How integration of security management and incident response enables organizational learning

Atif Ahmad
School of Computing and Information Systems, University of Melbourne, Australia, 3010. Ph: +613 8344 1396. Fax +316 9349 4596. E-mail: atif@unimelb.edu.au

Kevin Desouza
School of Management, QUT Business School, Queensland University of Technology, Australia, 4000. Ph: +61 7 3138 9019. Fax: +61 7 3138 1055. E-mail: kevin.c.desouza@gmail.com

Sean B Maynard *** Corresponding Author**
School of Computing and Information Systems, University of Melbourne, Australia, 3010. Ph: +613 8344 1573. Fax +316 9349 4596. E-mail: seanbm@unimelb.edu.au

Humza Naseer
School of Computing and Information Systems, University of Melbourne, Australia, 3010. Ph: +613 8344 1396. Fax +316 9349 4596. E-mail: humza.naseer@unimelb.edu.au

Richard L Baskerville
Robinson College of Business, Georgia State University, Atlanta, GA 30302. Ph: +1 404.413.7362. Fax: +1 404.413.7394. E-mail: baskerville@acm.org

Abstract

Digital assets of organizations are under constant threat from a wide assortment of nefarious actors. When threats materialize, the consequences can be significant. Most large organizations invest in a dedicated information security management (ISM) function to ensure that digital assets are protected. The ISM function conducts risk assessments, develops strategy, provides policies and training to define roles and guide behavior, and implements technological controls such as firewalls, anti-virus, and encryption to restrict unauthorized access. Despite these protective measures, incidents (security breaches) will occur. Alongside the security management function, many organizations also retain an incident response (IR) function to mitigate damage from an attack and promptly restore digital services. However, few organizations integrate and learn from experiences of these functions in an optimal manner that enables them to not only respond to security incidents but also proactively maneuver the threat environment. In this paper, we draw on organizational learning theory to develop a conceptual framework that explains how the ISM and IR functions can be better integrated. The strong integration of ISM and IR functions, in turn, creates learning opportunities that lead to organizational security benefits including – *increased awareness of security risks*, *compilation of threat intelligence*, *removal of flaws in security defenses*, *evaluation of security defensive logic* and *enhanced security response*.

Keywords: digital assets; information security management; incident response; organizational learning; cybersecurity; data security; system security; technology security

Introduction

Organizations face a significant challenge in protecting their digital assets from sophisticated, complex and evolving security threats. In 2012, members of Unit 61398 of the Chinese People's Liberation Army attacked the US-based computers belonging to SolarWorld AG, a German photovoltaic products company (United States Department of Justice, 2014). The attackers stole a large cache of sensitive information of the firm's Intellectual Property (IP), pricing and financial information, production capabilities, and business strategy. SolarWorld AG declared bankruptcy five years after suffering the breach. Like Unit 61398, a team of Russian hackers known as the 'Sandworm gang' used malware dubbed 'Black Energy' in 2014 and 2015 to attack several high-profile targets in Europe including a French telecommunications firm as well as Ukraine's power infrastructure that caused widespread outages (Case, 2016).

Purposive attacks motivated by financial or political considerations are a significant and emerging development in the modern threat landscape. This trend has been widely and consistently reported over the past five or more years and the trend continues unabated. For example, Verizon's '2018 Data Breaches Investigations' reported that outsiders perpetrated 73% of the surveyed 53,000 incidents (Verizon, 2018). Of these externally initiated incidents, half were committed by organized criminal groups and 12% by groups affiliated with state or state-affiliated actors. Given the business impact of security incidents, the level of expenditure in information security has dramatically increased in recent years. Worldwide spending on information security solutions is expected to reach $93 billion in 2018 (Gartner, 2017). As the aforementioned surveys suggest, even though organizations have significantly increased their investment in information security, security incidents continue to rise.

In this paper we look at the large organization with a mature Information Security Management capability conforming to 'best practice' industry standards (e.g. ISO 27000 suite). The organization has a permanent dedicated team responsible for a strategic-level Information Security Management (ISM) program that protects the digital assets of the organization. The program encompasses the policies and practices that cover issues such as appropriate use of digital assets, security protocols (e.g. passwords, firewalls) that regulate access and use of digital assets, risk identification and assessment processes that measure exposure and inform strategy, and education and training programs to raise awareness (Alshaikh, Ahmad, Maynard, & Chang, 2014). To address breaches of security the organization has a separate dedicated team that conducts operational-level Incident Response (IR) with a sole focus on ensuring that impact to digital assets (e.g. IT services) can be minimized and IT services can be promptly restored (Ahmad, Hadjkiss, & Ruighaver, 2012; Tøndel, Line, & Jaatun, 2014).

We draw a salient insight from a recent series of in-depth case studies in large organizations that retain well-resourced 'best-practice' teams for their strategic-level ISM and operational-level IR functions. The insight being that organizational investment in information security does not yield optimal benefits because the whole-of-organization response to security incidents tends to be fragmented and disorganized due to weak process-level integration among disconnected teams (Ahmad et al., 2012; Ahmad, Maynard, & Shanks, 2015; Jaatun, Albrechtsen, Line, Tøndel, & Longva, 2009; Tøndel et al., 2014; Webb, Ahmad, Maynard, Baskerville, & Shanks, 2017).

There are genuine reasons for why the ISM and IR functions are not structurally integrated (e.g. the IR function responds to non-security incidents as well). However, as a result of the disconnect, most organizations drift from one security crisis to another without much ability to improve their underlying security management program and incident response capabilities

(Ahmad et al., 2012; Ahmad et al., 2015; Desouza 2007). We therefore ask the following research question: *How can organizations better integrate their security management and incident response functions to enable proactive learning and optimize performance?*

The rest of the paper is organized as follows. In the next section, we discuss the two concepts critical to our framework – securing digital assets and learning from incident response. Following this, we outline the types of disconnects that occur between the ISM and IR functions in organizations. Toward this end, we use an illustrative case. Next, we sketch out our conceptual framework grounded in organizational learning theory that links the ISM and IR functions. We conclude the paper with a discussion of research and practitioner implications and avenues for further research.

Background

Organizational defenses are deliberately designed as a series of preventive barriers (consisting of one or more protective measures) working together in a defense-in-depth formation (similar to the concentric walls around a castle) (Baskerville, Spagnoletti, & Kim, 2014). Each barrier tends to have vulnerabilities or holes in various locations (e.g. engineering defects, misconfigurations, poor management practices) that present an opportunity for an attacker to exploit. If the attacker can exploit the right set of holes (and this becomes manifestly easier if circumstances allow for the holes to line up), then the organization will experience a breach. Breaches that are detected are considered incidents and result in the organization mounting a security response aimed at preserving continuity of function (Baskerville et al., 2014).

Protecting Digital Assets through Information Security Management Practices

Organizations secure digital assets through their ISM program, a combination of managerial practices and protective measures enacted at the operational, tactical, and strategic levels (Ahmad, Maynard, & Park, 2014; Sveen, Torres & Sarriegi, 2009). ISM protects the firm's digital assets using five key management practice areas relating to policy, risk, incident response, technical, as well as education, training and awareness (see Table 1). Each of these management practices is instituted in phases - development, implementation and maintenance, and evaluation. ISM is typically driven by a risk management perspective of information security (Shedden, Ahmad, Smith, Tscherning, & Scheepers, 2016). The starting point is an Information Security Risk Assessment (ISRA) where the organization makes an inventory of assets, maps threats to assets to identify risks (scenarios), and prioritizes risks by criticality using estimations of likelihood and impact (Shedden et al., 2016). Practices in all five aforementioned areas are subsequently used to generate protective strategies to reduce the organization's risk exposure (Shedden et al., 2016; Webb, Ahmad, Maynard, & Shanks, 2014).

