A Normative Decision Making Model for Cyber Security

Andrew M'manga, Shamal Faily, and John McAlaney

Bournemouth University, Poole, UK

Chris Williams

Defence Science and Technology Laboratory, Porton Down, UK and

Youki Kadobayashi and Daisuke Miyamoto

Nara Institute of Science and Technology, Ikoma, Japan

Abstract

Purpose - The purpose of this paper was to investigate security decision making during risk and uncertain conditions and to propose a normative model capable of tracing the decision rationale.

Design/methodology/approach – The proposed risk rationalisation model is grounded in literature and studies on security analysts' activities. The model design was inspired by established awareness models including Situation Awareness and Observe Orient Decide Act (OODA). Model validated was conducted using cognitive walkthroughs with security analysts.

Findings – The results indicate that the model may adequately be used to elicit the rationale or provide traceability for security decision making. The results also illustrate how the model may be applied to facilitate design for security decision makers.

Research limitations/implications – The proof of concept is based on a hypothetical risk scenario. Further studies could investigate the model's application in actual scenarios.

Originality/value – The paper proposes a novel approach to tracing the rationale behind security decision making during risk and uncertain conditions. The research also illustrates techniques for adapting decision making models to inform system design.

Keywords Normative, Decision-making, Rationalisation, Awareness, Uncertainty, Perception, Risk, Security

Paper type Research paper

1. Introduction

Security analysts regularly face the challenge of justifying decisions made under risk and uncertain conditions. While uncertainty stems from various sources such as dynamic conditions and information limitations, complications in decision making also arise because risk stems from multiple factors, rather than a single root cause (Hoffman et al., 2017). Analysts aim at identifying the best possible option, given the limited information as few decisions are actually made with absolute certainty (Huber, 2014).

Information limitations exemplify the difference between optimising in rational decision making where all options for a decision are known and satisficing in bounded rationality driven decision making where limited options are known (Simon, 1972). When decision making under risk and uncertainty is unsuccessful, the post-incident privilege of hindsight availed to others fails to portray the complexity of decision making in action. Equally, value is lost when decision making knowledge gained from those experienced remains tacit and incommunicable.

To facilitate the transparent understanding of security decision making, we present a conceptual model providing systematic traceability to risk rationalisation. We validate the model using cognitive walkthroughs and illustrate its application in a study where analysts' views on automating aspects of risk rationalisation during security analysis were elicited. This paper is an extended version of earlier work presented in M'manga et al., (2018).

2. Related work

Decision making research typically follows the normative or descriptive approach. Normative approaches model how decisions should be made; descriptive approaches understand how decisions are actually made. The normative approach's usefulness may be seen in its ability in providing theoretical adequacy for rational choice, whereas the descriptive approach's usefulness may be seen through empirical validity by uncovering insight in decision making (Bell et al., 1988). An alternative approach is to categorise decision making research based on the study environment. This may be the lab-based approach where studies are conducted in controlled environments and data collection is determined by predefined tests (MacKenzie 2013), or the naturalistic approach where studies are conducted in real settings and data collection is based on the observation of actual events (Klein, 2008). The differences in approaches do not imply that one is better than the other, but that each is suitable based on research objectives.

Descriptive research on expert decision making during risk and uncertainty focusses on context-specific decision making. This has been led by Klein's (1999) research on naturalistic decision making, where he identified that during uncertainty, experienced firefighters use situational familiarity to make quick decisions as opposed to

weighing all available alternatives. Similar work by Wong and his colleagues has examined how criminal intelligence analysts think (Wong, 2014: Wong and Kodagoda, 2015). They suggest that analysts flow from fluidity to rigour during decision making which is explained as moving from a loose story to account for identified data, to a formal rigorous and defensible argument. Hibshi et al., (2016) explores techniques taken by security experts as they transition through levels of situation awareness to identify security requirements. They identify that experts seem to skip some stages of situation awareness and attribute this to situation familiarity based on experience.

