Rationalising decision-making about risk: a normative approach.

M'MANGA, A., FAILY, S., MCALANEY, J. and WILLIAMS, C.

2018

Rationalising Decision Making about Risk: A Normative Approach

A. M'manga[1], S. Faily[1], J. McAlaney[1] C. Williams[2]

[1]Bournemouth University, Poole, United Kingdom
[2]Defence Science and Technology Laboratory, Porton Down, United Kingdom
e-mail: {ammanga, sfaily, jmcalaney}@bournemouth.ac.uk;
cwilliams@mail.dstl.gov.uk

Abstract

Techniques for determining and applying security decisions typically follow risk-based analytical approaches where alternative options are put forward and weighed in accordance to risk severity metrics based on goals and context. The reasoning or validity behind decision making can, however, prove difficult to determine in conditions characterised by uncertainty stemming from environments with insufficient or incoherent information. This paper approaches the problem by proposing a conceptual model that provides security decision making traceability through auditing decision makers' rationalisation of risk. Additionally, the model highlights the role metacognition plays in identifying and understanding information affordances used for decision making.

Keywords

Normative decision-making, Context-awareness, Uncertainty, Risk-perception, Security

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; few decisions are actually made with absolute certainty (Huber, 2014) reflecting the difference between optimising in rational decision making, and satisficing in bounded rationality (Simon, 1972) driven, naturalistic decision making. When decision making under risk and uncertainty fails, the post-incident privilege of hindsight available to others fails to portray the complexity of decision making in action. Similarly, value is lost when decision making knowledge gained remains tacit and cannot be communicated. To address these problems, the research aimed at formulating a systematic approach for providing traceability to the rationale behind security decision making during risk and uncertainty.

2 Related work

Decision making research has typically followed 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 view is the categorisation of 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, 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 they identified that during uncertainty, experienced firefighters use situational familiarity to make quick decisions as opposed to weighing all available options. In the same line, Wong presents a research series on how criminal intelligence analysts think (Wong, 2014: Wong and Kodagoda, 2015; Gerber et al., 2016). Among the various strategies identified, they suggest that during the absence of clear facts, a leap of faith occurs between intuition and insight that allows the decision makers to reach a preliminary comprehension of a situation. Hibshi et al., (2014) 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 this may be attributed to situation familiarity based on experience.

What is common in the above literature is the realisation that experts take leaps in decision making. While these findings are insightful, they do little in providing traceability to the rationale behind decision making and this is where normative approaches are beneficial through the provision of 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, and similarly, Boyd (1996) and Endsley (1995) played key roles in formalising the awareness steps leading to decision making. Unfortunately, normative approaches are usually too high-level and generalised, rendering them incapable of providing low-level context-specific information.

3 Model Design

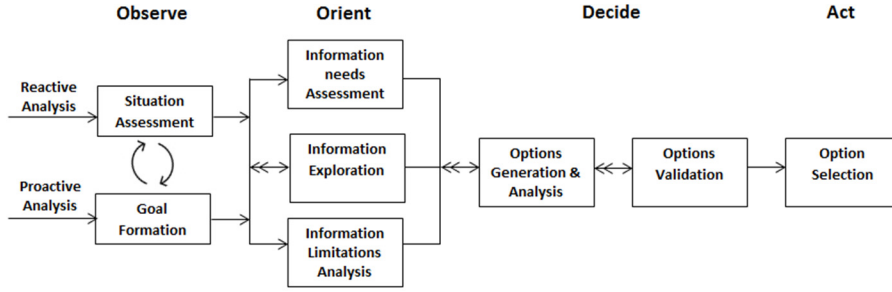

Figure 1: Risk Rationalisation Flow

We propose a normative model that provides traceability to security analysts' rationalisation of risk under uncertain conditions. The normative model builds on lessons learned from two studies with cyber security analysts and was formalised systematically using OODA (Boyd, 1996). The first study (M'manga et al., 2017) was conducted with 10 analysts from three different organisations with the aim of investigating factors influencing analysts' interpretation of risk during proactive risk analysis (vulnerability assessment and goal conflicts). Findings included risk interpretation influencers and risk analysis workflows. Building on the first, the second study (M'manga et al., 2018) was conducted with 30 analysts from 11 different sectors, it aimed at investigating risk rationalisation steps taken during reactive risk analysis (incidence response).

