Cybersecurity Agility: Antecedents and Effects on Security Incident Management Effectiveness

Research-in-Progress

Sessika Siregar **Kuo-Chung Chang**

Abstract

Increased dynamism and complexity of cybersecurity threat environments mean that traditional approaches of managing cybersecurity are no longer effective to minimize the harm of cybersecurity attacks. Although comprehensive guidelines and past studies that address the issue of effective incident management are available, a conceptual model that explains and addresses organizational factors that might help or impede organizational ability to manage cybersecurity incidents effectively is yet to be developed and empirically tested. To address this gap, this research aim to develop and empirically test a conceptual model that would address the role of both social and technical part of cybersecurity infrastructure in enhancing organization's incident management effectiveness. Based on dynamic capability perspective, a research model has been developed. Research motivation, literature review, research methodology, as well as potential research and practical implications are discussed in this manuscript.

Keywords: Cybersecurity incident detection, cybersecurity incident response, cybersecurity infrastructure, analytical capability, coordination

Introduction

Increased dynamism and complexity in cybersecurity threat environments mean that the traditional approach of managing information security is no longer enough (Baskerville, Spagnoletti, and Kim 2014; Spagnoletti and Resca 2008; Stobart 2017). The existence of novel and customized attacks such as Advanced Persistent Threats (APTs), increase of cyber criminals' networks and petty criminals, proliferation and introduction of unmanaged devices such as Internet of Things (IoT) on organization networks along with limited resources are among difficult-to-resolve vulnerabilities to encourage organizations to embrace a more realistic and productive posture of simply accepting that advanced attackers will undoubtedly bypass organization security (Baskerville et al. 2014; EY 2017). Minimizing organizational harm or possible harm in the current threats environment would therefore largely depends on the effective management of each cybersecurity incidents.

Yet there are several gaps in the literature such as small sample size in the existing literature (Ismail, Ahmad, and Shukran 2011; Jaatun and Koelle 2016; Tøndel et al. 2014), lack of theoretical model that explains incident management (Tøndel et al. 2014; Van der Kleij, Kleinhuis, and Young 2017), and lack of research that address holistically the role of IT infrastructure in effective incident management (Soomro, Shah, and Ahmed 2016). To fill these gaps, this study intends to develop and empirically

test a conceptual model that comprehensively addresses effective incident management handling using dynamic capabilities theories. Dynamic capabilities refer to organizational capabilities to revise the combinations of its knowledge, assets, and resources to adapt to the changing business environment in order to survive or remain competitive. It is based on the implications that organizations should continually revise their capabilities particularly when faced with dynamic or unpredictable environment (Eisenhardt and Martin 2000; Roberts and Grover 2012; Teece, Pisano, and Shuen 1997). Dynamic capability is distinctive from operational capability where operational capability relates to capability of organization in its current operation while dynamic capability relates to the efficient and responsive change and development on these organizational operations and resources. It is thus applicable to incident management in current dynamic threat environment because it explains and describe organizational capability required for creating series of temporary advantages when faced with hypercompetitive environment. Similarly, the current cybersecurity environment is filled with new, unknown, or unexpected attacks from unknown or unexpected attackers targeting unknown or unexpected part of organizational systems which requires organizations to create a series of temporary advantages over the attackers.

This manuscript proceeds as follows. First we form and describe the theoretical foundations of our research model. Then, we present our research model. Next, we describe the research methodology designed to test our research hypotheses. Lastly, we discuss potential research and practical contributions.

Theoretical Foundations

According to dynamic capability perspective, key for organizations' success in hypercompetitive environments is organizational agility which refers to organizational ability to sense relevant change and respond readily to market opportunities. In cybersecurity context, being agile to the new, unknown, or unexpected attacks is also important to handle incident more effectively as agility allows organization to continually enhance and redefine its ability in detecting and responding to these new, unknown, or unexpected attacks. As both detecting and responding capability are required to achieve agility, organizations can therefore handle incident more effectively if their detecting and responding capability are developed and applied in aligned way. For example, Disqus detected a breach in its systems by following a lead from one of its partner and they also respond quickly by containing the breach and notifying its users thus minimizing their damage (Hunt 2017). Meanwhile, Equifax failed to detect and respond in an effective manner to their data breach incident leading to higher organizational costs (Richter 2017). Hence, an aligned cybersecurity detecting and responding capability will lead to a more effective incident management. To achieve an aligned cybersecurity detecting and responding capability however organization would first need to develop and apply both cybersecurity detecting capability as well as responding capability.

