Editorial

The evolving cyber-threat landscape has given rise to new and increasingly potent attacks against organizations. Human attackers use sophisticated tools and techniques to disrupt and destroy cyber infrastructures, deny organizations access to IT services, and steal sensitive information including Intellectual Property, trade secrets and customer data. Organizational response to cybersecurity incidents occurs under considerable time pressure in a dynamic and rapidly changing environment with high levels of information load, information diversity and task uncertainty. Effective response requires command, control and coordination of diverse teams of organizational stakeholders as they develop situation awareness, adapt to the rapidly evolving situation, raise the necessary resources, and respond to threats. Although the need to improve the practice of incident response in organizations is widely acknowledged, the area is understudied. Hence the special issue sought submissions that study the real-world problem of incident response and contribute sound practical advice to industry.

In “Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence”, practitioner-philosopher Hettema argues that incident responders cannot be expected to have full knowledge of the all the particulars related to an unfolding incident. The author therefore proposes a suite of rationality constraints based on belief revision that simplify the epistemic requirements and reduce cognitive load placed on responders. These constraints are applied to a scenario to demonstrate their utility in the context of incident response. The key contribution to practice is the assertion that incident responders can be better trained to manage the ‘epistemic states’ that underpin the process of arriving to a conclusion and the provision of a three-state model of belief revision comprising expansion, contraction and revision.

In “Impact of Comprehensive Information Security Awareness and Cognitive Characteristics on Security Incident Management”, authors Thangavelu et al. model the relationship between cybersecurity awareness and threat management. Specifically, the authors break down cybersecurity awareness into its constituent parts and hypothesize their relationship to task performance in cyber-threat management. They validate their model using a quantitative survey of hundred respondents. The study is particularly interesting because it suggests the need to extend the body of knowledge in cybersecurity awareness and establishes the link between awareness of particular aspects of cybersecurity and performance of incident response.

Van der Kleij et al. study decision-support for cyber threat managers and incident responders in their paper titled “Developing Decision Support for Cybersecurity Threat and Incident Managers”. They contribute a critical thinking memory aid to assist incident responders to balance operational imperatives with strategic context. To develop this aid the authors used cognitive task analysis and cognitive work analysis using ten industry professionals. The memory aid was formatively evaluated iteratively to demonstrate its practical utility in real-world applications.

Given the emergence of sophisticated cyber-threat actors, organizations are recognizing the limitations of compliance-driven cybersecurity in producing generic defences and the need for more threat-intelligence driven cybersecurity for custom defences. Against this backdrop, Schlette et al. present a timely study of CTI integration in Security Operations Centres (SOCs). The primary contribution of their paper titled “CTI-SOC2M2 – The Quest for Mature, Intelligence-driven Security Operations and Incident Response Capabilities” is a capability maturity model. The model is developed from an analysis of intelligence-driven cybersecurity operations and evaluated using expert interviews.

The disparate effect of incident response actions on a firm’s stock value compared to its customers is the focus of “Apologize or Justify? Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies”. Masuch et al. use publicly available data to study breaches involving customer information. Interestingly, they find that issuing an apology negatively impacted investor behavior whereas a justification had no impact. The authors draw on their results to provide practical advice to organizations on formulating a response strategy.

Finally, in “Cyber-resilience of Critical Infrastructures: Integrating Digital Twins in the Electric Power Ecosystem”, Salvi et al. explore cyber-risks arising from power infrastructure using a digital twin. The authors develop a model to increase cyber situation awareness and cyber resilience by drawing on existing knowledge of situation awareness and common operational picture. The practice contribution

of this paper is enhanced incident response capacity through minimizing response time and reduced impact of cyber-attacks.

In total there were 13 submissions to the special issue. This low number reinforces our earlier point that the research area of incident response is understudied. Three of the submissions were desk rejected as they were deemed out of scope. The remaining ten submissions were reviewed. Despite the high quality of each of these manuscripts, six were accepted and four were rejected. Each of the accepted papers underwent two rounds of review. We would like to thank the panel of high calibre reviewers drawn from academia and industry for their profound commentary and expert assessment. The review pack for each paper was of a very high standard as was widely acknowledged by the authors.

We believe the six papers accepted in the special issue have made a significant contribution to the study of incident response in organizations. We hope that cybersecurity researchers around the world will draw insights and inspiration from these papers to generate new avenues of research. However, despite these important contributions, there is a need for significantly more *engaged scholarship* in incident response. Most importantly, there is a need for more in-depth case studies that explore the role of contingent factors on incident response. Such factors include organizational structure and organizational culture. We present some research questions as inspiration. How can organizations develop organizational structures that combine stability and preparedness with flexibility and rapid response? How does the widespread positioning of the incident response function inside the IT Operations Division affect an organization's capability to respond to cyber-attack? How does organizational culture influence incident communication and coordination in incident response?

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this editorial.

Atif Ahmad, University of Melbourne, Australia atif@unimelb.edu.au
Sean Maynard, University of Melbourne, Australia seanbm@unimelb.edu.au.
Richard Baskerville, Georgia State University, USA baskerville@acm.org

P1: Impact of Comprehensive Information Security Awareness and Cognitive Characteristics on Security Incident Management: An Empirical Study

Organizations deploy a team of dedicated security professionals and spend significant resources safeguarding their digital assets. Despite best efforts, security incidents are on the rise and remain a key challenge. The literature has focused inadequately on the lack of professionals' awareness of security, system, or situational aspects. Extant literature on the impact of awareness on threat management tasks is disjointed and does not adequately consider the metacognitive awareness and self-efficacy of security professionals. To this effect, we propose and empirically validate a model to study the relationship between security, system, situational awareness, and security professionals' ability to detect, assess, and mitigate threats. We also investigate the effects of metacognitive awareness and self-efficacy on the relationship between awareness and threat management tasks. We validate the model using a survey of 100 information security professionals. Results indicate a significant relationship between awareness, metacognitive awareness, self-efficacy, and threat management task performance. The analysis also demonstrates that metacognitive awareness and self-efficacy mediated the impact of awareness on threat management task performance. We discuss the effects and implications of this study for practice and research.