ISM Practice Areas	Representative Practices
Security policy management	Assess existing organizational policies; Develop policy directives; Distribute policy; Review policy periodically (Karyda, Kiountouzis, & Kokolakis, 2005; Knapp, Morris, Marshall, & Byrd, 2009; Rees, Bandyopadhyay, & Spafford, 2003; Whitman & Mattord, 2017)
Security risk management	Identify critical assets; Map threats to assets to identify risk scenarios; Estimate likelihood and impact of risk scenarios; Develop risk response strategies; Review risk management

	plans (Finne, 2000; Gerber & von Solms, 2005; Shedden, Smith, & Ahmad, 2010; Stoneburner, Goguen, & Feringa, 2002)
Security incident response management	See Table 2 for incident response practices and related references
Security education, training and awareness (SETA) management	Conduct a SETA needs assessment; Deliver SETA program using available techniques (e.g. posters, computer-assisted learning over online platforms, in-class teaching); Review utility of SETA programs periodically (Tsohou, Karyda, Kokolakis, & Kiountouzis, 2010; Whitman & Mattord, 2017; Wilson & Hash, 2003)
Technical management	Identify security technology controls; Design control architecture (to reduce risk); Implement control architecture; Review the implementation plan (Rees et al., 2003; Tsohou et al., 2010)

Table 1: Information Security Management Practices

Effectively leveraging the full range of practices and protective measures within the constraints of a budget to manage security in organizations is a challenge. Effectiveness frequently comes down to recognizing the interdependencies between security measures and determining how to leverage them in order to achieve the desired effect (Sveen, Torres, & Sarriegi, 2009). When implementing their security programs, organizations tend to focus on instituting technological controls at an operational level such as firewalls, intrusion detection systems and username/password combinations (Ahmad et al., 2014). However, the effectiveness of these controls relies on more foundational measures such as strategic plans, risk assessments and policy. For example, a poor risk assessment will result in a sub-optimal enterprise strategy that in turn leads to misconfiguration of technological controls leaving vulnerabilities for attackers to exploit. Organizational security culture underpins the entire security program (Da Veiga, 2019; Ruighaver, Maynard, & Chang, 2007). A weak security culture can render all protective measures ineffective. For example, policy and training on the use of passwords is futile if the organizational culture encourages the sharing of passwords. Similarly, a need-to-know policy enforced by classification matrices, document labeling, firewalls, and NDAs will be ineffective if senior managers consistently ignore, flaunt and/or dismiss protective confidentiality measures.

Fortifying Digital Asset Security by Learning from Incidents and Responses

Incidents and the associated security responses to them are critical episodes from which organizations can learn and develop their security functions. Incidents are adverse events in an information security system in which an exploited vulnerability has compromised the confidentiality, integrity, or availability of information assets (Cichonski, Millar, Grance, & Scarfone, 2012). Examples of incidents include unauthorized access to sensitive information and significant disruption to networked services. Incidents such as the leakage of trade secrets may have multiple and catastrophic consequences such as loss of competitive advantage, loss of company reputation and customer confidence, legal penalties, loss of productivity and direct financial loss (Manzini & Lazzarotti, 2016).

The IR function diagnoses incidents, contains their impact, eradicates the causes, and restores IT systems to their routine functionality (Cichonski et al., 2012). Incident Response is a cyclic process of six sequential stages (Table 2 summarizes practice literature). IR teams

engage in pre-incident preparation followed by identification, containment, eradication, recovery and follow-up post-incident. The follow-up phase allows for reflection on the incident handling experience where 'lessons learned' are identified for incorporation into standard operating procedures.

Phase	Description
Preparation	• Develop preventative measures (e.g. security policies, procedures, threat models) • Preparing for incident handling by building a 'response kit' tools to assist during an incident (USB drives, laptops, software, stationery and cabling) and establishing other support • Proactive prevention of incidents through incident management awareness briefings and training
Identification	• When an incident occurs: o Determine if an incident exists. o Validate the scope and potential impact o Determine how the incident occurred
Containment	• After incident identification: o Contain the incident to reduce the likelihood that it will worsen o Prevent further contamination of the system o Preserve evidence for potential future legal proceedings.
Eradication	• Clean up after the incident, based on the information gathered on the incident. • Attempt to neutralize the attack (e.g. deleting malicious code).
Recovery	• Transfer the system back into regular organizational use • Monitor the system to check normal operation
Follow-Up	• Validate and improve the incident handling process o Complete incident reports o Present reports to management o Analyze incident response and draw insights and learning to improve the incident response process from technical and managerial perspectives o Define a strategy and plan for implementing the changes

Table 2: Description of Incident Response Phases (Cichonski et al., 2012; Kelver, 2002; Northcutt, 2003; West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003)

The response function to incidents in organizations is manifested in diverse configurations (Ruefle et al., 2014). Small to medium sized organizations with limited resources tend to create incident response teams in an ad hoc, reactive manner at the time the incident is detected and then disband the team after the incident response is completed (Ahmad et al., 2012). In large organizations (mostly in the financial sector particularly banks), IR will have a permanent operational-level team addressing a broad range of security and non-security IT incidents (e.g. caused by acts of human error or failure, forces of nature such as fire, flood, lightning, earthquakes, and technology failure arising from hardware malfunctions or software defects as well as breaches to digital assets) (Hove, Tarnes, Line, & Bernsmed, 2014). In such organizations IR teams are called into action when an incident is detected but is otherwise engaged in preparation and follow-up activities at other times. A key part of the follow-up phase is drawing insights and learning from past incidents to improve future incident response performance.

Organizational Learning in Incident Response and Security Management

Organizational learning as a field of research examines how organizations develop knowledge and 'routines' to guide their behaviors (Argyris & Schön, 1997; Dow, Hackbarth, & Wong, 2013; Pahor Škerlavaj, & Dimovski, 2008). The organizational-learning literature makes an important distinction between types of learning. Single-loop learning is a simple process of 'error correction' whereby any deviation from established organizational objectives, policies and norms is corrected. Single-loop learning, or adaptive organizations aim to correct existing problems in their routines by making incremental changes only. However, double-loop learning involves questioning the assumptions and principles underpinning practices and norms (Argyris & Schön, 1997; Huber, 1991; Shrivastava, 1983; Walsh & Ungson, 1991). Double-loop learning, or generative organizations, engage in cycles of experimentation and feedback through the restructuring of strategies, norms and processes. For organizations operating in turbulent environments, double-loop learning offers the unique opportunity to compare established norms with the changing environment and institutionalize the necessary changes into organizational routines.

To better explain the relationships between key constructs in organizational security defense we make use of a metaphor. As Bacharach (1989) points out, metaphors are precursors to theory. Organizational security defense can be conceived as a metaphorical 'shield'. The shield is made up of the collective formal controls (e.g. risk management, policy and procedures), informal controls (e.g. training), and technological controls (e.g. firewalls, intrusion detection systems, encryption layers) (Dhillon, 2018; Sveen et al., 2009). These work together to provide coverage against risk exposure (e.g. the 'size' and 'shape' of the 'shield') as well as multiple overlapping layers in a defense-in-depth formation (e.g. the 'thickness' of the 'shield'). Despite the existence of such a shield, incidents will occur (holes/flaws in the 'shield' are exploited). Incident response eradicates the cause of the incident and restores the organization to its original state.