To effectively handle cybersecurity incidents, it is firstly important for organization to detect significant event or incident as quickly as possible as it is the outputs of this capability which signals the start of incident management (Mitropoulos, Patsos, and Douligeris 2006). Without knowing that there is an unwanted event or incident happening inside organizational systems, organization would not initiate the action to handle the incident. Furthermore, the longer an event or incident is left undetected, the more difficult it is for organizations to accurately measure the damage it may have caused to itself as well as to its partners and customers. Thus, organization capability to quickly detect relevant attacks is important to effectively handle cybersecurity incident.

Just knowing about an incident or possible incident without actually doing anything about it is of course futile in managing cybersecurity incident let alone to handle it effectively. This task becomes even more difficult when the attacks are new, unknown, or unexpected as it demands organization ability to quickly develop and deploy security safeguards with similar characteristics of newness or unexpectedness (Baskerville et al. 2014; Mickos 2017). The readier organization is in deploying the customized safeguards, the more effective their incident management capability is. Hence, organization capability to readily respond to new, unknown, or unexpected attacks is important to effectively handle cybersecurity incident.

Cybersecurity detecting capability relates to being able to detect relevant changes in organization information systems quickly. With the amount of data generated from organization information resources as well as the often limited resources for security, it is simply difficult if not impossible for humans to perform this task manually. IT infrastructure comprises of technical and human aspect of organization information management resources. Human aspect of IT infrastructure refers to the knowledge and skills necessary to manage IT resources within an organization (Broadbent and Weill 1997; Byrd and Turner 2000). Meanwhile technical aspect of IT infrastructure refers to a set of shared and tangible IT resources including platform technology, network and telecommunication technologies, data, as well as core software applications that formed the foundation for business applications (Byrd and Turner 2000; Duncan 1995). Both technical and human aspects of IT infrastructure are essential in assisting organization to rapidly identify relevant changes in organization information systems. Hardware or computer programs designed to identify attacks in organization network or system, such as Intrusion Detection and Prevention Systems (IDS/IPS) and Web Application Firewalls, provides information and insights that can significantly enhance organization ability to notice irregular patterns in its systems (Souissi et al. 2017). The knowledge and skills of IT personnel however would often be needed to configure the technologies to fit organizational structures as well as to intercept when the technologies fail. Technical security IT infrastructure can therefore enhance organization cybersecurity detecting capability, but their relation would be affected by the knowledge and cybersecurity skills of the personnel in charge, particularly their ability to analyze the technical security IT infrastructure.

Meanwhile, cybersecurity responding capability relates to being able to respond readily to new, unknown, or unexpected threats. Organizational readiness to act depends heavily on the formative structure of its existing constituents, namely how quick and willing are its members in modifying their existing routines and conventional ways of acting and behaving to fit organizational needs (Spagnoletti and Resca 2008). As organization involves interdependencies between its members such as sharing of resources, synchronization of activities, and prerequisite activities, organization's readiness to respond depends heavily on organization's ability to manage these interdependencies through coordination (Bartnes, Moe, and Heegaard 2016). As security incident more often than not is not merely a technical or IT issue, cybersecurity responding capability therefore affected not only by internal coordination between cybersecurity personnel but also the external coordination between cybersecurity personnel with individuals from different parts of the organization as well as outside of it (Mitropoulos et al. 2006).

These cybersecurity detecting and responding capabilities need to be developed and applied at the same time to capitalize on agility (Roberts and Grover 2012). The alignment between the two capabilities essentially acts as the dynamic portion that allow organization to adapt to the dynamic environment of cybersecurity threats. Thus in this research we argue that it is detecting-responding alignment that has direct relations to cybersecurity incident management effectiveness and not the distinctive capabilities.