The movement from ambiguity to certainty is the common point in the literature, however, much is still required to understand the rationale behind decision making. Normative models are particularity useful for this as they act as blueprints upon which sensemaking may be traced and communicated. Early work by Rasmussen (1974) on the Decision ladder template has played a key role in identifying the generic categories of activity in decision making, similarly, Boyd (1996) and Endsley (1995) played key roles in formalising the awareness steps leading to awareness. Regrettably, normative approaches are usually too high-level and generalised, rendering them incapable of providing low-level context-specific guidance.

3. Model Design

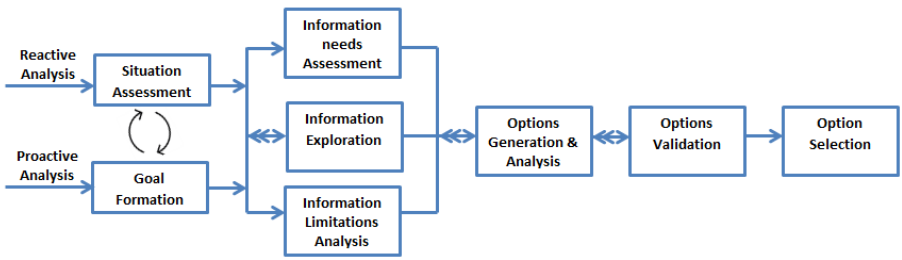

Figure 1: Risk Rationalisation Flow

The model builds on our findings in M'manga et al., (2017), where we identified factors influencing risk interpretation and conflicts to security decisions, and lessons learned from the literature on awareness and analysts' decision making activities (Werlinger et al. 2010; D'Amico et al. 2005). The model was formalised systematically using OODA (Boyd, 1996).

The normative model consists of eight steps to risk rationalisation and contains two complementary elements; the Flow and Actions collectively referred to as the risk rationalisation process (RRP). The first element is a risk rationalisation flow (RRF) highlighting cognitive sequences and iterations during risk rationalisation. Illustrated in Figure 1, RRF indicates two alternative starting points; Reactive risk analysis beginning with *Situation assessment* and continues to *Goal formation,* while Proactive risk analysis has an inverse flow of beginning with *Goal formation* and

continuing to *Situation assessment*. The difference is based on the understanding that incidents precede response strategy in reactive analysis. Therefore, situation assessment begins before goals are formed, while the inverse is true in proactive analysis where goals are set beforehand. The second phase of RRF consists of the three information related steps, these are; *Information needs assessment, Information exploration, and Information limitations analysis.* Their adjacent positioning in Figure 1 indicates that the steps may overlap and occur in varying order. The final three steps occurring in sequence relate to options. These are; *Options generation and analysis*, *Option validation*, and *Option selection.* Risk rationalisation is an iterative process; this is illustrated in RRF by the reverse arrows at each point of possible iteration.

The second element of RRP consists of the risk rationalisation actions illustrated in Figure 2. The actions address the lack of low-level 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 extended as the knowledge of knowledge (what one knows about their thinking), and the regulation of knowledge (how one uses that knowledge to regulate thinking) (Schraw and Moshman, 1995). For instance, to understand the rationale behind the characterisation of a situation, the question "*how may a situation be understood*?" is posed. The questions are 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 putting 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. We detail the eight RRP steps below.

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: recognition through situation familiarity and the knowledge of normal.
- Knowledge of evidence: recognising information affordances in an environment to achieve greater awareness.
- Situational time-line: recognising whether a situation is static or evolving, current or elapsed.
- Data correlation: recognising data correlation needs to achieve greater awareness.