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; the Reactive risk analysis beginning with *Situation assessment* and continues to *Goal formation,* or the Proactive risk analysis that takes the inverse approach of beginning with *Goal formation* and continues 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 for proactive analysis. The second phase of RRF consists of the three cognitive actives; *Information needs assessment, Information exploration and Information limitations analysis.* The adjacent illustration indicates that the steps may overlap and occur in various orders. *Options generation and analysis*, *Option validation*, and *Option selection* form the final three steps and they occur in sequence. Risk rationalisation is an iterative process and this is illustrated in RRF by the double back arrows at each point of possible iteration.

The second element of the normative model consists of the risk rationalisation actions (Figure 2). The actions address the lack of low-level detail in normative models by providing context-oriented meta-cognitive questions at each rationalisation step.

Metacognition is defined as awareness or analysis of one's own thinking processes, and this may further be explained as the knowledge of knowledge (what one knows about cognition), or the regulation of knowledge (how one uses that knowledge to regulate cognition) (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 presented. The risk rationalisation actions take this a step further by defining sub-procedures clarifying the questions which could, in this case, be through *data correlation*, explained as the putting together of disparate data sets to derive meaning. By using the steps, meta-cognitive questions and sub-procedures, our normative approach 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 sub-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 available or required data correlation needs to achieve greater awareness.

3.2 Goal formation

Goal formation is the second step 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 we 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.

