on page 95.]

Faily, S. and Fléchais, I., 2010a. Barry is not the weakest link: Eliciting Secure System Requirements with Personas. *Proceedings of the 24th BCS Interaction Specialist Group Conference*, British Computer Society, 124–132. [Cited on page 31.]

Faily, S. and Fléchais, I., 2010b. A meta-model for usable secure requirements engineering. *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems*, ACM, 29–35. [Cited on page 76.]

Faily, S. and Fléchais, I., 2011. Eliciting Policy Requirements for Critical National Infrastructure using the IRIS Framework. *International Journal of Secure Software Engineering*, 2 (4), 114–119. [Cited on page 37.]

Faily, S. and Fléchais, I., 2016. Finding and resolving security misusability with misusability cases. *Requirements Engineering*, 21 (2), 209–223. [Cited on page 75.]

Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F., 2014. Current challenges in information security risk management. *Information Management & Computer Security*, 22 (5), 410–430. [Cited on page 1.]

Finucane, M. L., Alhakami, A., Slovic, P. and Johnson, S. M., 2000. The affect heuristic in judgments of risks and benefits. *Journal of behavioral decision making*, 13 (1), 1. [Cited on page 17.]

Fischer, G., 1991. The importance of models in making complex systems comprehensible. *Human Factors in Information Technology*, Elsevier, volume 2, 3–36. [Cited on page 37.]

Fischhoff, B. and Kadvany, J., 2011. *Risk: A very short introduction*. Oxford University Press. [Cited on page 10.]

Fischhoff, B., Watson, S. R. and Hope, C., 1984. Defining risk. *Policy Sciences*, 17 (2), 123–139. [Cited on page 10.]

Fisher, C. W. and Kingma, B. R., 2001. Criticality of data quality as exemplified in two disasters. *Information & Management*, 39 (2), 109–116. [Cited on pages 2 and 91.]

Fiske, S. T. and Taylor, S. E., 2013. *Social Cognition: from brains to culture*. Los Angeles: SAGE, 2nd edition edition. [Cited on page 17.]

Flechais, I., 2005. *Designing secure and usable systems*. Ph.D. thesis, University College London. [Cited on pages 41 and 87.]

Flechais, I., Mascolo, C. and Sasse, M. A., 2007. Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1 (1), 12. [Cited on pages 30 and 37.]

Flechais, I. and Sasse, M. A., 2009. Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-Science. *International Journal of Human-Computer Studies*, 67 (4), 281–296. [Cited on page 2.]

Flick, U., 2014. *An introduction to qualitative research*. Los Angeles: Sage, edition 5 edition. OCLC: ocn863173053. [Cited on page 66.]

Franke, U. and Brynielsson, J., 2014. Cyber situational awareness–a systematic review of the literature. *Computers & Security*, 46, 18–31. [Cited on page 90.]

Fraser, J. M., Smith, P. J. and Smith, J. W., 1992. A catalog of errors. *International Journal of Man-Machine Studies*, 37 (3), 265–307. [Cited on page 18.]

Friess, E., 2012. Personas and decision making in the design process: an ethnographic case study. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, 1209–1218. [Cited on page 31.]

Furnell, S., 2005. Why users cannot use security. *Computers & Security*, 24 (4), 274–279. [Cited on page 12.]

Fuxman, A., Pistore, M., Mylopoulos, J. and Traverso, P., 2000. Model checking early requirements specifications in Tropos. IEEE Comput. Soc, 174–181. [Cited on page 90.]

Gentner, D., 2001. Mental Models, Psychology of. *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier, 9683–9687. [Cited on page 16.]

Gerber, M., Wong, B. W. and Kodagoda, N., 2016. How Analysts Think: Intuition, Leap of Faith and Insight. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 60 (1), 173–177. [Cited on pages 18 and 36.]

Gersh, J. R., McKneely, J. A. and Remington, R. W., 2005. Cognitive engineering: Understanding human interaction with complex systems. *Johns Hopkins APL technical digest*, 26 (4), 377–382. [Cited on page 27.]

Gigerenzer, G., 1991. How to make cognitive illusions disappear: Beyond "heuristics and biases". *European review of social psychology*, 2 (1), 83–115. [Cited on page 17.]

Gilovich, T., Griffin, D. and Kahneman, D., 2002. *Heuristics and biases: The psychology of intuitive judgment*. Cambridge university press. [Cited on page 17.]

Glaser, B. G. and Strauss, A. L., 1967. *The discovery of grounded theory: strategies for qualitative research*. Chicago: Aldine. [Cited on page 40.]

Grant, T. and Kooter, B., 2005. Comparing OODA & other models as operational view C2 architecture. *Proceedings of the 10th International Command and Control Research Technology Symposium*. [Cited on pages 21 and 22.]

Gray, D., 2016. *Doing research in the business world*. Thousand Oaks, CA: SAGE Publications Ltd, 1st edition edition. [Cited on pages 38 and 39.]

Great Britain, 1998. *Data Protection Act*. London: Stationery Office. [Cited on page 49.]

Green, M. and Smith, M., 2016. Developers are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security & Privacy*, 14 (5), 40–46. [Cited on page 2.]

Grispos, G., Glisson, W. B. and Storer, T., 2015. Security Incident Response Criteria: A Practitioner's Perspective. *21st Americas Conference on Information Systems, AMCIS 2015, Puerto Rico, August 13-15, 2015*. [Cited on page 14.]

Groenewald, C., Wong, B. L. W., Attfield, S., Passmore, P. and Kodagoda, N., 2017. How Analysts Think: How Do Criminal Intelligence Analysts Recognise and Manage Significant Information? IEEE, 47–53. [Cited on page 91.]

Guba, E. G. and Lincoln, Y. S., 1994. Competing paradigms in qualitative research. *Handbook of qualitative research*, London: Sage, volume 2 of *N. K. Denzin & Y. S. Lincoln*, 105–117. [Cited on page 38.]

Gutzwiller, R. S., Fugate, S., Sawyer, B. D. and Hancock, P. A., 2015. The Human Factors of Cyber Network Defense. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59 (1), 322–326. [Cited on pages 33, 36, and 37.]

Gutzwiller, R. S., Hunt, S. M. and Lange, D. S., 2016. A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, San Diego, CA, USA: IEEE, 14–20. [Cited on pages 14, 28, and 91.]

HAISA, 2019. International Symposium on Human Aspects of Information Security & Assurance, Nicosia, Cyprus, 15-17 July 2019. URL `https://haisa.org/`. [Cited on page 12.]

Heath, H. and Cowley, S., 2004. Developing a grounded theory approach: a comparison of Glaser and Strauss. *International Journal of Nursing Studies*, 41 (2), 141–150. [Cited on page 40.]

Heineman, G. T., Pollice, G. and Selkow, S., 2016. *Algorithms in a nutshell*. In a nutshell, Sebastopol, CA: O'Reilly, second edition edition. OCLC: ocn910773336. [Cited on page 99.]