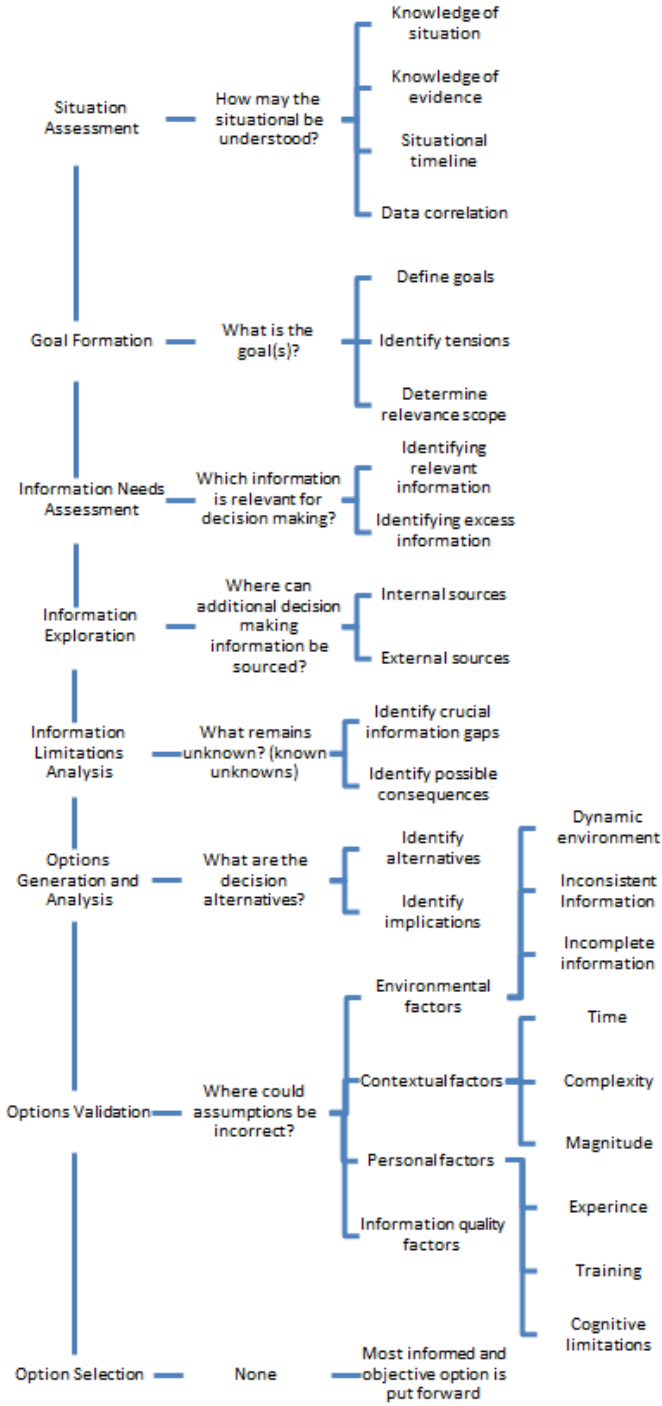

Figure 2: Risk Rationalisation Actions

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 acts as a minimum level for the continued pursuit of a goal. For example, analysts interviewed in M'manga et al., (2017) 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 unnecessary. In other words, the relevance scope for pursuing the products risk was below minimum.

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*. An example would be procedures taken in identifying false positives during an incident.

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 information sources is subject to available time. Information sources may be subject matter experts within an analysts' environment e.g. legal officer, public relations manager, or external expertise such as CERT advisory (Computer Emergency Response Teams).

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. For example, it would greatly aid an analyst to acknowledge that an attack vector has been identified although the motive and capabilities remain unknown. Knowledge of the motive could hint at the possibility of follow-up attacks leading to better preparedness (Rashid et al., 2016).

3.6. Options generation and analysis

Options generation and analysis is the first of two steps corresponding to OODA's Decide. Based on the cumulative understanding from the previous steps, the decision maker identifies possible options for decision formulation and their implications. For example, an analyst's response to a data breach could be to refrain from disclosing the breach, even though data protection regulations advise otherwise. The aim of the step is to identify and understand the reasoning behind options considered by the decision maker. At this point, limited understanding may inadvertently lead to the first form of meta-risk, which is risk resulting from risk response e.g. increased threat exposure.

3.7. Options validation

Options validation focusses on uncertainty by verifying if there were elements of uncertainty hindering the decision making process and how it was managed. Evaluating one's own decision is no easy task; the failure to validate an option introduces a second form of meta-risk, which is the risk of risk understanding.
To provide a comprehensive understanding of uncertainty, we categorise it to the following four groups:

- ***Environmental factors*:** dynamic environments, inconsistent or incomplete information from the environment.
- ***Contextual factors*:** time limitations, situation complexity or magnitude.
- ***Personal factors*:** experience, training and cognitive limitations.
- ***Information factors*:** accurate, current, relevant specific, understandable, comprehensive, unbiased and comparable (Wang et al., 2005).