However, incident response also provides the organization with opportunities to learn. Single-loop learning occurs when organizations only take 'corrective actions' by patching existing vulnerabilities (Ahmad et al., 2012; Ahmad et al., 2015). This is equivalent to plugging holes in the metaphorical shield to improve the overall level of protection against threats. Double-loop learning occurs when organizations restructure and optimize their security strategies, norms and processes to address the challenges posed by evolving attack vectors from the threat landscape and thereby remove root causes of vulnerabilities in the security system (Ahmad et al., 2015; Baskerville et al., 2014). This is equivalent to changing or transforming the shield itself (e.g. 'size', 'shape', and 'thickness') rather than improving the existing shield.

How much an organization can benefit from single loop and double learning depends on the extent to which ISM and IR functions are integrated and how strong or weak the links are. A strong link between ISM and IR allows for both functions to learn from each other's experiences and develop together whereas a weak or absent link presents a barrier to the organization's ability to meet its current security objectives or develop new and more appropriate ones.

The following section elaborates on the impact of weak or absent links by identifying the barriers to organizational learning. We present a hypothetical scenario of a security response to an incident that is perceived to be low-impact (from an IT availability perspective) but represents a strategic security risk to the firm's competitive advantage. The disconnect events in the scenario has been drawn from the behaviors and justifications found in the literature

from Ahmad et al. (2012), Ahmad et al. (2015), Grispos et al. (2015), Hove et al., 2014, Koivunen (2010), and Line et al. (2014).

The Disconnects – Security Management & Incident Response

Scenario: *Forsberg Industries manufactures high performance vehicles capable of generating more than 1300 horsepower that can accelerate from 0 to 100 km/h (62 miles per hour) in 2.9 seconds. Their competitive advantage is the ability to forge superior aerodynamic bodies made of ultra-light advanced composite materials. In May of 2017 one of Forsberg's R&D servers crashed unexpectedly. The IT incident response team restored the device within 24 hours allowing the firm to continue working with minimal disruption. Incident responders noted that the server logs had been deleted, however as the incident was not deemed to be 'critical', there was no formal post-incident report generated and the note about the log deletion was not picked up by security managers. Two years after the server incidents, Trans-Atlantic Performance Industries released a high-performance vehicle with similar design and construction features to Forsberg's NextGen supercar.*

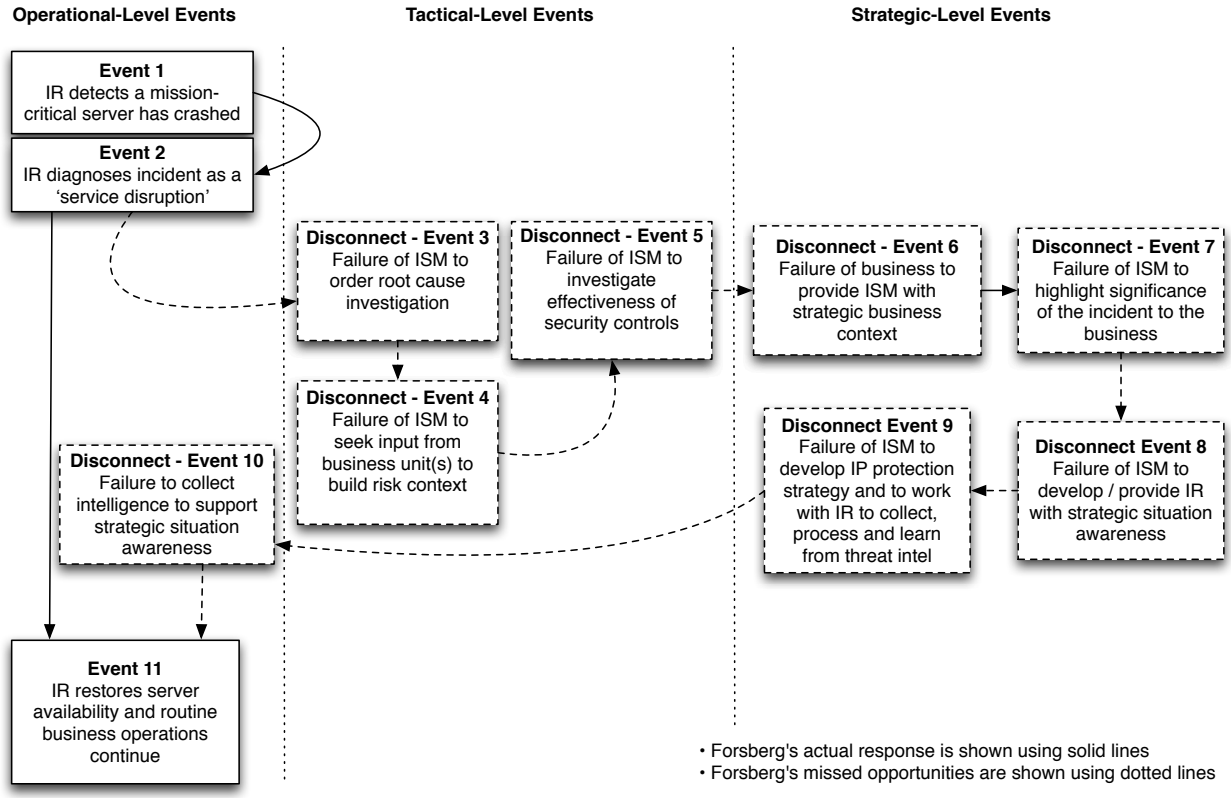

Figure 1: Disconnects between Forsberg's key organizational functions

Tactical Level Disconnect

Forsberg's Incident Response team detects the mission-critical server has crashed [Figure 1 – Event 1]. The team diagnosed the incident as a minor 'service disruption' [Figure 1 – Event 2] and acted immediately to restore the server to minimize disruption to the organization's routine functions [Figure 1 – Event 11]. Given the incident was minor and did not meet the 'critical' or 'high impact' threshold, the server was not forensically preserved and only a log entry documenting the date/time, server id, incident type, and handling personnel was created (Forsberg's response to minor incidents is typical of organizations as can be seen in the case studies in Ahmad et al. (2015), Hove et al. (2014), Koivunen (2010), and Line et al. (2014)).

Security managers were not notified of the incident and no post-incident review report was generated and circulated.

The disconnect between IR and ISM results in several missed learning opportunities at the tactical level: (1) ISM did not investigate the IT incident to determine if the breach was the result of a malicious attack on the organization, how the attacker penetrated Forsberg's defenses and what other activities the attacker might have undertaken in the Forsberg IT ecosystem (Ahmad et al., 2012, p. 650; Grispos et al. 2015, p. 10) [Figure 1 – Disconnect Event 3]. The root cause investigation was critical to Forsberg's decision whether to immediately patch the 'holes' (possibly warning the attacker they had been discovered) or delay the patch to collect intelligence and evidence about the attacker's motives (such intelligence would have been critical to strategic-level security planning); (2) ISM did not determine the contents of the R&D server and seek input from the relevant business units to assist a strategic-level assessment of business risk (Ahmad et al. (2012, p.650; Grispos et al. 2015, p. 10, Hove et al. 2014, p. 32) [Figure 1 – Disconnect Event 4], and (3) ISM did not use the incident as an opportunity to conduct a broader investigation into the effectiveness of the security controls that were circumvented or the suitability of the existing overarching security strategy informing control selection (Ahmad et al. (2012), p.651; Line et al. 2014, p. 52) [Figure 1 – Disconnect Event 5].