Hibshi, H., Breaux, T. D., Riaz, M. and Williams, L., 2016. A grounded analysis of experts' decision-making during security assessments. *Journal of Cybersecurity*, 2 (2), 147–163. [Cited on pages 12, 14, 22, 36, and 58.]

Hoffman, R., Feltovich, P., Ford, K. and Woods, D., 2002. A rose by any other name...would probably be given an acronym [cognitive systems engineering]. *IEEE Intelligent Systems*, 17 (4), 72–80. [Cited on page 27.]

Hofstede, G., Hofstede, G. J. and Minkov, M., 2010. *Cultures and organizations: software of the mind ; intercultural cooperation and its importance for survival*. New York:

McGraw-Hill, rev. and expanded 3. ed edition. OCLC: 699216499. [Cited on pages 55 and 122.]

Hollan, J., Hutchins, E. and Kirsh, D., 2000. Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 7 (2), 174–196. [Cited on pages 23, 43, and 91.]

Horkoff, J. and Yu, E., 2011. Analyzing goal models: different approaches and how to choose among them. *Proceedings of the 2011 ACM Symposium on Applied Computing - SAC '11*, TaiChung, Taiwan: ACM Press, 675. [Cited on page 32.]

Hutchins, E., 2000. *Cognition in the wild*. Cambridge, Mass: MIT Press, nachdr. edition. OCLC: 248968842. [Cited on page 23.]

Hutchins, E. and Klausen, T., 1996. Distributed cognition in an airline cockpit. *Cognition and communication at work*, Cambridge: Cambridge University Press, y. engestrom and d middleton edition, 15–34. [Cited on page 23.]

Hutchison, A. J., Johnston, L. H. and Breckon, J. D., 2010. Using QSR-NVivo to facilitate the development of a grounded theory project: an account of a worked example. *International Journal of Social Research Methodology*, 13 (4), 283–302. [Cited on pages 43 and 100.]

IBM Australia, 2016. Inquiry into The Preparation, Administration and Management of the 2016 Census by the Australian Bureau of Statistics. Technical report. [Cited on page 76.]

ISO, 2013. *ISO/IEC 27001: Information Technology – Security Techniques – Requirements.*. ISO/IEC. [Cited on page 84.]

ISO, I., 2009. 31000: 2009 Risk management–Principles and guidelines. *International Organization for Standardization, Geneva, Switzerland*. [Cited on page 10.]

ISO 9241-210, 2010. Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems. [Cited on pages 26 and 29.]

Jajodia, S., Liu, P., Swarup, V. and Wang, C., eds., 2010. *Cyber Situational Awareness*, volume 46 of *Advances in Information Security*. Boston, MA: Springer US. [Cited on page 22.]

Jenkins, D. P., Stanton, N. A. and Walker, G. H., 2017. *Cognitive Work Analysis: Coping with Complexity*. OCLC: 1004350430. [Cited on pages xiv, 28, and 29.]

Johnson, D. D., Blumstein, D. T., Fowler, J. H. and Haselton, M. G., 2013. The evolution of error: Error management, cognitive constraints, and adaptive decision-making biases. *Trends in ecology & evolution*, 28 (8), 474–481. [Cited on page 2.]

Johnson, H. M. and Seifert, C. M., 1994. Sources of the continued influence effect: When misinformation in memory affects later inferences. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 20 (6), 1420–1436. [Cited on page 16.]

Johnson, J. and Henderson, A., 2002. Conceptual models: begin by designing what to design. *interactions*, 9 (1). [Cited on page 74.]

Kahneman, D., 2002. Maps of bounded rationality: A perspective on intuitive judgment and choice. *Nobel prize lecture*, 8, 351–401. [Cited on page 89.]

Kahneman, D., 2003. A Psychological Perspective on Economics. *American Economic Review*, 93 (2), 162–168. [Cited on page 10.]

Kahneman, D., 2011. *Thinking, fast and slow*. Macmillan. [Cited on pages 17 and 89.]

Kahneman, D. and Klein, G., 2009. Conditions for intuitive expertise: a failure to disagree. *American Psychologist*, 64 (6), 515. [Cited on page 18.]

Kahneman, D. and Tversky, A., 1979. Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the econometric society*, 263–291. [Cited on pages 10, 15, and 17.]

Kandogan, E. and Haber, E. M., 2005. Security administration tools and practices. *Security and Usability: Designing Secure Systems that People Can Use*, Sebastopol, CA: O'Reilly, l. f. cranor & s. garfinkel edition, 357–378. [Cited on page 14.]

Ki-Aries, D. and Faily, S., 2017. Persona-centred information security awareness. *Computers & Security*, 70, 663–674. [Cited on page 31.]

Kim, S. J., Lim, G. J., Cho, J. and Côté, M. J., 2017. Drone-Aided Healthcare Services for Patients with Chronic Diseases in Rural Areas. *Journal of Intelligent & Robotic Systems*, 88 (1), 163–180. [Cited on page 95.]

Klein, G., 1999. *Sources of power: How people make decisions*. MIT press. [Cited on pages 18 and 58.]

Klein, G., 2008. Naturalistic Decision Making. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 50 (3), 456–460. [Cited on pages xiv, 19, and 20.]

Klein, G., Calderwood, R. and MacGregor, D., 1989. Critical decision method for eliciting knowledge. *IEEE Transactions on Systems, Man, and Cybernetics*, 19 (3), 462–472. [Cited on pages 27 and 89.]

Klein, G., Phillips, J. K., Rall, E. L. and Peluso, D. A., 2007. A data-frame theory of sensemaking. *Expertise out of context: Proceedings of the sixth international conference on*

naturalistic decision making, New York, NY, USA: Lawrence Erlbaum, 113–155. [Cited on pages 77 and 79.]

Klein, G. A., 1993. *Decision making in action: models and methods*. Norwood, N.J.: Ablex Pub. OCLC: 25510308. [Cited on page 20.]

Knight, F. H., 2009. *Risk, uncertainty and profit*. Kissimmee, Fla: Signalman. OCLC: 845718098. [Cited on page 11.]

Knox, K. T., 2004. A researcher's dilemma-philosphical and methodological pluralism. *The Electronic Journal of Business Research Methods*, 2 (2), 119–128. [Cited on pages 38 and 39.]

Kotulic, A. G. and Clark, J. G., 2004. Why there aren't more information security research studies. *Information & Management*, 41 (5), 597–607. [Cited on page 14.]

van Lamsweerde, A., 2000. Requirements engineering in the year 00: a research perspective. *Proceedings of the 22nd international conference on Software engineering - ICSE '00*, Limerick, Ireland: ACM Press, 5–19. [Cited on page 32.]

van Lamsweerde, A. and Letier, E., 2000. Handling obstacles in goal-oriented requirements engineering. *IEEE Transactions on Software Engineering*, 26 (10), 978–1005. [Cited on pages 32, 83, and 92.]