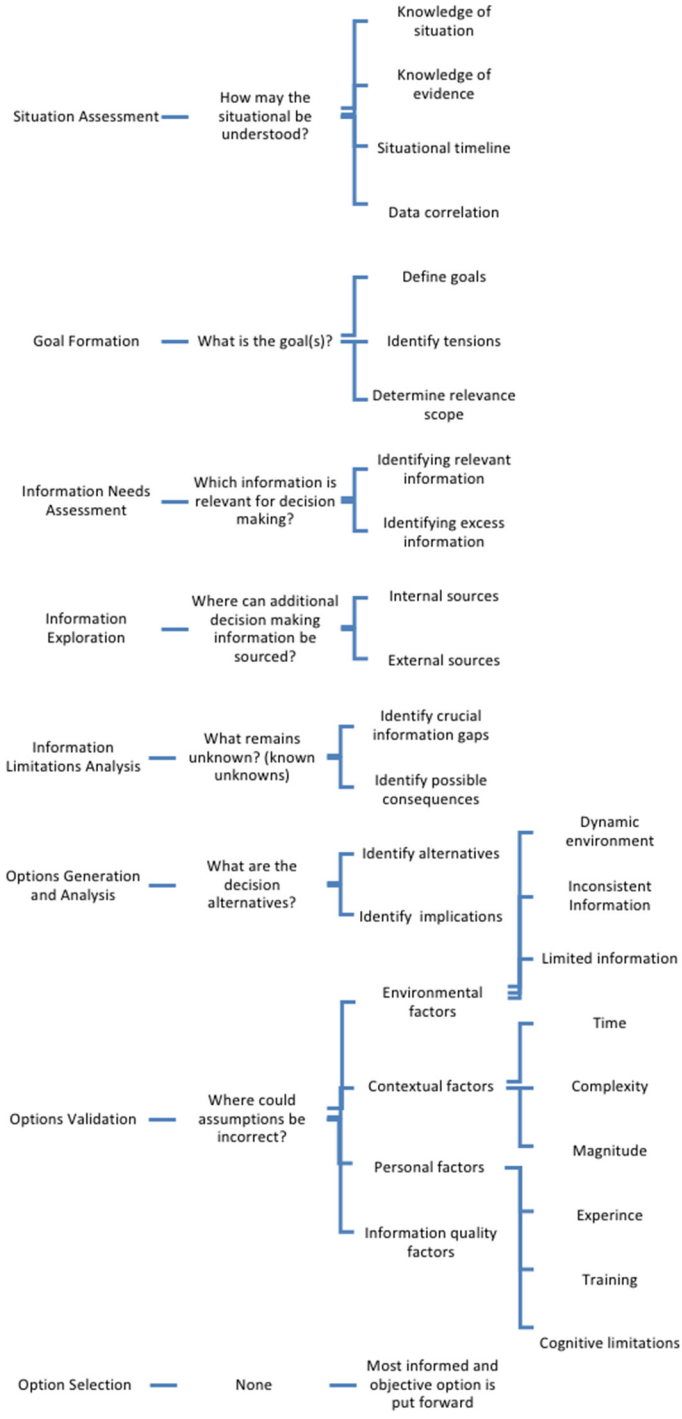

Figure 2: Risk Rationalisation Actions

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 to decision making and excess information for filtering. 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*. Typical examples are the procedures taken to identify false positives.

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

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 remains unknown. Knowledge of the motive could hint at the possibility of a 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, poor understanding may inadvertently lead to meta-risk; 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. To simplify the understanding and expression of uncertainty, the meta-cognitive question posed is; where could assumptions be incorrect? Validating one's own actions is by no means an easy task. Failure at the stage introduces a second form of meta-risk,

which is the risk of risk understanding due to uncertainty. We categorise the elements of uncertainty into four groups:

- ***Environmental factors*:** dynamic environments, inconsistent or limited 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 validation

The model was validated using cognitive walkthroughs (Rieman et al., 1995) with three security analysts (P1 -3). The three validated the model's logic flow, and not its ability to support 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 as part of 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, and taking into account that some of the breached data was already on the Internet. The participants were asked to compare the model with decisions they would make in the scenario. In addition, P3 run 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 Conclusion and future work

This paper presented a normative model for rationalising analysts' decision making about risk and uncertainty. The propose 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. The benefit and use of the model are in several folds. Firstly the model is designed as a series of steps, meta-cognitive questions and sub-procedures that may be used as a blueprint by stakeholders unfamiliar with risk analysis procedures in security such as the different approaches to proactive and reactive analysis. Second, the model may be used in training analysts be identifying gaps in their reasoning when compared to model steps. And third, the model may be used as a basis for eliciting design requirements that would facilitate decision making about risk through the identification of critical areas of risk rationalisation.

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 various forms. We believe that the model will complement existing decision making and awareness approaches lacking a focus on risk and uncertainty. For future work, we are investigating techniques to elicit design requirements for risk-based decision making, based on data collected using RRP.

6 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, pp123–125.

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, pp32–64.

Gerber, M., Wong, B. L. W., and Kodagoda, N. (2016), How Analysts Think: Intuition, Leap of Faith and Insight. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 60, No. 1, pp173–177.

Hibshi, H., Breaux, T., Riaz, M., and Williams, L. (2014), Towards a framework to measure security expertise in requirements analysis. *In*: *Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop,* pp146-155._

Hoffman, R. R., Mueller, S. T., and Klein, G. (2017), Explaining Explanation, Part 2: Empirical Foundations. *IEEE Intelligent Systems*, Vol. 32, No. 4, pp78–86.

Huber, O. (2014), Complex problem solving as multistage decision making. *In*: *Complex problem solving: The European perspective,* pp151–173.

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, pp456–460.

M'manga, A., Faily, S., McAlaney, J., and Williams, C. (2017), Folk Risk Analysis: Factors Influencing Security Analysts' Interpretation of Risk. *In*: *3rd Workshop on Security Information Workers 12-14 July 2017 Santa Clara, USA. Usenix Association.*

M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y., and Miyamoto, D. (2018), Eliciting Persona Characteristics for Risk Based Decision Making. *In*: *Proceedings of the 32nd International BCS Human Computer Interaction Conference*. BCS.

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, pp387–388.

Schraw, G. and Moshman, D. (1995), Metacognitive theories. *Educational Psychology Review*, Vol. 7, No. 4, pp351–371.

Simon, H. A. (1972), Theories of bounded rationality. *Decision and organization*, Vol.1, No. 1, pp161–176.

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.

Wong, B. L. W., 2014. How Analysts Think (?): Early Observations. *In*: IEEE, pp296–299.

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, pp269–273.