3.8. Option selection

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

4. Model flow validation

The model was validated using cognitive walkthroughs (Rieman et al., 1995) with three security analysts from the UK (P1 -3). The three validated the model's logic flow and not the tracing of risk rationalisation. P1 and P2 worked as part of a cyber security team monitoring events within their organisation and possessed 1-3 years' professional experience in security. P3 worked for a counter-terrorism and intelligence unit and possessed over 24 years of relevant experience.

Each participant was provided with a copy of RRP and given a brief tutorial on its use. Participants were then presented with a scenario about a hypothetical data breach that incorporated tensions related to possible decisions and uncertainty due to insufficient information. 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 participants were asked to compare the model with decisions they would make in the scenario. Additionally, P3 ran a second validation scenario, based on his experience in counter-terrorism. Each walkthrough took approximately 40 minutes, and the participants presented their critiques of the model's logic. Opinions were divided on whether *Option validation* was an independent step or a part of *Option generation and analysis*. We concluded that it remains an independent step to cater for understanding inexperienced decision makers lacking the ability to generate and validate decision alternatives consecutively.

5. Model Application

To demonstrate the application of RRP, a study was conducted with information systems (IS) personnel from a variety of organisations in Japan with the aim of eliciting their views on automating aspects of risk rationalisation during security analysis. Under real settings, the understanding gleaned would form the basis for nuanced security automation requirements that are grounded in user understanding as opposed to default automation for all.

The findings do not aim to present statistical accuracy as we did not work with a representative sample size. Rather, the aim is to illustrate how RRP may be applied in facilitating understanding and designing for security decision makers (proof of concept). Demographic factors such as experience, security roles and industry could be used in representative and longitudinal studies to uncover decision rationalisation norms and deviations thereof. Findings could hint at hidden biases and suggest training and design requirements.

5.1. Participants

As illustrated in Figure 3, the nine participants were part of a group undertaking a training programme in cyber security. Two of the nine worked in security-specific roles; while the rest had security as a part of their other IS responsibilities. The participants had work experience ranging from one to ten years, four had a maximum of two years (referred to as novices) and the remaining five had a minimum of six years (referred to as experienced).

5.2. Data collection

Like the validation exercise (Section 4), participants were trained on RRP and provided with a cybersecurity decision making scenario containing elements of risk and uncertainty. Participants were then asked to indicate whether or not they would use automation during the different step of risk rationalisation during security analysis. We sought to elicit the participants' general opinion, not one driven by existing tool capabilities. The steps considered were from *situation assessment* to

options validation. *Option selection* was intentionally omitted as the objective was to automate with the human as the final decision maker (human-in-the-loop).

5.2.1. Scenario

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?

Industry	Role	Experience (years)
IT	IS Support	1
Electricity	CSSIRT Analyst	1
Printing	CSSIRT Analyst	1
Electricity	IS Support	2
Electricity	IS Support	6
IT	IS Support	8
Oil	IS Support	9
IT & Communication	Engineer	9
Chemical	System Operations	10

Figure 3: Study participants

5.3. Findings

5.3.1. All respondents

Illustrate in Figure 4, the first part of the findings represents all respondents (novices and experienced) as one group. *Situation assessment* was the most recommended for automation with seven of the nine participants selecting to automate. Participants' comments for the choice included:

> "Systems have a better understanding of network traffic and monitoring for signs of risk."

> "It would be possible to issue alerts at the point of anomaly detection."