Literature Review

Cybersecurity Infrastructure

The arrangement of organization tangible technical IT resources and services such as platforms, network and telecommunication technologies, data, and software applications is defined as IT infrastructure (Roberts and Grover 2012) Cybersecurity infrastructure can therefore be defined as the arrangement of organization tangible IT resources as well as IT services for the confidentiality, integrity, availability, and resilience of organization's systems, networks, and critical data assets. Mitropoulos et al. (2006) list several categories of cybersecurity infrastructure such as: Host and Network-Based Intrusion Detection Systems (IDS), sniffers, audit log consolidation software, backup software, network traffic monitoring, virus scan, and (Near) Real Time Threat Management Systems. Werlinger et al. (2010) identify four important functions of organization cybersecurity infrastructure, namely: monitoring, verification, assessment, and tracking the source of anomaly. Meanwhile, Souissi et al. (2017) argue that cybersecurity infrastructure involves collecting logs or alerts from different

probes and to aggregate, prioritize, and correlate them to decrease the number of alerts that cybersecurity personnel has to deal with. Metzger et al. (2011) identify three ways through which organization IT infrastructure can be utilized to detect incident, namely: manual incident reports through email or phone, automatic security warnings or report from other third party services, and local security monitoring mechanisms.

Analytical capability

Analytical capability refers to the ability of cybersecurity personnel to visualize, articulate, and conceptualize or solve both complex and uncomplicated problems by making decisions that are sensible given the available information. It involves using data, explanatory and predictive models, statistical and quantitative analysis as well as facts extensively in making decisions and taking actions (Davenport et al. 2007; Roberts and Grover 2012). Responding to incident demands a set of skills such as pattern recognition, hypothesis generation, and cooperation as well as knowledge about IT infrastructure, protocols, and attack patterns (Werlinger, Botta, and Beznosov 2007). It also requires strategies of isolation and simulation to figure out the source of the incident and to verify the existence of the unwanted intrusions. Cybersecurity personnel need to be able to interpret alerts, put pieces together, know about possible attacks and understand their impacts (Bartnes et al. 2016). It involves three-phase processes, namely: situation recognition, situation comprehension, and situation projection (Barford et al. 2010).

Internal and External Coordination

Coordination relates the degree to which two or more parties develop a mutual understanding of each other's capabilities and align their goals and activities based on such understanding (Roberts and Grover 2012). It refers to managing interdependencies between organizational activities so that its individual parts can realize a collective performance (Bartnes et al. 2016; Malone and Crowston 1994; Okhuysen and Bechky 2009). Internal coordination refers to mutual understanding and alignment of goals and activities among organization cybersecurity personnel. Meanwhile, external coordination refers to mutual understanding and alignment of goals and activities between cybersecurity personnel with other actors inside and outside the organizations.

Cybersecurity Detecting Capability

Cybersecurity detecting capability can be defined as the ability of organization cybersecurity personnel to quickly recognize, notice, and verify relevant security events or incidents in organization information systems. It involves accurate and timely awareness of important changes in organization environment (Dove 2005; Trinh-Phuong, Molla, and Peszynski 2012). In incident management, detection involves the proactive and reactive act to gather information on current events, potential incidents, vulnerabilities, and other computer security or incident management information (Chiu and Lin 2017). Detecting of incident begins with the notification of an incident, verifying that the incident does actually exist, determining its scope, and notifying relevant personnel and agencies as well as affected users (Wack 1991). Werlinger et al. (2010) argue that diagnostic part of incident response that is the act of noticing and categorising problems involves four aspects, namely: monitoring, verification, assessment, and tracking the source of the anomaly. Monitoring refers to the act of generating meaningful reports on organization's IT systems usage through a variety of security tools as well as notifications from various stakeholders such as IT professionals and end-users. Verification refers to the act of confirming with alternate data sources that compromise actually happened. Assessment refers to the estimation of the magnitude and consequences of the incident. Meanwhile, tracking of anomaly source refers to the act of determining the source of the incident such as the malicious software or the compromised servers.