P2: Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence

In this paper I develop a model for the application of rationality constraints in cyber incident handling, attribution and threat intelligence. The basic idea of this paper is that handling, analysis and attribution involves `epistemic states' that are based on a limited understanding of the attackers motives, opportunities, steps and specific movements. These states are updated dynamically during the incident response process. In a similar manner, epistemic states also play a role in cyber threat intelligence and attribution. Such updates are limited in scope and piecemeal. The paper argues that despite these limitations, such updates are still valuable contributors to a robust explanation of events. I contrast this characterization with current assumptions in the literature and argue for the moral strength of specific rationality constraints in how intelligence from cyber attributions is analyzed, reported and disseminated.

P3: Developing decision support for cybersecurity threat and incident managers

Cybersecurity threat and incident managers in large organizations, especially in the financial sector, are confronted more and more with an increase in volume and complexity of threats and incidents. At the same time, these managers have to deal with many internal processes and criteria, in addition to requirements from external parties, such as regulators that pose an additional challenge to handling threats and incidents. Little research has been carried out to understand to what extent decision support can aid these professionals in managing threats and incidents. The purpose of this research was to develop decision support for cybersecurity threat and incident managers in the financial sector. To this end, we carried out a cognitive task analysis and the first two phases of a cognitive work analysis, based on two rounds of in-depth interviews with ten professionals from three financial institutions. Our results show that decision support should address the problem of balancing the bigger picture with details. That is, being able to simultaneously keep the broader operational context in mind as well as adequately investigating, containing and remediating a cyberattack. In close consultation with the three financial institutions involved, we developed a critical- thinking memory aid that follows typical incident response process steps, but adds big picture elements and critical thinking steps. This should make cybersecurity threat and incident managers more aware of the broader operational implications of threats and incidents while keeping a critical mindset. Although a summative evaluation was beyond the scope of the present research, we conducted iterative formative evaluations of the memory aid that show its potential.

P4: CTI-SOC2M2 – The quest for mature, intelligence-driven security operations and incident response capabilities

Threats, cyber attacks, and security incidents pertain to organizations of all types. Everyday information security is essentially defined by the maturity of security operations and incident response capabilities. However, focusing on internal information only has proven insufficient in an ever-changing threat landscape. Cyber threat intelligence (CTI) and its sharing are deemed necessary to cope with advanced threats and strongly influence security capabilities. Therefore, in this work, we develop CTI-SOC2M2, a capability maturity model that uses the degree of CTI integration as a proxy for SOC service maturity. In the course, we examine existing maturity models in the domains of Security Operations Centers (SOCs), incident response, and CTI. In search of adequate maturity assessment, we show threat intelligence dependencies through applicable data formats. As the systematic development of maturity models demands, our mixed methodology approach contributes a new in-depth analysis of intelligence-driven security operations. The resulting CTI-SOC2M2 model contains CTI formats, SOC services and is complemented with an evaluation through expert interviews. A prototypical, tool-based implementation is aimed to document steps towards the model's practical application.

P5: Cyber-resilience of Critical Cyber Infrastructures: integrating digital twins in the electric power ecosystem.

This contribution presents a model for cyber-resilience of Critical Cyber Infrastructures (CCI) based on the implementation of a digital twin. It addresses the risks associated with the integration of computational, communication and physical aspects of CCIs. We focus specifically on cybersecurity in the electric power sector due both to its salience and to the potential risks associated to failures in guaranteeing resilience. Informed by the literature on information security management, situational awareness (SA) and common operational picture (COP), we derive an overarching model to provide CCIs' actors with increased cyber situational awareness, common understanding of incidents and enhanced response capacity. On the practical side, the model seeks to minimize response time and to reduce the impact of cyber-attacks on the organizations and on society as a whole. We develop a process model and validate three design propositions through a formative evaluation in the context of a digital twin implementation in the EU electrical power sector. We discuss the implications of this model for further research as well as practical applications for the electrical power sector.

P6: Apologize or Justify? Examining the Impact of Data Breach Response Actions on Stock Value of Affected Companies

As cybersecurity incidents increase and become more potent, affected companies must react. This is especially relevant for data breaches, where companies are legally required to notify those affected. Hence, it can be assumed that data breaches invariably cause damage through disappointed customers and dissatisfied investors. By applying response actions of a response strategy in a data breach announcement, a company can mitigate these consequences. However, the literature reveals an inconsistent landscape regarding the effect of response actions on customers or investors. Using an event study, we show that the response actions impact a company's stock value and that this impact does not necessarily match the impact on the customer. We code the real-world response actions to data breaches, examining their impact on investor behavior using stock value. The results show that data breaches involving customer data have a negative impact on stock value. In addition, an apology for a data breach has been found to have harmful effects on investor behavior. Whereas justifying the data breach has no or a positive impact. These results add to the investor-focused literature on data breaches, showing that an impact on stock value can emerge from response actions. The literature on data breaches can be informed by the fact that not just is the customer perspective important, but also reactions from other affected groups should be included in formulating a response strategy. The paper also provides practical implications, showing how companies can improve their response strategies based on the results.