Lapouchnian, A., 2005. Goal-oriented requirements engineering: An overview of the current research. Technical report. [Cited on pages 31, 32, and 80.]

Lee, D., 2018. Uber pays $148m over data breach cover-up. URL `https://www.bbc.com/news/technology-45666280`. [Cited on page 1.]

Lehaney, B. and Vinten, G., 1994. "Methodology": An Analysis of Its Meaning and Use. *Work Study*, 43 (3), 5–8. [Cited on page 38.]

Lewin, K., 1946. Action Research and Minority Problems. *Journal of Social Issues*, 2 (4), 34–46. [Cited on page 41.]

Li, J., Ou, X. and Rajagopalan, R., 2010. Uncertainty and risk management in cyber situational awareness. *Cyber Situational Awareness*, Springer, 51–68. [Cited on pages 13, 14, 42, and 51.]

Lin, Y. C., Paul, A., Corotis, R. B. and Liel, A. B., 2015. Framework Methodology for Risk-Based Decision Making for Transportation Agencies. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 1 (3), 04015006. [Cited on pages 2 and 11.]

Lintern, G., 2010. A Comparison of the Decision Ladder and the Recognition-Primed Decision Model. *Journal of Cognitive Engineering and Decision Making*, 4 (4), 304–327. [Cited on page 18.]

Macesker, B., Myers, J. J., Guthrie, V. H., Walker, D. A. and Schoolcraft, S. G., 2002. Quick-reference Guide to Risk-based Decision Making (RBDM): A Step-by-step Example of the RBDM Process in the Field. *19th, International system safety conference*, Huntsville, Alabama. [Cited on page 11.]

MacGibbon, A., 2016. Review of the events surrounding the 2016 ECENSUS: improving institutional cyber security culture and practices across the Australian government. Technical report, Department of the Prime Minister and Cabinet. URL `https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22`. [Cited on page 76.]

MacKenzie, I. S., 2013. *Human-computer interaction: an empirical research perspective*. Amsterdam: Morgan Kaufmann. [Cited on page 72.]

McGeorge, P. and Rugg, G., 1992. The uses of 'contrived' knowledge elicitation techniques. *Expert Systems*, 9 (3), 149–154. [Cited on page 89.]

Militello, L. G., Dominguez, C. O., Lintern, G. and Klein, G., 2009. The role of cognitive systems engineering in the systems engineering design process. *Systems Engineering*, n/a–n/a. [Cited on pages xiv, 26, and 27.]

Ministry of Communications and Informations, 2019. Public Report of the Committee of Inquiry into the Cyber Attack on Singapore Health Services Private Limited's Patient Database on or Around 27 June 2018. Technical report. [Cited on page 76.]

Moeckel, C., 2018. From user-centred design to security: building attacker personas for digital banking. *Proceedings of the 10th Nordic Conference on Human-Computer Interaction - NordiCHI '18*, Oslo, Norway: ACM Press, 892–897. [Cited on page 31.]

Nesse, R. M., 2005. Natural selection and the regulation of defenses: A signal detection analysis of the smoke detector principle. *Evolution and Human Behavior*, 26 (1), 88–105. [Cited on page 17.]

Nextgen Group, 2016. Nextgen's Response to Senate Inquiry Into 2016 Census. Technical report. [Cited on page 76.]

Nickerson, R. S., 1998. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, 2 (2), 175–220. [Cited on page 17.]

Norman, D. A., 1999. Affordance, conventions, and design. *interactions*, 6 (3), 38–43. [Cited on page 62.]

O'Hagan, T., 2004. Dicing with the unknown. *Significance*, 1 (3), 132–133. [Cited on page 11.]

Ollis, G., 2019. *Helping developers to help each other: a technique to facilitate understanding among professional software developers.*. PhD Thesis, Bournemouth University. [Cited on page 113.]

Orasanu, J. and Connolly, T., 1995. The reinvention of decision making. *Decision making in action: Models and methods*, New Jersey: Norwood, 3–20. [Cited on page 19.]

Osinga, F. P., 2007. *Science, strategy and war: The strategic theory of John Boyd*. Routledge. [Cited on page 22.]

Parasuraman, R. and Manzey, D. H., 2010. Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 52 (3), 381–410. [Cited on page 33.]

Parasuraman, R., Sheridan, T. B. and Wickens, C. D., 2000. A model for types and levels of human interaction with automation. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, 30 (3), 286–297. [Cited on page 34.]

Parush, A., 2017. Situational awareness: a tacit yet viable concept. *Canadian Journal of Anesthesia/Journal canadien d'anesthésie*, 1–4. [Cited on pages 22 and 36.]

Paul, C. L. and Whitley, K., 2013. A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. *Human aspects of information security, privacy, and trust*, Springer, 145–154. [Cited on page 14.]

Pirolli, P. and Card, S., 2005. The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. *Proceedings of International Conference on Intelligence Analysis*, 2–4. [Cited on page 21.]

Pohl, K., 1994. The Three Dimensions of Requirements Engineering: A Framework and Its Applications. *Inf. Syst.*, 19 (3), 243–258. [Cited on page 93.]

Pohl, K. and Rupp, C., 2015. *Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam, foundation level, IREB compliant*. Santa Barbara, CA: Rocky Nook, second edition edition. [Cited on pages 93 and 98.]

Potts, C., 1995. Using schematic scenarios to understand user needs. *Proceedings of the conference on Designing interactive systems processes, practices, methods, &*

techniques - DIS '95, Ann Arbor, Michigan, United States: ACM Press, 247–256. [Cited on page 32.]

Pruitt, J. and Adlin, T., 2006. *The Persona Lifecycle : Keeping People in Mind Throughout Product Design*. The Morgan Kaufmann Series in Interactive Technologies, Amsterdam: Morgan Kaufmann. [Cited on page 31.]

Rajkomar, A. and Blandford, A., 2012. Understanding infusion administration in the ICU through distributed cognition. *Journal of biomedical informatics*, 45 (3), 580–590. [Cited on pages 24 and 43.]

Rashid, A., Naqvi, S. A. A., Ramdhany, R., Edwards, M., Chitchyan, R. and Babar, M. A., 2016. Discovering "unknown known" security requirements. *38th International Conference on Software Engineering*, ACM Press, 866–876. [Cited on page 64.]

Rasmussen, J., 1974. The human data processor as a system component. Bits and pieces of a model. Technical Report Risø-M-1722, Danish Atomic Energy Commission, Roskilde, Denmark. [Cited on pages xiv, 18, 19, and 58.]

Rasmussen, J., Pejtersen, A. M. and Goodstein, L. P., 1994. *Cognitive systems engineering*. Wiley series in system engineering, New York: Wiley, 2. dr. edition. OCLC: 832455151. [Cited on page 28.]