Implications

Forsberg was successfully penetrated by a competitor seeking to steal its IP. However, even after the firm detected the incident, the firm's security readiness remained at a low level, its perceived security risks did not change, and it did not take the opportunity to engage in learning by eliminating the vulnerabilities that allowed the attacker to penetrate Forsberg's defensive 'shield' (single-loop learning). Further, from a business perspective, Forsberg's IP assets remain exposed and business executives remained unaware that the incident triggered a series of events resulting in the erosion of the firm's capability and competitive advantage (more IP and sensitive information were stolen, staff with competitively sensitive knowledge left Forsberg to join Trans-Atlantic Performance Industries).

Instead, the firm's response was to simply restore the infrastructure service affected. This was a missed opportunity to mount an effective response to protect the critical business asset (and protect other business assets) as opposed to just restoring the integrity of the infrastructure.

Strategic Level Disconnect

Forsberg's ISM team was not aware of the significance of the incident to the business because of the failure of the business to provide strategic risk context (e.g. potential competitors interested in acquiring IP, competitors' trajectory in developing competing products) (Koivunen 2010, p. 66) [Figure 1 – Disconnect Event 6]. As a result, Forsberg did not highlight the significance of the incident with the business (Koivunen 2010, p. 67) [Figure 1 – Disconnect Event 7]. Forsberg's ISM team had not been providing IR teams with regular and consistent briefings about the strategic business context of the firm and key business and technology risks (Grispos et al. 2015, p. 9; Hove et al. 2014, p. 40) [Figure 1 – Disconnect Event 8]. Forsberg's ISM could have identified potential competitors interested in acquiring IP and modeled each competitor's trajectory towards developing a competing product. From that analysis ISM could have generated a list of security risks (scenarios), target digital assets (e.g. IP but also supply chain information, pricing lists, customized high-precision tools and equipment), and timeframes when competitors were likely to need such information to inform a leakage mitigation strategy (Line et al. 2014, p. 56) [Figure 1 – Disconnect Event 9]. As a result of the disconnect, IR personnel were in a low state of readiness when the attack occurred. They did not forensically preserve the 'crime scene' and

they did not engage in any collection of intelligence to support strategic awareness of the threat and strategy development (Koivunen 2010, p. 64; Hove et al. 2014, p. 40) [Figure 1 – Disconnect Event 10].

Implications

The strategic-level disconnect implies that the firm's response was slow as a result of low readiness and sub-optimal as it only addresses the operational and technological aspect of attacks whilst ignoring the strategic business aspects. Further, the absence of a reliable and continuous stream of intelligence from IR impairs Forsberg's awareness of its security threat environment as well as its perceived security risk exposure. The flow-on impact of these impairments are sub-optimal security strategies as security resources and controls are not used to their best advantage and Forsberg is unable to adapt to the threat environment. As a result, Forsberg did not take the opportunity to engage in learning by evaluating and possibly transforming the existing security strategy/capability to fit its strategic business context, rectify the root causes and thereby better protect IT infrastructure from future penetration and IP from leakage and theft (double-loop learning).

An Integrated Framework for Securing Digital Assets

In this section we present five integration processes (I1 to I5) that link ISM and IR to enhance security response to threats. For each integration process we discuss the single loop and double loop learning opportunities to the organization and specify the particular disconnect events in the Forsberg case scenario (figure 1) that are resolved. In table 3 we summarize the single loop learning opportunities (column 2) and double loop learning opportunities (column 3). The table further links the overall benefit to the organization of the learning opportunities in integration processes I1 to I4 to ISM practices such as risk, policy and SETA (column 4). The benefit to the organization of the learning opportunities in integration process I5 is linked to IR practices such as preparation, identification, containment, eradication and recovery. Figure 2 points out that tactical-level integration between ISM and IR through these five processes enables organizations to engage in tactical-level single-loop learning (solid-line loop) as specified in column 2 of Table 3 and strategic-level double-loop learning (dotted-line loop) as specified in column 3 of Table 3.

Security Benefits from Integration Processes	**Single Loop Learning**	**Double loop learning**	**Organizational learning: Impact on other ISM practices e.g. Risk, Policy and SETA**
I1: Increased Awareness of Security Risks	ISM can analyze incident intelligence for new risks as well as frequency and impact metrics of known risks for incorporation in the risk register	Discovery of new risks (scenarios) and optimization of risk assessment strategies and processes continuously improves organizational awareness of security risks in operating environment	The greater the level of awareness of security risks, the better the coverage of security practices and measures (see areas in table 1) against the range of risk scenarios

I2: Compilation of Threat Intelligence	ISM can identify new threat types and attack scenarios through collection, monitoring and analysis of incident-related information	Evaluation of the quality and utility of threat intelligence about the threat environment improves overall organizational security strategy, practices and tactics	The greater the accumulated threat intelligence against attacking parties, the better the fit of the organization's security posture to the threat environment
I3: Removal of Flaws in Security Defenses	ISM can analyze incident reports to identify failures and precursor-to-failures to identify and remove vulnerabilities in the organization's defenses (e.g. lack of guidance in policy and training)	Continuous learning from incidents of failure (and near-misses) deepens understanding of root causes of flaws in security defenses further enabling modification of underlying security strategies and practices so vulnerabilities can be removed	Increased removal of vulnerabilities (e.g. improving guidance in policy and training for particular risky behaviors, 'holes' in the network perimeter) leads to greater reduction in security risk exposure and higher quality security practices (e.g relating to policies, SETA and technologies
I4: Evaluation of Security Defensive Logic	IR can provide critical feedback to ISM on the effectiveness of existing security defenses. ISM can act on the feedback to take corrective actions by reconfiguring security practices and measures	Evaluating the effectiveness of security defenses against incidents enables organizations to transform their defensive system so that they can proactively and swiftly adapt to an evolving threat landscape	The more proactively and swiftly ISM can restructure strategies, norms and processes of security defenses, the more effective the defenses in protecting the organization from the evolving threat landscape
I5: Enhanced Security Response	ISM provides IR with strategic and tactical guidance on policy, SETA, and technology controls leading to security response capability (enhanced preparation, identification, containment and eradication)	Continuous sharing of strategic and tactical intelligence on enterprise threats from ISM to IR leads to IR transforming its response capability to better fit the organization's risk profile	The more effective the IR function, the greater the organization's ability to identify, contain, eradicate, and recover from security incidents.