Cybersecurity Responding Capability

Responding refers to the ability to modify business processes and tailor operational responses in real time (Dove 2005; Trinh-Phuong et al. 2012). Meanwhile, cybersecurity responding capability can be

defined as the ability of organization cybersecurity personnel to readily adjust, modify, or reconfigure the structure of organization existing information resources when new, unknown, or unexpected event or incident occurs. Responding to new or unexpected cybersecurity incident often requires creativity as more than one correct solution might be available and there are numerous uncertainties and interdependencies to be considered (Bartnes et al. 2016). Spagnoletti and Resca (2008) identify three practices which describe organization capable of responding readily to unpredictable attacks, namely: bricolage, improvisation, and hacking. Bricolage refers to the capacity to tinker with existing technology and practices when faced with unpredictable events or incidents. Improvisation refers to the ability to act in a extemporaneous, sudden, and unpredictable way in order to gain control or produce favorable conditions when faced with unpredictable events or incidents. Lastly, hacking refers to the ability to reinterpret and use existing software programs in an unorthodox way to produce new or unexpected solutions to unpredictable events or incidents.

Detecting-Responding Alignment

Alignment refers to the degree to which the objectives and structure of an organization cybersecurity detecting capability are consistent to the objectives and structure of its cybersecurity responding capability (Roberts and Grover 2012). The higher the alignment between organization detecting and responding capability, the greater the effect of cybersecurity agility on incident management effectiveness because strong detecting with weak responding means organization would notice an incident but cannot act on the information in a proper manner leading to time loss and confusions. Similarly it is no use of having strong ability to response to incident but organizations are slow in realizing that an incident such as breach has happened.

Cybersecurity Incident Management Effectiveness

Incident management consists of organizational action to contain and mitigate security events or incidents and recover organization systems to its original or intended functions. The ultimate objective of incident management is to minimize organization damage due to cybersecurity event or incident (Mitropoulos et al. 2006). Event refers to an observable occurence in organization systems or network, while incident can be defined as any real or suspected danger that could lead to loss or disturbance in organization's operations, services, or functions (Chiu and Lin 2017). Five types of cybersecurity incidents can happen in organization systems, namely: Denial of Service, Malicious Code, Unauthorized Access, and Inappropriate Usage (Chiu and Lin 2017; Howard and Longstaff 1998; Sahibudin, Sharifi, and Ayat 2008). Kossakowski, Allen, Alberts, Cohen, and Ford (1999) categorize incident responding practices into three categories, namely: preparation, handling/managing, and follow-up. Handling/managing involves six recommended practices: analyzing all available information to characterize an intrusion, communicate with all parties that need to be made aware of an intrusion and its progress, collect and protect information associated with an intrusion, apply short-term solutions to contain an intrusion, eliminate all means of intruder access, and return systems to normal operation.

Metrics to objectively measure organization effectiveness in managing incident are scarce (Bada, Creese, Goldsmith, Mitchell, and Phillips 2014; Kleij, Kleinhuis, and Young 2017; Wiik, Gonzalez, and Kossakowski 2006). To effectively measure incident response team's effectiveness, a combination of technical performance measurements as well as behavioral assessment measurements are needed (Granåsen and Andersson 2016). Many existing metrics however are more focused on the technical part such as time to identification, speed to solution, number of errors, incident rates over time, mean time to repair, costs, etc (Kleij et al. 2017). The most comprehensive and internationally recognized documentation and what is at present the most recommended practice of cybersecurity incident management process is ISO/IEC 27035 (ISO/IEC 2011). A metric that also involves behavioral metrics such as cybersecurity incident response team performance and cooperation is still absent.

Research Model

Figure 1 presents our research model. This study specifically argues that effective management of incidents in the hyperdynamic cybersecurity environment requires organization cybersecurity agility which can be achieved when organization cybersecurity detecting and responding capabilities are aligned. This alignment involves the simultaneous development and application of both cybersecurity detecting capability and cybersecurity responding capability. Cybersecurity detecting capability can be enhanced through the use of cybersecurity infrastructure. The relationship between cybersecurity infrastructure and cybersecurity detecting capability however depends on the analytical capability of organization cybersecurity personnel. Meanwhile, cybersecurity responding capability strongly depends on the capability of organization to coordinate its cybersecurity activities internally and externally.