RedHat, 2017. Security Backporting Practice. URL `https://access.redhat.com/security/updates/backporting`. [Cited on page 63.]

Rieman, J., Franzke, M. and Redmiles, D., 1995. Usability evaluation with the cognitive walkthrough. *Conference companion on Human factors in computing systems*, ACM, 387–388. [Cited on page 66.]

Ritter, F. E., Baxter, G. D. and Churchill, E. F., 2014. *Foundations for designing user-centered systems: what system designers need to know about people*. London: Springer. OCLC: ocn866931414. [Cited on page 33.]

Roedl, D. J. and Stolterman, E., 2013. Design research at CHI and its applicability to design practice. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, Paris, France: ACM Press, 1951. [Cited on page 2.]

Rolland, C., Souveyet, C. and Achour, C., 1998. Guiding goal modeling using scenarios. *IEEE Transactions on Software Engineering*, 24 (12), 1055–1071. [Cited on page 31.]

Rosson, M. B. and Carroll, J. M., 2002. *Usability engineering: scenario-based development of human-computer interaction*. The Morgan Kaufmann series in interactive technologies, San Francisco, Calif.: Kaufmann, repr., 2. druck edition. OCLC: 845847524. [Cited on page 30.]

Roth, E. M., Patterson, E. S., Mumaw, R. J. and Wiley, J., 2001. *Cognitive Engineering: Issues in User-Centered System Design*, volume 2 of *Encyclopedia of Software Engineering*. New York: Wiley- Interscience, j. j. marciniak edition. [Cited on pages 29 and 89.]

Royal Society, ed., 1983. *Risk assessment: report of the a Royal Society Study Group*. London: The Royal Soc. OCLC: 10394029. [Cited on page 10.]

Rumbaugh, J., Jacobson, I. and Booch, G., 1999. *The unified modeling language reference manual*. The Addison-Wesley object technology series, Reading, Mass: Addison-Wesley. [Cited on page 76.]

Saldana, J., 2015. *The coding manual for qualitative researchers*. Sage. [Cited on page 102.]

Salmon, P., Stanton, N., Walker, G. and Green, D., 2006. Situation awareness measurement: A review of applicability for C4i environments. *Applied ergonomics*, 37 (2), 225–238. [Cited on page 22.]

Sasse, M. A., Brostoff, S. and Weirich, D., 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, 19 (3), 122–131. [Cited on page 2.]

Saunders, M., Lewis, P. and Thornhill, A., 2009. *Research methods for business students*. Harlow: Financial Times Prentice Hall, 5. ed edition. OCLC: 298611650. [Cited on pages 38 and 40.]

Schraw, G. and Moshman, D., 1995. Metacognitive theories. *Educational Psychology Review*, 7 (4), 351–371. [Cited on page 61.]

Schwalbe, K., 2014. *Information technology project management*. Boston, MA: Course Technology, Cengage Learning, seventh edition edition. [Cited on page 48.]

Seffah, A. and Metzker, E., 2004. The obstacles and myths of usability and software engineering. *Communications of the ACM*, 47 (12), 71–76. [Cited on page 113.]

ServiceNow, 2019. ServiceNow - Digital Workflows for Enterprise - Make work, work better. URL `https://www.servicenow.com`. [Cited on page 45.]

Shadbolt, N. and Smart, P., 2015. Knowledge Elicitation: Methods, Tools and Techniques. *Evaluation of human work*, Boca Raton, FL: Taylor & Francis, 3rd ed edition, 163–200. [Cited on pages 19 and 89.]

Simon, H. A., 1972. Theories of bounded rationality. *Decision and organization*, 1 (1), 161–176. [Cited on page 18.]

Smetters, D. K. and Grinter, R. E., 2002. Moving from the design of usable security technologies to the design of useful secure applications. *Proceedings of the 2002 workshop on New security paradigms*, ACM, 82–89. [Cited on page 1.]

Squires, A., 2009. Methodological challenges in cross-language qualitative research: A research review. *International Journal of Nursing Studies*, 46 (2), 277–287. [Cited on page 52.]

Stamatelatos, M., Dezfuli, H. and Apostolakis, G., 2006. A proposed risk-informed decision-making framework for nasa. *Eigth International Conference on Probabilistic Safety Assessment and Management*. [Cited on page 11.]

Stanton, N. A., Salmon, P. M., Walker, G. H. and Jenkins, D. P., 2010. Is situation awareness all in the mind? *Theoretical Issues in Ergonomics Science*, 11 (1-2), 29–40. [Cited on page 23.]

Steele, A. and Jia, X., 2008. Adversary Centered Design: Threat Modeling Using Anti-Scenarios, Anti-Use Cases and Anti-Personas. *Proceedings of the 2008 International Conference on Information & Knowledge Engineering, IKE 2008, July 14-17, 2008, Las Vegas, Nevada, USA*, 367–370. [Cited on page 31.]

Suchman, L. A., 1987. *Plans and situated actions: The problem of human-machine communication*. Cambridge university press. [Cited on page 25.]

Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J. and Rajagopalan, S. R., 2015. A human capital model for mitigating security analyst burnout. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 347–359. [Cited on page 12.]

Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L. and Hoffmann, M., 2014. A Tale of Three Security Operation Centers. *Proceedings of the 2014 ACM Workshop on Security Information Workers*, ACM, 43–50. [Cited on page 14.]

Toma, S.-V., Chiriţă, M. and Şarpe, D., 2012. Risk and Uncertainty. *Procedia Economics and Finance*, 3, 975–980. [Cited on page 91.]

Turner, M. E. and Pratkanis, A. R., 1998. Twenty-Five Years of Groupthink Theory and Research: Lessons from the Evaluation of a Theory. *Organizational Behavior and Human Decision Processes*, 73 (2-3), 105–115. [Cited on page 8.]

Tversky, A. and Kahneman, D., 1973. Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, 5 (2), 207–232. [Cited on page 17.]

Tversky, A. and Kahneman, D., 1974. Judgment under uncertainty: Heuristics and biases. *Utility, probability, and human decision making*, Springer, 141–162. [Cited on page 17.]

University of Toronto, 2000. GRL - Goal-oriented Requirement Language. URL https://www.cs.toronto.edu/km/GRL/. [Cited on page 90.]

University of Toronto, 2011. i* Intentional STrategic Actor Relationships modelling - istar. URL http://www.cs.toronto.edu/km/istar/. [Cited on pages 32, 80, and 90.]

USENIX, 2018. Symposium On Usable Privacy and Security. URL https://www.usenix.org/conference/soups2019. [Cited on page 12.]

Varga, J., Iacob, C., Grote, M. and Stanton, N., 2015. Constraint Analysis for Aircraft Landing in Distributed Crewing Contexts. *Procedia Manufacturing*, 3, 2682–2689. [Cited on pages 26 and 29.]