Table 3: Securing Digital Assets through ISM and IR - Integration Opportunities and Learning Benefits

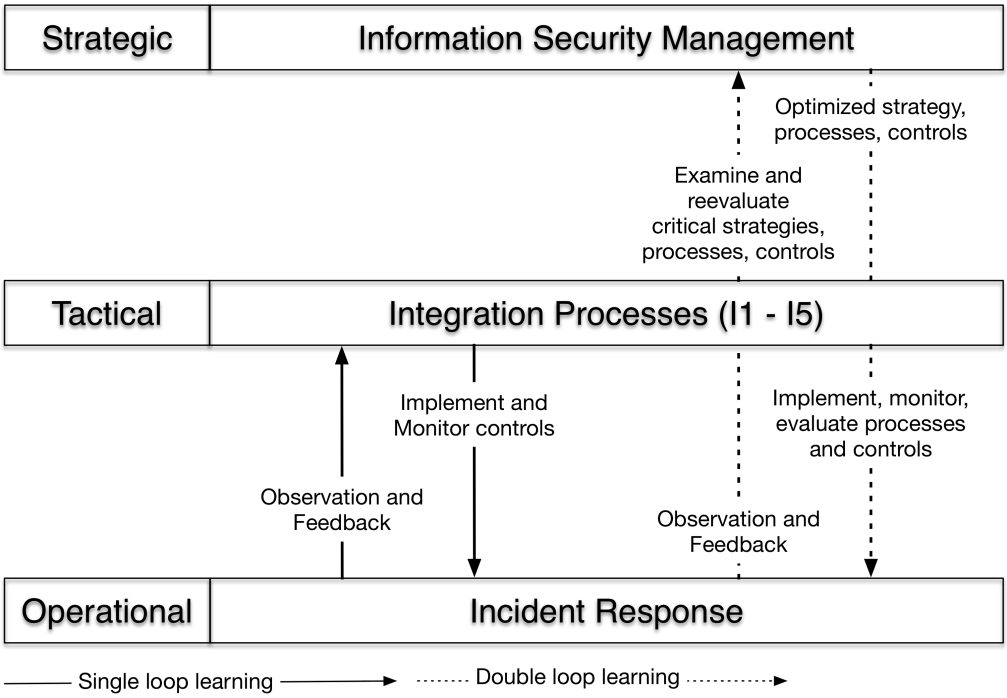

Figure 2: Single and Double Loop Learning through Tactical-level Integration of ISM and IR

I1: Increased Awareness of Security Risks

A security incident is the realization of one or more security risks. Given IR is responsible for the handling of incidents, they are best positioned to collect incident-related information (e.g. a description of the incident scenario including which assets were affected and which controls were implemented, frequency of such incidents, impact to the organization) for processing and analysis by ISM's risk team. Risk scenarios identified by ISM can be compared to the risk register for the purpose of identifying new assets, risks, and vulnerabilities. Further, ISM can mine the collected information for frequency and impact metrics of known risks and reconcile these against previous estimations in the risk register (this would be especially valuable where previous estimations were speculative and relied on qualitative interviews of staff).

Organizations that discover new risks (scenarios) and optimize their risk assessment strategies and processes continuously improve their awareness thereby enhancing their incident response capability. The increased awareness comes from monitoring an increased range of risk scenarios but also from knowledge of their relative criticality (measured as a combination of probability and impact). This ability is critical to developing an effective security strategy and selecting appropriate security controls to mitigate security risk exposure. On the one hand ISM relies on IR's ability to collect incident-related information to inform the risk management process, whereas on the other hand IR relies on ISM to provide sufficient organizational risk context (e.g. key assets and business and technology risks) to guide their collection of incident-related information (addresses Disconnect Event 8 in figure 1).

A weak link between ISM and IR leads to the organization's risk management process being largely speculative without the benefit of insights from ongoing incidents. The flow-on effects of an inaccurate risk assessment are protective strategies and security measures that

are not suited to the organization's risk environment. These include insufficient and/or misleading guidance in policy and training and ineffective or inadequate technology controls. The weak link renders IR isolated leading to their handling of incidents to be largely from a technology-centered perspective where the aim is purely the restoration of infrastructure services as they lack the ability to understand the business context (addresses Disconnect Event 7 in Figure 1).

The greater the awareness of threats to organizational assets (i.e. the number of risk scenarios identified) of an organization, the greater the potential coverage of security controls against the range of scenarios the organization is exposed to. The range and fit of guidance in policy and Security Education Training and Awareness (SETA) can potentially improve with the discovery of more risks scenarios. Similarly, where technological controls can play a role, they too can be developed to increase their applicability and effectiveness. New risk scenarios can be fed forward to IR for training and planning purposes.

I2: Compilation of Threat Intelligence

ISM can give IR teams strategic awareness of risks to digital assets, so they can engage in the collection of security-related 'intelligence'. This can be done while they collect incident-related information as part of their attempts at reconstructing the circumstances of the incident. IR teams routinely interview personnel relevant to the incident as well as collect and analyze information from system and network logs, files on storage devices, surveillance videos, and even phone logs (see the following standards - NIST SP-800-61 (Cichonski et al., 2012) and SANS Incident Handling Guide (Northcutt, 2003). ISM can mine this reservoir of incident-related information to develop detailed profiles of various types of attack (e.g. timing, location, patterns of access) as well as the attacking entity (e.g. IP addresses, targets of interest - these can be gleaned from the attacker's commands if preserved).

Organizations that continuously evaluate the quality and utility of intelligence about the threat environment improve their overall organizational security strategy, processes and tactics. In doing so organizations develop a comprehensive knowledge base of profiles on attackers and associated attack scenarios. The knowledge base is critical to the transformation of security strategy (e.g. selection of security technologies, development of training protocols, policies and procedures to guide behavior) as well as incident response. This is vital in resolving Disconnect Event 9 (Figure 1). Organizations can expect higher levels of readiness against sophisticated attacks and more effective security strategies by leveraging threat intelligence. Therefore, the greater the accumulated threat intelligence against attacking parties, the greater the potential fit of the organization's security posture to the attack(s).

Detailed threat profiles of attackers help to generate richer and more realistic and accurate attack scenarios. These can be used by ISM as a basis for the hardening of security controls and by IR to improve readiness. IR readiness against sophisticated attacks (e.g. APTs) includes developing detailed profiles of attack types (tactics, techniques and tools used in attacks) to inform the development of policy and SETA guidance on how to handle attacks. For example, readiness against an APT attack aimed at stealing IP would start with identifying the information needs of particular competitors and developing a strategy on how to deny the APT access to the complete set of information through compartmentalization (policy, procedures and SETA on where such information is stored, how it is handled and technological controls including systems-level access control, intrusion detection, and Data Leakage Prevention (DLP) systems to help enforce the compartmentalization strategy) (Thompson & Kaarst-Brown, 2005).

I3: Removal of Flaws in Security Defenses

Although IR teams in large organizations may respond to thousands of incidents every year, only a small fraction lead to post-incident learning and reflection. These are usually incidents that are classified as critical or high-impact to the organization (Ahmad et al., 2012; Ahmad et al., 2015; Northcutt, 2003). However, from the perspective of ISM, all incidents that result from the failure of the information security system and even precursor-to-failure incidents (unplanned sequences of events that have the potential for significant impact - also known as near-misses) are valuable sources of learning that can improve organizational security (Ahmad et al., 2012). An incident of a successful attack against an organizational business asset (e.g. IP theft) or technological asset (e.g. denial-of-service of an ecommerce server) provides an opportunity for ISM to learn about the asset (e.g. how the asset form, structure, or location can be changed to make it easier to protect) as well as the cause of the incident as it relates to the 'holes' or vulnerabilities in the organization's defenses.

Therefore, the criteria for selecting an incident for (post-incident) learning and reflection should be expanded to include: (1) the need to increase security learning about critical information assets and associated business or technology risks; and (2) the need to learn about the causal structures of security incidents. Integration can be improved by IR routinely providing ISM with intelligence from failures and near-misses and ISM providing IR with a list of critical information assets and indicators of risk to provide IR with business and technological context to enable the necessary incident selections for learning and reflection.