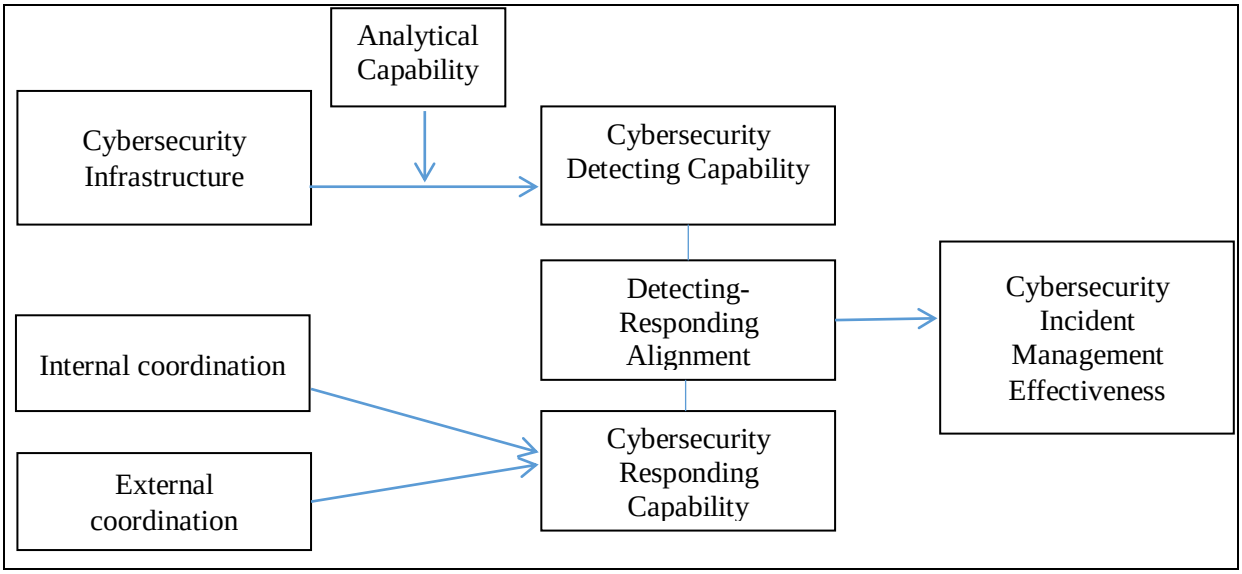

Figure 1. Research Model

Methodology

The unit of analysis in this study is organizational level. Data will be collected through survey. The key respondents will be IT personnel or organizational members responsible for cybersecurity tasks in various organizations in Taiwan and Indonesia. In terms of construct development and refinement, the study adopts Moore and Benbasat's (1991) and Churchill's (1979) scale development procedure. For each construct presented in the research model, a thorough search will be undertaken to identify existing measures in the literature. Pertinent scales will be reviewed for their coverage of content and psychometric properties, where possible existing measures that have demonstrated reliability and validity will be used. When no existing scales is available, new scales will be developed with the reliability and the content validity of the various scales being developed will be measured by asking a panel of judges to sort the scale items into different construct categories (Moore and Benbasat 1991). The instrument will then be pilot tested on a representative sample of the target population using conditions similar to those anticipated during actual data collection. The improved survey document resulting from the pilot test will be used to conduct a survey. A sample will be drawn from the Taiwan and Indonesia industries with the primary focus on high-technology companies. SPSS and PLS will be used as tool of analysis.

Potential Contributions

Academic Contributions

- Provide empirical study to better understand organizational factors that might influence cybersecurity incident management effectiveness across different organizations

- Increase conceptual understanding on the issues and findings about effective cybersecurity incident management through the application of dynamic capabilities perspective
- Comprehensively address the role of cybersecurity infrastructure in facilitating cybersecurity agility and effective management of cybersecurity incident

Practical Implications

- Provide comprehensive and practical tactics that organization can apply to significantly increase the effectiveness of organization cybersecurity incident management
- Provide theoretical and empirical basis that organization can refer to in order to increase the effectiveness of organization cybersecurity incident management

References

Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. 2012. "Incident response teams–Challenges in supporting the organisational security function," *Computers and Security* (31:5), pp. 643-652.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J. T., Jajodia, S., and Ning, P. 2010. "Cyber SA: Situational Awareness for Cyber Defense," *Cyber Situational Awareness* (46:1), pp. 3-13.

Bartnes, M., Moe, N. B., and Heegaard, P. E. 2016. "The future of information security incident management training: a case study of electrical power companies," *Computers and Security* (61), pp. 32-45.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-centered information security: Managing a strategic balance between prevention and response," *Information and Management* (51:1), pp. 138-151.