Vicente, K. J., 1995. Task Analysis, Cognitive Task Analysis, Cognitive Work Analysis: What's the Difference? *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 39 (9), 534–537. [Cited on page 28.]

Vicente, K. J., 1999. *Cognitive work analysis: toward safe, productive, and healthy computer-based work*. Mahwah, NJ: Erlbaum. OCLC: 246268183. [Cited on page 28.]

Vocus Communications, 2016. Senate inquiry into 2016 census: Response of Vocus Communications Ltd to the submission of IBM Australia Ltd. Technical report. [Cited on page 76.]

Wang, Y. R., Pierce, E. M., Madnik, S. E., Fisher, C. W. and Zwass, V., eds., 2005. *Information quality*. Number v. 1 in Advances in management information systems, Armonk, N.Y. ; London, England: M.E. Sharpe. OCLC: ocm60564423. [Cited on page 65.]

Werlinger, R., Muldner, K., Hawkey, K. and Beznosov, K., 2010. Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security*, 18 (1), 26–42. [Cited on pages 12, 14, 16, and 70.]

Wilson, K. M., Helton, W. S. and Wiggins, M. W., 2013. Cognitive engineering: Cognitive engineering. *Wiley Interdisciplinary Reviews: Cognitive Science*, 4 (1), 17–31. [Cited on page 2.]

Wong, B. L. W., 2014. How Analysts Think (?): Early Observations. IEEE, 296–299. [Cited on page 58.]

Wong, B. W. and Kodagoda, N., 2015. How Analysts Think: Inference Making Strategies. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 59 (1), 269–273. [Cited on page 58.]

Wong, B. W. and Varga, M., 2012. Black holes, keyholes and brown worms: Challenges in sense making. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, SAGE Publications, volume 56, 287–291. [Cited on page 79.]

Wright, P. C., Fields, R. E. and Harrison, M. D., 2000. Analyzing human-computer interaction as distributed cognition: the resources model. *Human-Computer Interaction*, 15 (1), 1–41. [Cited on page 24.]

WSIS, 2018. 4th Workshop on Security Information Workers. URL `https://wsiw2018.l3s.uni-hannover.de/`. [Cited on page 12.]

Yeganeh, H. and Su, Z., 2004. A critical review of epistemological and methodological issues in cross-cultural research. *Journal of Comparative International Management*, 7 (2), 66–87. [Cited on page 38.]

Yu, E. S., 1997. Towards modelling and reasoning support for early-phase requirements engineering. *Requirements Engineering, 1997., Proceedings of the Third IEEE International Symposium on*, IEEE, 226–235. [Cited on pages 80 and 90.]

Yu, E. S. K., ed., 2011. *Social modeling for requirements engineering*. Cooperative information systems, Cambridge, Mass: MIT Press. OCLC: ocn459208266. [Cited on page 2.]

Appendices

.1 Risk Analysis Practices Data

Appendix .1 aims to give further detail on the interview processes, ethical considerations, and data analysis methods used during the risk analysis practises studies covered in Chapter 4.

The appendix begins by presenting predefined interview questions guiding the vulnerability analysis study in Appendix .1.1. A participant information sheet used to inform participants on ethical consideration and the aim of the study, and a participant agreement form used to obtain written consent are then presented in Appendix .1.2 and .1.3 respectively. These follow Bournemouth University's ethics procedures for interviews and focus groups. Two sample screenshots are then presented illustrating Grounded Theory work during the proactive risk analysis study undertaken in Section 4.2, the first screenshot illustrates themes derived from the interview transcripts (Appendix .1.4), and the second screenshot illustrates coding progression using NVivo (Appendix .1.5). Appendix .1 concludes by presenting sample participant responses in Japanese from the reactive analysis study covered in Section 4.3.

.1.1 Predefined interview questions

- What guidelines do you follow to help you manage risk?
- How do you select vulnerabilities to act upon when time and resources are limited?
- Are vulnerabilities identified as high or critical by the automated scanners representative of your work environment?
- How do you identify false positives?
- What were the occasions when you had to accepted risk?
- What kind of decision making constraints have you experienced during your work?

.1.2 Participant Information Sheet

Bournemouth University

The title of the research project

Designing for Cyber Security Risk-based Decision Making

Invitation to take part

You are being invited to take part in a research project. Before you decide, it is important for you to understand why the research is being conducted and what it will involve. Please take the time to read the following information carefully and discuss it with others if you wish. Ask us if there is anything that is not clear or if you would like more information. Take time to decide whether or not you wish to take part.

Researcher

This study is being carried out by Andrew M'manga a PhD researcher at Bournemouth University under the faculty of Science and Technology. The research is in Cyber Security with a focus on designing systems for decision making during risk and uncertainty.

Research Funders

This research is funded collaboratively by Defence Science and Technology Laboratory (Dstl) and Bournemouth University.

Purpose of the project

Cyber security is an area that has been given a lot of attention in recent years due to the current state of information security. This project has been undertaken with the understanding that it is better to consider security and usability issues early during the design stages as opposed to implementing them as an afterthought. Security professional regularly face the challenge of identifying the most effective response when faced with risk under uncertain conditions. The project aims to facilitate the decision making process by proposing techniques for incorporating risk-based decision making requirements during design.

Why have I been chosen?

Participants for this research have been chosen based on the reason that they are cybersecurity professionals or play a role essential to understanding decision making during risk and uncertainty in their organisation. Recruitment is based on management recommendation from your organisation, and participants will most likely not exceed ten.

Do I have to take part?

It is up to you to decide whether or not to take part. If you do decide to take part, you will be given this information sheet to keep and be asked to sign a participant agreement form. You can withdraw during the interview at any time and without giving a reason and we will remove any data collected

about you from the study. Once the interview has finished you can still withdraw your data up to the point where the data has been analysed and has become anonymous, so your identity cannot be determined. Deciding to take part or not will not adversely impact affect you or others in any way.

What would taking part involve?

The interviews will involve a series of unstructured questions aimed at eliciting requirements that could facilitate your decision making during risk and uncertainty. The facilitation will take the form of jointly developing policies or tools that take risk-based decision making into account. Interviews could be on a one-to-one or group discussion (focus group) basis and should last for roughly an hour, to two for focus groups.
Using a hand-held audio recording device, audio recordings of the interviews shall be taken purely for the purpose of transcribing the data for qualitative analysis and all personal identification information (if any) shall be anonymised. As the interviews shall be unstructured, the direction the interview questions take shall be based on participant's responses. All interviews shall be held within the participant's organisations or by Skype where need be.

What are the advantages and possible disadvantages or risks of taking part?

Based on the participating organisation's requirements, it is hoped that tools, policies or procedures that take risk-based decision making into account shall be developed or improvements shall be made to current practices. There are no foreseeable risks or discomfort expected as a result of participating, and all interviews shall be held during normal working hours.