Organizations that continuously learn from incidents of failure (and near-misses) deepen their understanding of root causes of flaws in the security defenses which further enables them to modify underlying security strategies and processes so that root causes of vulnerabilities in the security system can be removed (addresses Disconnect Event 3 in Figure 1). In fact, increased removal of root causes of vulnerabilities leads to greater reduction of security risk exposure and higher quality security policies, SETA programs and technology controls. Examples of flaws are vulnerabilities in technological security controls, poor or lack of guidance in a policy about particular security behaviors, and inadequate training to address security-related perceptions.

The benefits of single and double loop learning from failures and near-misses flows to the organization's security practice areas (e.g. Risk, Policy, SETA and technological controls). The continuous identification and removal of root causes of vulnerabilities through a double-loop learning process progressively reduces the organization's security risk exposure. These result in higher quality security policies and SETA through the removal of vulnerabilities such as gaps in coverage (i.e. no policy or SETA guidance on important matters) and even misdirected or impractical guidance such as directives that go against the grain of organizational culture.

I4: Evaluation of Protective Logic in Security Posture

Organizational systems of defense typically consist of multiple barriers where each barrier consists of a combination of security practices and technological controls (Baskerville et al., 2014). For example, many organizations use network firewalls to form a perimeter barrier to separate the trusted internal network from the untrusted external network. A second layer of defense can be an intrusion prevention system that analyses network traffic flows and drops malicious packets, blocks traffic from suspect sources and resets network connections. The organization's security strategy (embodied in policies, procedures, guidelines) includes statements defining the kinds of traffic that are acceptable and unacceptable as well as instructions to filter network traffic. These inform the configurations of the firewalls and intrusion prevention systems and form part of barrier security.

However, each barrier in the defensive system has vulnerabilities (Ahmad et al., 2014; Sveen et al., 2009). A successful attack through the network perimeter will typically exploit one or more vulnerabilities. IR teams responding to the attack are therefore well positioned to provide critical feedback to ISM on the specific vulnerabilities that were exploited and the effectiveness of existing security controls. ISM can act on the feedback to take corrective actions by reconfiguring security controls.

Organizations that continuously evaluate the effectiveness of security defenses against incidents are able to transform their defensive system so that they can proactively and swiftly adapt to an evolving threat landscape (addresses Disconnect Event 5 in Figure 1). In fact, the more proactively and swiftly ISM can restructure and transform their strategies, norms and processes of security defenses, the more effective the defenses will be in protecting the organization from the evolving threat landscape. The double loop learning comes from IR feedback to ISM on the (in)effectiveness of specific policies, training programs and technologies that contributed to the incident. This feedback potentially provides ISM with much needed insights into the failures and vulnerabilities of the security. ISM can leverage this feedback to restructure and transform strategies, norms and processes to address the challenges posed by evolving attack vectors from the threat landscape. This is equivalent to changing the metaphorical shield itself (e.g. 'size', 'shape', and 'thickness') rather than improving the existing shield through removing vulnerabilities. Organizational learning permits the organization to gauge if the overarching strategy behind the preventative 'shield' is valid or must be changed to address the evolving threat environment.

I5: Enhanced Security Response

The ISM function can provide IR with strategic and tactical guidance on: (1) policy, for example with guidance on how to handle particular types of security incidents (Northcutt, 2003), what 'intelligence' to collect and evidence to preserve (Sundaramurthy, Bardas, Case, Ou, Wesch, McHugh, & Rajagopalan, 2015) as well how to manage privacy, legal, and contractual sensitivities when accessing / confiscating / preserving information from across the organization (Ab Rahman & Choo, 2015; Ruefle et al., 2014); (2) security education, training and awareness (SETA), to develop the IR team's Knowledge Skills, and Abilities (KSAs) required for handling security incidents in complex, dynamic and stressful environments (Chen et al., 2014). These include perturbation training (forcing operational deviation from established routines); stress exposure training (desensitization to common stressors through exposure); and tactical gaming exercises (simulations and drills honing tactical decision-making) (Steinke et al., 2015); (3) technologies, as they assist IR teams by lending processing power to analysis and can also reduce workload through the automation of routine tasks (Sundaramurthy et al., 2015).

However, when facing the likes of APT, organizations must be able to engage in proactive defense against intelligent/strategizing threats. Defense against APT attacks is a seven-phase operation that requires both ISM and IR to work together in response (detect attack, deny access to digital assets, disrupt attempts to infiltrate a weapon, degrade and deceive to combat APT's command and control capability, contain attempts to exfiltrate valuable information/assets - e.g. see APT scenarios and the corresponding kill chain model in Hutchins, Cloppert, and Amin (2011)). ISM's continuous sharing of strategic and tactical intelligence on dynamic threats such as APTs with IR leads to the transformation of IR's response capability to deal with uncertain and evolving threats. In this case ISM's compilation of threat intelligence will be useful in directing a joint effort of ISM and IR to combat APT maneuvers (e.g. reconfiguring security defenses, hardening systems with valuable digital assets, deploying deception tactics such as honey pots for intelligence

collection, training personnel with access to sensitive information in operational security measures).

Providing IR with strategic and tactical guidance on policy, SETA, and technological support improves the effectiveness and efficiency of the organizational security response. For example, the strong link on policy mentioned above may allow IR to collect sufficient incident-related information and evidence (e.g. from employee emails, folders) to allow the organization to respond to an incident(s) in a swift and timely manner. In the Forsberg scenario a weak link between IR and ISM may have resulted in the IR team being unaware of its privacy, legal, and contractual obligations when accessing information on servers, systems and networks. In this case, Forsberg would have lost valuable time waiting for advice from its policy and legal experts while the attacker erased his/her tracks thereby preventing the organization from effectively responding to the incident. Similarly, strong support from ISM on SETA and technologies may inculcate in the IR team the most suitable response processes and skills and provide the necessary tools to analyze the compromised server and engage in containment and eradication. The primary benefit of enhanced incident response is improved risk mitigation after a security failure has occurred. The more effective the incident response function, the greater the organization's ability to contain, eradicate, and recover from security incidents.

Discussion

Literature widely acknowledges that effective organizational learning is critical if organizations are to overcome barriers in responding effectively to cybersecurity attacks. Industry 'best practice' literature states that organizations should follow-up episodes of incident response with a period of reflection where 'lessons learned' are identified towards improving incident response in the future (see 'Follow Up' in Table 2). Both industry standards and academic literature focus largely on single loop learning – i.e. the need to follow security strategies and processes and to take 'corrective actions' to fix or remove vulnerabilities in organizational defenses (we provide a comprehensive specification of these in Column 2 of Table 3).

Our review of case study literature showed that although large organizations do engage in reflective learning, the learning tends to take place at an operational level and within the IR function resulting in lost opportunities in responding to security incidents and proactively maneuvering the threat environment. In this paper we define what the literature calls 'lost opportunities' in terms of particular disconnects (weak or absent links) between ISM and IR, and we describe the strategic implications to the organization's security risk exposure.