Chiu, C.-C., and Lin, K.-S. 2017. "Importance-Performance Analysis Based Evaluation Method for Security Incident Management Capability," *The Asian Conference on Intelligent Information and Database Systems*.

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. "Computer security incident handling guide," *NIST Special Publication* 800 (61).

Denning, D. E. 1987. "An intrusion-detection model," *IEEE Transactions on software engineering* (2), pp. 222-232.

Eisenhardt, K. M., and Martin, J. A. 2000. "Dynamic capabilities: what are they?," *Strategic Management Journal*, pp. 1105-1121.

Granåsen, M., and Andersson, D. 2016. "Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study," *Cognition, Technology and Work* (18:1), pp. 121-143.

ISO/IEC. 2016. *ISO/IEC 27035 Information security incident management*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:-1:ed-1:v1:en: ISO/IEC.

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., and Longva, O. H. 2009. "A framework for incident response management in the petroleum industry," *International Journal of Critical Infrastructure Protection* (2:1), pp. 26-37.

Jaatun, M. G., and Koelle, R. 2016. "Cyber Security Incident Management in the Aviation Domain," *The Availability, Reliability and Security (ARES)*, 2016 11th International Conference.

Kleij, R. V. d., Kleinhuis, G., and Young, H. 2017. "Computer Security Incident Response Team Effectivess: A Needs Assessment," *Frontiers in Psychology* (8). (doi: 10.3389/fpsyg.2017.02179)

Lundberg, N., and Tellioğlu, H. 1999. "Understanding complex coordination processes in health care," *Scandinavian Journal of Information Systems* (11:1), pp. 5.

Martin, A., Dmitriev, D., and Akeroyd, J. 2010. "A resurgence of interest in Information Architecture," *International Journal of Information Management* (30:1), pp. 6-12.

Metzger, S., Hommel, W., and Reiser, H. 2011. "Integrated Security Incident Management--Concepts and Real-World Experiences," Paper presented at the *IT Security Incident Management and IT Forensics (IMF)*, 2011 Sixth International Conference.

Mitropoulos, S., Patsos, D., and Douligeris, C. 2006. "On Incident Handling and Response: A state-of-the-art approach," *Computers and Security* (25:5), pp. 351-370.

Pulkkinen, M., Naumenko, A., and Luostarinen, K. 2007. "Managing information security in a business network of machinery maintenance services business–Enterprise architecture as a coordination tool," *Journal of Systems and Software* (80:10), pp. 1607-1620.

Roberts, N., and Grover, V. 2012. "Leveraging information technology infrastructure to facilitate a firm's customer agility and competitive activity: An empirical investigation," *Journal of Management Information Systems* (28:4), pp. 231-270.

Soomro, Z. A., Shah, M. H., and Ahmed, J. 2016. "Information security management needs more holistic approach: A literature review," *International Journal of Information Management* (36:2), pp. 215-225.

Spagnoletti, P., and Resca, A. 2008. "The duality of Information Security Management: fighting against predictable and unpredictable threats," *Journal of Information System Security* (4:3), pp. 46-62.

Teece, D. J., Pisano, G., and Shuen, A. 1997. "Dynamic capabilities and strategic management," *Strategic Management Journal*, pp. 509-533.

Tøndel, I. A., Line, M. B., and Jaatun, M. G. 2014. "Information security incident management: Current practice as reported in the literature," *Computers and Security* (45), pp. 42-57.

Trinh-Phuong, T., Molla, A., and Peszynski, K. 2012. "Enterprise Systems and Organizational Agility: A Review of the Literature and Conceptual Framework," *Communications of the Association for Information Systems* (31).

Van der Kleij, R., Kleinhuis, G., and Young, H. 2017. "Computer Security Incident Response Team Effectiveness: A Needs Assessment," *Frontiers in Psychology* (8), pp. 2179.

Wack, J. 1991. "Establishing a Computer Security Incident Response Capability (CSIRC)," *NIST Special Publication* 800(3).

Werlinger, R., Botta, D., and Beznosov, K. 2007. "Detecting, analyzing and responding to security incidents: a qualitative analysis," Paper presented at the Proceedings of the 3rd symposium on *Usable privacy and security*.

Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K. 2010. "Preparation, detection, and analysis: the diagnostic work of IT security incident response," *Information Management and Computer Security* (18:1), pp. 26-42.