What type of information will be sought from me and why is the collection of this information relevant for achieving the research project's objectives?

The research will only aim at collecting data to understand decisions making during risk and uncertainty and from an information security perspective. The information collected will depend on the tools, policies or procedures your organisation wishes to develop. However, no personal identifiable data or confidential information will be required of you. Questions will relate to; understanding the nature of risk and uncertainty in the organisation, identifying information sources for decision making, goals, obstacles, and key decision making roles.

Will I be recorded, and how will the recorded media be used?

As mentioned above, audio recordings of the interviews will be made during this research and will be used only for analysis and for illustration at conference presentations and lectures. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the recordings.

How will my information be kept?

All the information we collect about you during the course of the research will be kept strictly in accordance with current Data Protection Regulations. You will not be able to be identified in any reports or publications without your specific consent.

All personal identification data relating to this study (e.g. organisation and participant names) will be held only up to the date of publication of the research. Bournemouth University will hold the information we collect on a protected secure network.

Except where it has been anonymised, we will restrict access to your personal data to those individuals who have a legitimate reason to access it for the purpose or purposes for which it is held by us. As well as BU staff and the BU student working on the research project and the project funders who will be given access to it in anonymised form.

The information collected about you may be used in an anonymous form to support other research projects in the future and access to it in this form will not be restricted. It will not be possible for you to be identified from this data. Anonymised data will be added to Bournemouth Universities' Data Repository (a central location where data is stored) and which will be publicly available.

Contact for further information

If you have any questions or would like further information, please contact Dr Shamal Faily and Dr John McAlaney.

Bournemouth University
Poole House,
Talbot Campus, Fern Barrow,
Poole, Dorset BH12 5BB,
Tel +44 (0) 1202 965078

Any concerns about the study should be directed to sfaily@bournemouth.ac.uk. If your concerns have not been answered within two weeks, you should contact Professor Marcin Budka, Faculty of Science and Technology, Bournemouth University by email to researchgovernance@bournemouth.ac.uk.

Finally

If you decide to take part, you will be given a copy of the information sheet and a participant agreement form to sign and keep.

Thank you for considering taking part in this research project.

.1.3 Participant Agreement Form

Full title of project: Designing for Cyber Security Risk-based Decision Making

Name, position and contact details of researcher: Andrew M'manga, PhD Researcher, Bournemouth University. Fern Barrow, Poole BH12 5BB. ammanga@bournemouth.ac.uk

Name, position and contact details of supervisor: Dr Shamal Faily, Senior Lecturer (Sci-Tech), PhD Researcher, Bournemouth University. Fern Barrow, Poole BH12 5BB. sfaily@bournemouth.ac.uk

Please tick the appropriate boxes	***Yes***	***No***
Taking Part:		
I have read and understood the Project Participant Information Sheet	☐	☐
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 are processed and become anonymous, so my identity cannot be.	☐	☐
Should I not wish to answer any particular question(s), I am free to decline.	☐	☐
I understand that the interview will be digitally recorded (audio) and then transcribed.	☐	☐
I agree to take part in the project.	☐	☐
Use of the information I provide for this project only:		
I understand my personal details such as name and organisation will not be revealed to people outside this project.	☐	☐
I understand that my words may be quoted anonymously in publications, reports, web pages and other research outputs.	☐	☐
I understand that I will not be identified from quotations in publications.	☐	☐
Use of the information I provide beyond this project:		
I understand that the anonymised transcript from the interview will be deposited in Bournemouth University's Online Research Data Repository.	☐	☐
I understand that the anonymised information given in this interview may be used by the research team to support other research projects in the future, including future publications, reports or presentations	☐	☐