Double loop learning is a critical learning tool for the protection of digital assets in organizations. We use double loop learning to broaden the scope of the reflective 'lessons learned' practice in industry standards to include strategic-level learning in organizations. Further, applying double loop learning enabled us to identify security practices that leverage inter-team collaboration between ISM and IR to drive more effective organizational response to security incidents. Unlike other frameworks and models, our framework is useful because it utilizes single and double loop learning to overcome these disconnects or organizational learning barriers through a series of integration processes that develops inter-team collaboration across operational and strategic levels in large organizations.

For example, had Forsberg's ISM team continuously analyzed incident-related intelligence supplied by IR, they would have likely discovered security risk scenarios related to the intellectual property assets of the firm and conveyed the knowledge to IR resulting in a higher level of readiness when the attack occurred (Disconnect Event 9). Double loop

learning allows organizations to examine and reevaluate the underlying assumptions behind their security strategies and processes and question their utility in order to improve them. By doing so, organizations are able to optimize their security strategies and processes and remove the underlying root causes that make them vulnerable.

Organizations that better integrate their ISM and IR functions are better able to secure their digital assets and proactively navigate the threat environment. The benefit to organizations of single and double loop learning opportunities created by leveraging the two functions depends on the extent to which ISM and IR functions are integrated and how strong or weak the links are. A strong link between ISM and IR allows organizations to better adapt their security defenses to the threat environment whereas a weak or absent link results in stagnating security defenses and presents a barrier to the organization's ability to meet its current security objectives or develop new and more appropriate ones.

Given the vast majority of security research has focused on technical aspects of incident response, this study adds to security research from a management perspective. We believe there has been little research on the role of learning in security management in general, and in particular there has been little recognition of the potential role of incident response as a tool for learning and feedback for wider organizational objectives in particular security management.

From a theoretical perspective, we argue that strong process-level integration of ISM and IR creates single and double loop learning opportunities, which further contributes to improvement in security performance. In other words, the greater the integration between the ISM and IR functions, the more the learning opportunities and as a result, the greater the security performance of the organization (which includes the ability to secure digital assets). Given this relationship, there are further avenues of research that can be studied. For example, researchers can use the integration framework to measure the relationship between organizational conditions and the integration of ISM and IR by using the links identified in the framework. Further, given teamwork is an essential component of achieving 'high reliability', researchers can use our framework to study process-level integration related to cybersecurity response in high reliability organizations (HROs) (Baker, Day & Salas, 2006).

From a practice perspective, organizations can use our framework to enable strong integration between their ISM and IR functions, leverage the learning opportunities, and enhance security defenses and mitigate purposive threats. They can do this by transforming and optimizing the practices of their security and response teams to implement the particular security capabilities and knowledge sharing processes identified in the framework. The framework provides clear learning objectives as well as outcomes and benefits that can be used to assess the strengths and weaknesses of the integration links.

For practitioners, the framework specifies intelligence collection priorities (e.g. intelligence on threats, failures and near-misses, effectiveness of security controls) to enable strategic-level security learning to occur. These priorities are useful in redesigning the response process, particularly the post-incident review phase where the IR team determines lessons learned and reports findings to stakeholders.

For security management practitioners, the framework identifies the specific motivations and benefits of engaging with incident response to improve the effectiveness of security management practices (risk, policy, SETA and technologies) as well as the overall security defensive system. For example, in the case of risk management, greater integration provides a number of benefits such as (1) greater coverage of risks through the identification of new risk scenarios, (2) richer and more accurate risk scenarios accompanied with threat profiles of

attackers, (3) more accurate estimations of likelihood and impact for risks, (4) identification of particular vulnerabilities in existing cyber defenses, and (5) assessments of the effectiveness of existing security controls and the underlying protective logic of the cyber defense system.

Conclusion and Research Directions

Given the rise of intelligent and sophisticated attacks in a complex and rapidly evolving threat landscape, organizations need to adapt their security defensive system and proactively maneuver the threat environment. A key barrier for organizations that have separate and dedicated teams to security practice areas is the weak integration between ISM and IR (lack of communication, collaboration and knowledge-sharing) - a recurring theme in the security literature. This weak integration results in several lost opportunities for security learning and improved enterprise security capability and organizational security performance.

Our primary contribution is a framework grounded in organizational learning theory that comprehensively explains how ISM and IR can be integrated, and the corresponding security-learning opportunities and benefits to the organization. The value of the framework to organizations is in resolving the disconnects between ISM and IR functions by pointing out the opportunities for organizational learning and the particular benefits to security management (i.e. increased awareness of security risks, compilation of threat intelligence, removal of flaws in security defenses, evaluation of security defensive logic and enhanced security response).

There are several opportunities for future research. First, researchers can study organizational learning opportunities in various functional combinations of ISM and IR such as where a specialized security response team is contained within a larger ISM team. Another possibility is to consider if the strategic objectives of ISM become more response-oriented, effectively merging the objectives of the two functions. Second, in this paper the discourse on integration between ISM and IR has been at a whole-of-function level (and to some extent at a practice-area level) because the unit of analysis is the organization and the primary objective is to identify overarching organizational learning benefits arising from linking two traditionally disconnected functions. Researchers can extend this study by discussing integration possibilities between individual ISM and IR practices and the potential flow-on benefits to organizational learning as a consequence. However, it must be noted that learning is a time-consuming and reflective activity and IR typically only has the luxury of engaging in learning in the follow-up phase (and perhaps the preparation phase) but not in the identification, containment, eradication and recovery phases as these are pro-active, not reflective, and extremely time-sensitive for organizations.

Information Systems researchers can test the organizational conditions that make the integrative links between the two functions stronger or weaker. For example, researchers can conduct a series of experiments measuring the situation awareness of ISM and IR teams in various integrative configurations while they engage in a simulated live response to a ‘fast-burning’ crisis. Further, researchers may conduct in-depth and explorative case studies in organizations where IR is more closely integrated with operational network and systems security teams. For example, many telecommunications firms retain Security Operations Centers (SoCs) that perform both prevention and response activities within the narrow scope of IT (analyzing security alerts, triaging breaches, developing cognitive maps as a means of contextualizing and hypothesizing the root cause of alert(s), and coordinating responses) (Zomlot et al., 2016). Researchers can use the integration links in our framework to measure the relative maturity of organizations (i.e. where the integration between ISM and IR is

absent, low, strong or ideal). Further, metrics can be devised to evaluate the strength of the integrative links as part of the overall maturity of the organization.

Future research is also needed to examine how system and organizational complexities impact the integration processes between ISM and IR and the subsequent single and double loop learning opportunities. For example, the more vulnerabilities and complexity in an organization, the more important it is for the organization to utilize the single and double loop learning as both of these learnings enable organizations to identify the underlying weaknesses and assumptions that exist due to the system and organizational complexity and address them through the necessary integration processes for effective learning and subsequent response.

This study can be seen as a first step towards a broader investigation into the application of learning theories in organization response. The literature on organizational learning is vast and contains numerous frameworks, models and perspectives. There are other learning models such as the 4I (intuiting, interpreting, integrating, institutionalizing) framework (Crossan et al., 1999), Information Processing theory (Huber, 1991), the spiral model (Nonaka et al., 1995), and informal learning (Marsick et al., 2001) that may be consulted. Further contributions to organizational response can be made from a decision-making perspective (e.g. strategic decision-making frameworks such as OODA, see Schneier, 2014 and Situation Awareness theory, see Endsley, 1995).