Information needs assessment had the lowest outcome with none of the participants recommending it, seconded by *Option validation* with one recommendation. Participants' comments for not selecting *Information needs assessment* included:

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

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

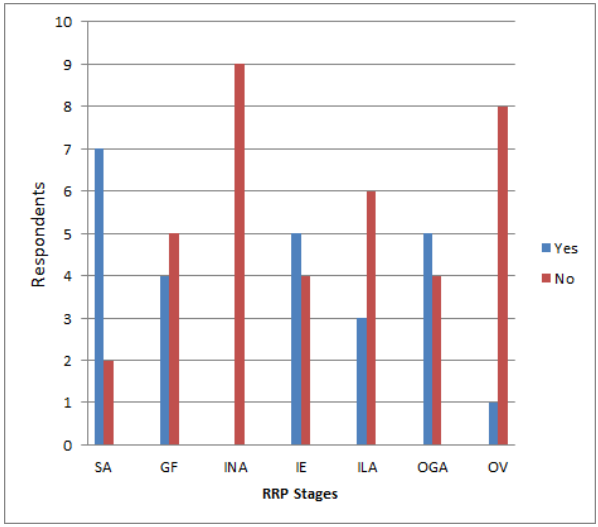

Figure 4: Automating security analysis (all respondents)

5.3.2. Novice versus Novices

Illustrate in Figure 5, the second part of analysing the findings aimed at identifying if there were visible differences in the novice versus experienced view.

As an overall, the results indicate that the experienced where lesser inclined to automate. We could speculate that this reflects a lack of self-belief and tool dependency by the novices. Significant differences were observed under *Information limitations analysis* and *Options validation* where none of the experienced chose to automate, in contrast to the larger number of novices who chose to automate. Reasons for choosing not to automate the two steps included:

"New information might emerge continuously; thus, automation would be impossible."

"It would be possible to establish frameworks, but it cannot be automated."

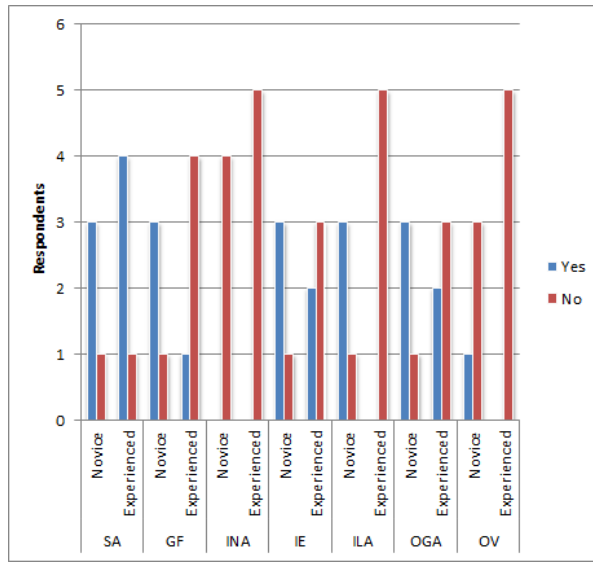

Figure 5: Automating security analysis (novice vs experienced)

As explained above, we do not aim to draw too much from the findings due to the limited sample size, however, the clear difference in the novice versus the experienced choices indicates the soundness in the application of RRP as a nuanced view to risk rationalisation.

6. Conclusion

This work presented a normative model for rationalising security analysts' decision making. The purpose of the model is not to propose a new approach to decision making, but rather to propose a systematic approach capable of communicating and providing traceability to the rationale behind security decision making during risk and uncertainty. To address this, we considered the shortfalls presented in descriptive approaches which usually provide no explanation for expert judgement and the shortfalls in normative approaches which are usually too high level to derive contextual meaning.

We believe there are three benefits from the use of this model. First, the model is designed as a series of steps, cognitive questions and procedures that may be used as a blueprint by stakeholders unfamiliar with risk analysis procedures in security e.g. proactive or reactive analysis. Second, the model may be used in training analysts be identifying gaps in their reasoning when compared to model steps. Finally, the model may be used as a basis for eliciting design requirements that would facilitate decision making about risk through the identification of crucial areas of risk rationalisation in security.

The model places emphasis on validation and the consideration of uncertainty by highlighting the iterative nature of decision flows, presenting an options validation step, and the consideration of meta-risk in two forms (risk of understanding and risk of response). We believe that the model complements existing decision making and awareness approaches lacking a focus on risk and uncertainty.