_____ _____ _____

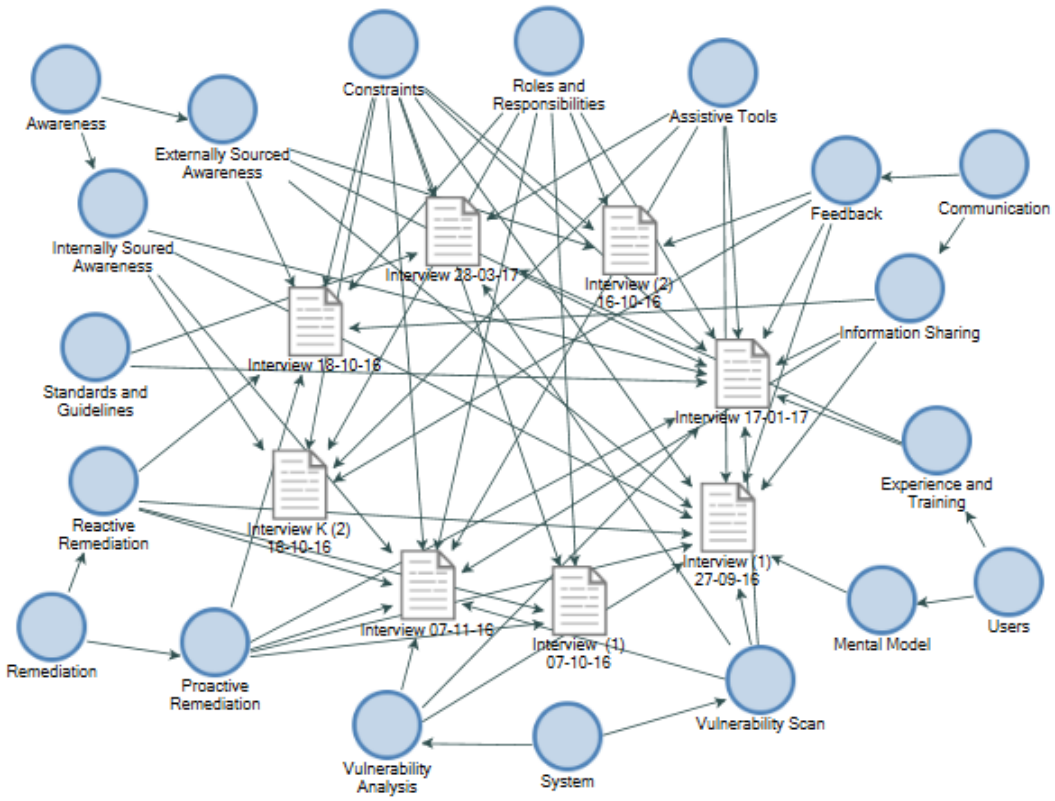
Name of Participant Date Signature

_____ _____ _____

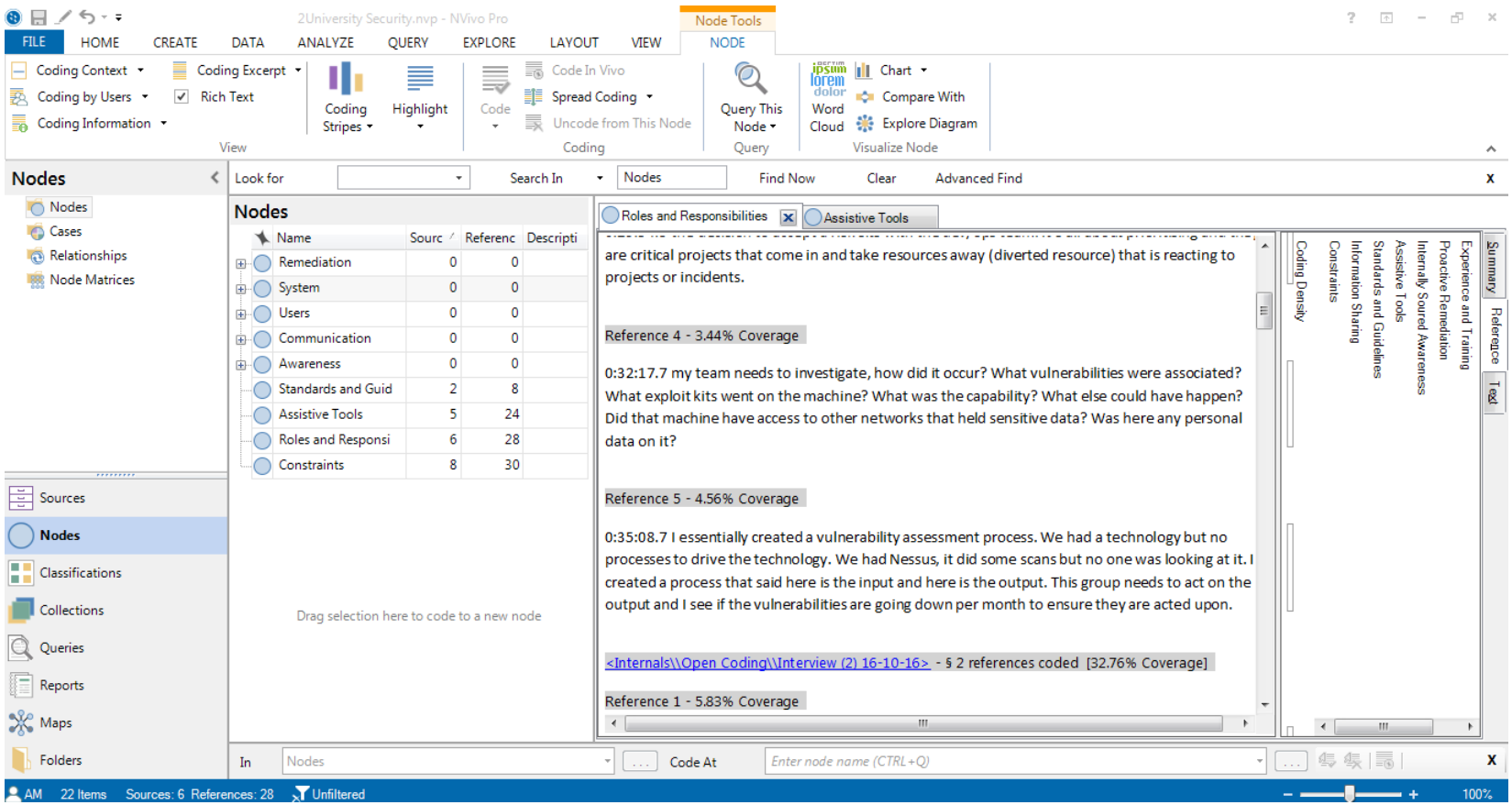
Name of Researcher Date Signature

This form should be signed and dated by all parties after the participant receives a copy of the participant information sheet and any other written information provided to the participants. A copy of the signed and dated participant agreement form should be kept with the project's main documents which must be kept in a secure location.

.1.4 NVivo - Interview to theme relationships



.1.5 NVivo - Grounded Theory coding



.1.6 Sample participant responses in Japanese/Katakana

問 必要情報の評価　例：意思決定に関連する情報および不必要な情報は何か？	問 情報調査　例：追加意思決定情報の発信元はどこか？	問 限られた情報での分析　例：意思決定に影響を及ぼす可能性がある未確認状態の重要情報とは何か？	問 選択肢の創出および分析　例：あなたが識別しうる、他の意思決定の選択肢とは何か？	問 選択肢の妥当性確認　例：仮説の欠陥はどこか？
必要な情報：情報セキュリティ方針が承認している内容の詳細 不必要な情報：期限が迫っている点	事業部長 情報セキュリティアナリスト	情報セキュリティ方針が定めているその他の伝送方法 代替手段の使用している暗号化方式などの安全性	代替手段の使用についての可否確認	必ずしも実施可能ではない点
選択可能な情報選択手段とそれらのコスト、リスク等特性 伝達対象の情報の機密性の高さ 情報伝達の緊急性	両社の情報伝達を行いたい部署 両社の情報伝達を実現する手段を提供する部署	攻撃者の動向	契約書等の重要な文書であれば、封緘し人が持ち運ぶ	輸送中に紛失する
必要：情報セキュリティ方針	追加意思決定情報発信元：暗号転送ウェブサイトの仕様、セキュアなメール送信方法を紹介するサイト	暗号転送ウェブサイトの安全性、セキュアなメールの送信方法	ウェブ、メール以外の選択肢としてFAX、新幹線での運搬	FAXの安全性未確認、新幹線で運べる人員の可否
必要な情報：ビジネスパートナーの情報セキュリティ方針。情報送信期限。	ビジネスパートナー及び自社システム部門	電子メールおよびオンライン上の暗号転送ウェブサイトの危険性	緊急機密情報送付期限の延期について交渉する。	分かりません。
緊急性、情報の機密性、部長のやりたいこと、やりたくないこと	部長の上司、ビジネスパートナー	ビジネスパートナーの意思	送らない	送らなければならないという固定観念
緊急度合い（2-3時間以内でよいのか）。情報の量（TB、GB、MB、B）。送信する機密情報の形(word、excel、pdf、jpeg)、使用用途（再加工、印刷、展示、念写）、送信先会社の信頼度(社会的信頼度)	担当部署	送信会社の信頼性、緊急度合い、使用用途	ハンドキャリー、TV会議、代替情報の提示（詳細をはしょったデータ）	時間的余裕がない場合（５分）、アホみたいな量のデータ（12.1兆桁の円周率結果等）
必要情報：過去の漏洩の事例・セキュリティ向上手段の調査結果	脆弱性共有機関やセキュリティ専門企業	最近見つかった脆弱性など	物理的な伝送	ゼロデイ攻撃
送信方法、送信方法のセキュリティレベル・セキュリティリスク	JPCERT	不明	時間的制約を排除し、評価軸を見直す	物理的な輸送が検討候補にない
関連情報：緊急機密情報を送る必要がある、承認された安全性の高い暗号化通信チャネルは無い 不必要：電子メール経由の送信またはオンライン上の暗号転送ウェブサイトなど	事業部長もしくは大阪の会社の担当者	承認された安全性の高い暗号化通信チャネルは無い	大阪の会社が使用する情報セキュリティツールの内容、他メディア（音声等）での搬送可否、物理的に搬送することも踏まえ送付に必要な猶予日数	承認された暗号化通信チャネルは所有していなくても他の暗号化通信チャネルを持っている可能性がある。緊急かどうか不明。オンラインで送る必要があるかどうか不明。
送付しないという選択肢は無いため、各送付方法と要する時間、情報漏洩の可能性のみが必要	電子メール、暗号転送ウェブサイト等のキャリア	所属組織の情報セキュリティ方針が安全であるか否か	飛行機、新幹線等でハンドキャリーする	所属組織の情報セキュリティ方針が安全であるという仮説
必要：ビジネスパートナーのネットワーク、位置、緊急機密情報の緊急度、安全性が確保できる通信経路の有無 不必要：暗号転送webサイトの問題	ビジネスパートナー、自社のインフラ管理部門	メールの通信の安全確保状況	バイク便、書留での情報伝達。外部のコンサルに依頼する	データを途中で盗聴される、盗難される可能性がある
大阪のパートナーへのヒアリングの情報	事業部長からの状況ヒアリング	利用されているソリューションの情報、NDAの締結	許可しない、代替策の提案（自社の方針に合致したオンラインソリューション、または訪問）	情報漏洩のリスクがある
相手企業が受け取れる方法かどうか	メールソフト開発元やウェブサイトのQAなど	暗号化方式に脆弱性はないか	バイク便などの宅配方法の選択	時間、コスト、情報漏洩の危険性