In this research we focused on integration processes between teams rather than interactions within each team and between the organization and threat actors, which requires further research. We did not focus on the effective sharing of security intelligence or information, know-how and the collaborative development of skills and expertise among the individuals in ISM and IR teams. For example, an important study would be to explore the barriers to information and knowledge sharing among ISM and IR such as competing priorities among the teams, diverse conditions of work where IR is under significant time-pressure to resolve incidents and restore services, and need-to-know policy preventing ISM from sharing sensitive intelligence about organizational competitive strategies with IR.

References

Ab Rahman, N. H., & Choo, K.-K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security, 49*, 45-69.

Ahmad, A., Hadjkiss, J., & Ruighaver, A. B. (2012). Incident Response Teams - Challenges in Supporting the Organizational Security Function. *Computers & Security, 31*(5), 643-652.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information Security Strategies: Towards an Organizational Multi-Strategy perspective. *Journal of Intelligent Manufacturing*.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management, 35*(6), 717-723.

Argyris, C., & Schön, D. (1997). Organizational learning: a theory of action perspective. *Revista Española de Investigaciones Sociológicas, 77/78*, 345-348.

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *Academy of Management Review, 14*(4), 496-515.

Baker, D. P., Day, R., & Salas, E. (2006). Teamwork as an essential component of high-reliability organizations. *Health services research*, 41(4p2), 1576-1598.

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

Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*.

Chen, T. R., Shore, D. B., Zaccaro, S. J., Dalal, R. S., Tetrick, L. E., & Gorab, A. K. (2014). An Organizational Psychology Perspective to Examining Computer Security Incident Response Teams. *IEEE Security & Privacy, 12*(5), 61-67.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Da Veiga, A. (2019). Achieving a Security Culture *Cybersecurity Education for Awareness and Compliance* (pp. 72-100): IGI Global.

Dhillon, G. (2018). *Principles of Information Systems Security* B. L. Golub (Ed.) (pp. 1-559).

Dow, K. E., Hackbarth, G., & Wong, J. (2013). Data architectures for an organizational memory information system. *Journal of the American Society for Information Science and Technology, 64*(7), 1345-1356.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human factors*, *37*(1), 32-64.

Finne, T. (2000). Information Systems Risk Management: Key Concepts and Business Processes. *Computers & Security, 19*(3), 243-242.

Gartner. (2017). Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017. Retrieved from https://www.gartner.com/newsroom/id/3836563

Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & Security, 24*(1), 16-30.

Grispos, G., Glisson W. B., & Storer. T (2015). Security Incident Response Criteria: A Practitioner's Perspective. The 21st Americas Conference on Information Systems (AMCIS 2015), (pp. 1-16). Puerto Rico, USA.

Hove, C., Tarnes, M., Line, M. B., & Bernsmed, K. (2014, 12-14 May 2014). Information security incident management: identified practice in large organizations. In *2014 Eighth international conference on IT security incident management & IT forensics* (pp. 27-46). IEEE.

Hutchins, E., Cloppert, M., & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Proceedings of the International Conference on Information Warfare & Security*, 113.

Gost, R. (2008). ISO/IEC 18044-2007. Information technology. Security techniques. Information security incident management]. M.: FATRiM Rossii.

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

Karyda, M., Kiountouzis, E. A., & Kokolakis, S. A. (2005). Information Systems Security Policies: A Contextual Perspective. *Computers & Security, 24*, 246-260.

Kelver, L. (2002). Incident Response in a Global Environment. *GSEC Version, 1*.

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information Security Policy: An Organisational-level Process Model. *Computers & Security, 28*, 493-508.

Koivunen, E. (2010, October). "Why Wasn't I Notified?": Information Security Incident Reporting Demystified. In *Nordic Conference on Secure IT Systems* (pp. 55-70). Springer, Berlin, Heidelberg.

Kotulic, A. G., & Clark, J. G. (2004). Why There Aren't More Information Security Research Studies. *Information and Management, 41*, 597-607.

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2014, May). Information security incident management: Planning for failure. In *2014 Eighth International Conference on IT Security Incident Management & IT Forensics* (pp. 47-61). IEEE.

Manzini, R., & Lazzarotti, V. (2016). Intellectual property protection mechanisms in collaborative new product development. *R&D Management, 46*(S2), 579-595.

Northcutt, S. (2003). *Computer Security Incident Handling: Step by Step, a Survival Guide for Computer Security Incident Handling*: Sans Institute.

Pahor, M., Škerlavaj, M., & Dimovski, V. (2008). Evidence for the network perspective on organizational learning. *Journal of the American Society for Information Science and Technology, 59*(12), 1985-1994.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM, 46*(7), 101-106.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy, 12*(5), 16-26. doi:10.1109/MSP.2014.89

Ruighaver, A., Maynard, S., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Shedden, P., Ahmad, A., & Ruighaver, A.B. (2011, Dec). Informal Learning in Security Incident Response Teams. Paper presented at the 22nd Australasian Conference on Information Systems. Sydney, Australia. (pp. 1-11). University of Sydney.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Information Security Risk Assessment: A Business Practice Approach. *Communications of the Association of Information Systems, 39*, 15.

Shedden, P., Smith, W., & Ahmad, A. (2010). *Information Security Risk Assessment: Towards a Business Practice Perspective*. Paper presented at the Proceedings of the 8th Information Security Management Conference, Perth, Australia: Edith Cowan University.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., . . . Tetrick, L. E. (2015). Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research. *IEEE Security & Privacy, 13*(4), 20-29. doi:10.1109/MSP.2015.71

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *SP 800-30. Risk Management Guide for Information Technology Systems*. Retrieved from https://dl.acm.org/citation.cfm?id=2206240

Sundaramurthy, S. C., Bardas, A. G., Case, J., Ou, X., Wesch, M., McHugh, J., & Rajagopalan, S. R. (2015). *A human capital model for mitigating security analyst burnout.* Paper presented at the In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).

Sveen, F. O., Torres, J. M., & Sarriegi, J. M. (2009). Blind information security strategy. *International Journal of Critical Infrastructure Protection, 2*(3), 95-109.

Tan, T., Ruighaver, T., & Ahmad, A. (2003). Incident Handling: Where the need for planning is often not recognised. *Proceedings of the 1st Australian Computer, Network & Information Forensics Conference*.

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology, 56*(3), 245-257.

Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security, 45*, 42-57. doi:http://dx.doi.org/10.1016/j.cose.2014.05.003

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. A. (2010). Aligning Security Awareness with Information Systems Security Management. *Journal of Information System Security, 6*(1), 36–54.

United States Department of Justice. (2014). U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage [Press release]. Retrieved from https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Verizon. (2018). 2018 Data Breach Investigations Report. Retrieved from https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Webb, J., Ahmad, A., Maynard, S. B., Baskerville, R., & Shanks, G. (2017). *Organizational Security Learning from Incident Response.* Paper presented at the International Conference On Information Systems (ICIS), Seoul, South Korea.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A Situation Awareness Model for Information Security Risk Management. *Computers & Security, 44*, 391-404. doi:10.1016/j.cose.2014.04.005

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., & Ruefle, R. (2003). *Handbook for computer security incident response teams (csirts)*. Retrieved from

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). Boston, Mass.: Centage.

Wilson, M., & Hash, J. (2003). *Building an information technology security awareness and training program*. Retrieved from

Zomlot, L., Sundaramurthy, S., Horne, W., & Bhatt, S. (2016). The Role of Processes in Security Operations Centers *Psychosocial Dynamics of Cyber Security* (pp. 86-103): Routledge.