The case study presented acts as a proof of concept on the application of the model. It illustrated how the rationalisation steps in security analysis could be considered for automation based on user requirements and understanding. We believe this is a sound approach for leveraging human and system capabilities for decision making about security risk.

7. Acknowledgement

The research was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RBDM, with the initial collaborative meeting between UK/Japan researchers facilitated by support from the Great Britain Sasakawa Foundation. We are also grateful to DSTL for their sponsorship of this work.

8. References

Bell, D. E., Raiffa, H., and Tversky, A. (1988), *Decision making: Descriptive, normative, and prescriptive interactions,* Cambridge University Press.

Boyd, J. R. (1996), "The essence of winning and losing". *Unpublished lecture notes*, Vol. 12, No. 23, pp. 123–125.

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". *In*: *Proceedings of the human factors and ergonomics society annual meeting*. SAGE Publications Sage CA: Los Angeles, CA, pp. 229–233.

Endsley, M. R. (1995), "Toward a theory of situation awareness in dynamic systems". *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 37, No. 1, pp. 32–64.

Hibshi, H., Breaux, T. D., Riaz, M., and Williams, L. (2016). "A grounded analysis of experts' decision-making during security assessments". *Journal of Cybersecurity*, Vol. 2 No. 2, pp. 147–163.

Hoffman, R. R., Mueller, S. T., and Klein, G. (2017), "Explaining Explanation, Part 2: Empirical Foundations". *IEEE Intelligent Systems*, Vol. 32, No. 4, pp.78–86.

Huber, O. (2014), "Complex problem solving as multistage decision making". *In*: P. A. Frensch, & J. Funke (Eds.), *Complex problem solving: The European perspective,* Lawrence Erlbaum Associates, Hillsdale NJ, pp. 151–173.

Klein, G. (1999), *Sources of power: How people make decisions*. MIT press.

Klein, G. (2008), "Naturalistic decision making", *Human Factors: The Journal of the Human Factors and Ergonomics Society*, Vol. 50 No. 3, pp. 456–460.

MacKenzie, I. S. (2013), *Human-computer interaction: an empirical research perspective*. Morgan Kaufmann, Amsterdam.

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), Santa Clara, USA,12-14 July 2017, Usenix Association.*

M'manga, A., Faily, S., McAlaney, J., and Williams, C. (2018), Rationalising Decision Making about Risk: A Normative Approach, *In Proceedings of the twelfth International Symposium on Human Aspects of Information Security & Assurance (*HAISA), Dundee UK, 29-31 August 2018, University of Plymouth, pp. 263-271.

Rashid, A., Naqvi, S. A. A., Ramdhany, R., Edwards, M., Chitchyan, R., and Babar, M. A. (2016), "Discovering 'unknown known' security requirements", *In 38th International Conference on Software Engineering,* ACM Press, pp. 866–876.

Rasmussen, J. (1974), *The human data processor as a system component. Bits and pieces of a model*. Roskilde, Denmark: Danish Atomic Energy Commission. No. Risø-M-1722.

Rieman, J., Franzke, M., and Redmiles, D. (1995), "Usability evaluation with the cognitive walkthrough". *In Conference companion on Human factors in computing systems,* ACM, pp. 387–388.

Schraw, G. and Moshman, D. (1995), "Metacognitive theories". *Educational Psychology Review*, Vol. 7 No. 4, pp. 351–371.

Simon, H. A. (1972), "Theories of bounded rationality", *Decision and organization*, Vol.1 No. 1, pp. 161–176.

Wang, Y. R., Pierce, E. M., Madnik, S. E., Fisher, C. W., and Zwass, V. (2005), *Information quality*. Armonk, N.Y. ; London, England, M.E. Sharpe.

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*, Vol. 18 No. 1, pp 26–42.

Wong, B. L. W. (2014), "How Analysts Think (?): Early Observations", In Joint Intelligence and Security Informatics Conference, IEEE, pp. 296–299.

Wong, B. L. W. and Kodagoda, N. (2015), "How Analysts Think: Inference Making Strategies", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 59 No. 1, pp. 269–273.