.2 Case study Data

Appendix .2 presents further information on findings from the case study conducted in Chapter 8.

The appendix first present a full description of the persona Mary Hughes in Appendix .2.1, who represents an archetypical counsellor used for eliciting the secure data handling policy's requirements in the study. Appendix .2.2 is the secure data handling policy designed by implementing the RBDM design guidelines.

.2.1 Case study - Persona

Mary Hughes - Counsellor [1]

Activities

Mary is a volunteer at a local charity offering counselling services to traumatised parents. Her role with the charity includes assessing referral, offering the clients emotional and practical support, keeping track of the client's progression and maintaining client files.

Skills

Mary trained as a counsellor and has a level 4 Diploma in counselling and psychotherapy. She is also a member of the British Association of Counselling and Psychotherapy (BACP) where she receives additional guidance. Listening to her clients' cases and taking notes have helped improve her skills in these areas.

Attitudes

Mary believes her job requires an open, empathetic, and non-judgemental approach to gaining the client's trust. Having no preconceived assumptions on the clients' situation is important and this is greatly aided by keeping a distance from the clients' social media accounts.

Mary is aware that her line of work requires strict adherence to rules and confidentiality. To unwind from stressful client sessions, she confides in a buddy assigned by the charity or her clinical supervisor.

From a personal perspective, Mary understands the importance of self-care and continuous professional development.

Aptitudes

Mary has the ability to listen attentively and provide guidance. She understands that her clients are vulnerable and require patience.

Motivations

Due to the nature of the work, distressful and shocking stories from the clients are un-

[1] Photo by Charisse Kenion on Unsplash

fortunately all too common; however, Mary is motivated by the clients improving mental state and the impact it has on their family life.

.2.2 Case study - Policy

Secure Client Data Handling Policy

The aim of this policy is to secure client data by focusing on possible decision and actions that could be made relating to the access, storage processing, and dissemination of client data.

To this effect, client data is considered with regards but not limited to the following security risks:

- Confidentiality
- Availability
- Integrity

1. Assets
Assets are artefacts belonging to Samaritans that hold client data and must be treated in a secure manner. Assets are, but not limited to:

- Paper-based (hard copy) forms and files
- Mobiles phones
- Computers
- Filing cabinets
- Digital storage devices

2. Counsellors
To ensure the secure handling of clients' data and confidential provision of counselling services:

- The councillors shall be a permanent employee or contracted volunteer at Samaritans.

- Permanent counsellors shall have a minimum of a level 4 Diploma in counselling and psychotherapy, while trainees shall at a minimum be in the final year towards achieving the level four Diploma in counselling and psychotherapy.
- Counsellors shall be registered with the British Association for Counselling and Psychotherapy (BACP) or similar professional bodies.
- Samaritans shall have Level 6 qualified clinical supervisors assigned to permanent councillors, or expect Colleges to assign supervisors to volunteering trainees (see Counselling policy).
- Counsellors shall read, sign, and have knowledge of related security and privacy policies and guidelines.
- Counsellors shall commit to regular refreshers on related security and privacy policies and guidelines.
- Counsellors shall have up to date DBS checks and have their own insurance from a reputable insurance provider.

3. Information sourcing and sharing

During your time with Samaritans, there may be situations where you may be required to seek or share information in order to make informed decisions on clients and their data. Information may only be sourced from, or shared with the following - authorised by Samaritans:

- Samaritans policies and guidelines
  These include, but not limited to the Counselling, Confidentiality, Privacy, Lone working, and Safeguarding policies and guidelines.
- Assigned clinical supervisor
  Information passed to the clinical supervisor shall be of a non-personal identifiable form.
- Assigned buddy
  Buddies are assigned and are not based on colleague availability.
- The Manager
  Information passed to the manager shall be kept confidential between the manager and the counsellor unless otherwise stated in relevant Samaritan policies or procedures.

- The Police
  Information shall be shared with Police in accordance with safeguarding procedures.
- The Multi-Agency Safeguarding Hub (MASH)
  Information shall be shared with MASH in accordance with safeguarding procedures.
- Relevant authorities
  Information shall be shared with relevant authorities such as a General practitioner (GP) in accordance with safeguarding procedures.

Sourcing and sharing information from, or with any other source such as social media is strictly prohibited. All actions and decisions shall be based on facts as presented by the client unless there is a clear or probable violation of the law.

4. Accessing and Storing Data

To ensure the secure storage and restricted access to client data, counsellors shall:

- Store paper-based files and folders in locked cabinets
- Lock filing cabinets
- Lock doors when offices are not in use
- Place phones in secure areas
- Password-protect computers
- Delete client messages in phones on a regular basis
- Destroy dated data as stipulated by guidelines in the privacy policy
- Maintain a clean desk policy

5. Data Availability

To ensure the continuous availability of client data enabling the fulfilment of the charity's services, counsellors shall:

- Conduct regular data backups
- Store backup devices in secure alternative locations

6. Disseminating Data

To preserve client confidentiality:

- Client data shall be disseminated to authorised parties and in a non-personal identifiable manner unless otherwise stated by relevant policies and guidelines.