Cybersecurity Incident Response in Organizations: An Exploratory Case Study and Process Model of Situation Awareness

Atif Ahmad , Sean B. Maynard , Kevin C. Desouza ,
James Kotsias , Monica T. Whitty , Richard L. Baskerville

PII: S0167-4048(20)30395-3
DOI: https://doi.org/10.1016/j.cose.2020.102122
Reference: COSE 102122

To appear in: *Computers & Security*

Received date: 18 September 2020
Revised date: 1 November 2020
Accepted date: 22 November 2020

Please cite this article as: Atif Ahmad , Sean B. Maynard , Kevin C. Desouza , James Kotsias , Monica T. Whitty , Richard L. Baskerville , Cybersecurity Incident Response in Organizations: An Exploratory Case Study and Process Model of Situation Awareness, *Computers & Security* (2020), doi: https://doi.org/10.1016/j.cose.2020.102122

Cybersecurity Incident Response in Organizations: An Exploratory Case Study and Process Model of Situation Awareness[1]

Atif Ahmad[a], Sean B. Maynard[a], Kevin C. Desouza[b], James Kotsias[c], Monica T. Whitty[d], Richard L. Baskerville[e]

[a]School of Computing and Information Systems, The University of Melbourne, Parkville, Australia

[b]QUT Business School, Queensland University of Technology, Queensland, Australia

[c]Deakin University, Burwood, Australia

[d]UNSW Canberra Cyber, UNSW (Canberra), Canberra, Australia

[e]Robinson College of Business, Georgia State University, Atlanta, Georgia

atif@unimelb.edu.au

seanbm@unimelb.edu.au

kevin.desouza@qut.edu.au

james.kotsias@deakin.edu.au

monica.whitty@unsw.edu.au

baskerville@acm.org

Abstract

Organized, sophisticated and persistent cyber-threat-actors pose a significant challenge to large, high-value organizations. They are capable of disrupting and destroying cyber infrastructures, denying organizations access to IT services, and stealing sensitive information including intellectual property, trade secrets and customer data. Past research points to Situation Awareness as critical to effective response. However, most research has focused on the technological perspective with comparatively less focus on the practice perspective. We therefore present an in-depth case study of a leading financial organization with a well-resourced and mature incident response capability that has evolved as a result of experiences with past attacks. Our contribution is a process model that explains how organizations can practice situation awareness of the cyber-threat landscape and the broad business context in incident response.

Keywords: cybersecurity management; information security management; incident response; cybersecurity; situation awareness; case study; process model.

1.0 Introduction

The rise of organized, sophisticated, and persistent cybersecurity attacks poses a significant challenge for modern organizations. Knowledgeable, well-trained and methodical human attackers use sophisticated tools and techniques to disrupt and destroy critical cyber infrastructures, deny organizations access to their own IT infrastructures and services (e.g.

[1] A research-in-progress (short) version of this paper was published at the International Conference on Information Systems, 2020

ransom-ware attacks), and steal sensitive information including Intellectual Property, trade secrets and customer data (Ahmad et al. 2019; Lemay et al. 2018). Such attacks may have negative consequences for organizations including: loss of competitive advantage, productivity, reputation and customer confidence; legal penalties and direct financial loss (Ahmad et al. 2019; Lemay et al. 2018).

Verizon's 2020 Data Breaches Investigations' reported that outsiders perpetrated 70% of the surveyed 157,252 incidents (Verizon 2020). Of these externally initiated incidents, 55% were committed by organized criminal groups and 12% by groups affiliated with state or state-affiliated threat-actors. Given the business impact of cybersecurity incidents, the level of expenditure in information security has dramatically increased in recent years. Worldwide spending on cybersecurity solutions is expected to have reached $123.8 billion in 2020 (Gartner 2020). As these surveys suggest, even though organizations have significantly increased their investment in cybersecurity, incidents continue to rise.

Understanding how organizations can protect their information resources from sophisticated and persistent cyber-attacks is a significant challenge for both research and practice. Incident response takes place under considerable time pressure in a dynamic and rapidly changing organizational environment with high levels of information load, information diversity and task uncertainty (Steinke et al. 2015). Incident response requires command, control and coordination of diverse people, processes, and technologies to develop situation awareness of the threat and incident environment within a rapidly evolving organizational context (Steinke et al. 2015). At the same time the positioning of incident response teams in IT support operations creates resourcing constraints as IT is widely seen as a cost-center rather than revenue generator (Peppard 2018). This constraint is a key reason why incident response tends to focus on the operational objective of IT continuity as opposed to the strategic objective of defending information resources (Ahmad et al. 2019).

Our review of the literature suggests that Situation Awareness is a critical attribute of organizational incident response. Situation Awareness is a measure of the human decision-making that is required to navigate the complexity of incident response in a dense socio-technical environment (Endsley 1995; Webb et al. 2014). A key reason to acquire Situation Awareness is to resolve the asymmetry between the effort exerted by cyber attackers to breach organizational security and the efforts of incident responders in defending the organization from attack (Komárková et al. 2018; Line et al. 2014; Macabante et al. 2019). Considerable effort has been invested in studying the technological aspects of developing Situation Awareness. However, there has been comparatively less focus on studying the practice perspective. In particular, there are few if any case studies that explain how organizations practice Situation Awareness in incident response.

We therefore pose the following research question: *"How can organizations practice situation awareness in incident response?"*

We first review academic and practitioner literature on the traditional cybersecurity incident response function in organizations and reflect on the lack of situation awareness in existing 'best practice' advice. To answer the question, we apply Situation Awareness theory to cybersecurity IR. After justifying our research method, we describe the IR capability of a mature and well-resourced function in a leading financial organization. Drawing on the theory of situation awareness and our case study findings we prescribe a generalized process model to explain how Situation Awareness can be practiced in IR. Finally, we highlight our contributions to theory and practice and conclude with future research directions.

2.0 Background

2.1 The Role of Cybersecurity Incident Response in Organizations

Organizations invest in a metaphorical "shield" made up collectively of formal controls (e.g., risk management, policy, and procedures), informal controls (e.g. training), technological controls (e.g., firewalls, intrusion detection systems, anti-virus software, layers of encryption), physical controls, administrative controls (e.g. COBIT, ISO/EIC 27001, NIST 800-53) and regulatory frameworks (e.g. GDPR, PCI-DSS, SOX, HIPAA) (Ahmad et al. 2020; Alshaikh et al. 2014; Dhillon 2018; Sveen et al. 2009; Weishäupl et al. 2018). The purpose of the shield is to prevent cyber-attacks from impacting organizational assets. However, organizations acknowledge that from time to time the shield will fail (e.g. holes/flaws in the "shield" are exploited by cyber-attacks). The role of IR is to restore the integrity of the shield by detecting the occurrence of an incident, containing the impact of the incident as much as possible, and eradicating the threat from the organization.

Organizations implement their IR function in diverse configurations. In small to medium sized organizations, IR might be conducted by the IT manager, a small team drawn from the IT unit, or may even be outsourced. Due primarily to resourcing constraints, incident response teams (IRTs) in small to medium sized organizations tend to be created in an ad hoc and reactive manner at the time the incident is detected (Ahmad et al. 2012). Large and well-resourced organizations particularly in the finance, telecommunications and defense sectors are likely to have a Security Operations Centre or SOC for continuous monitoring, analysis and response to security incidents across a large attack surface (networks and systems, servers and databases, network and wireless access points) (Agyepong et al. 2019). Having a SOC gives organizations a considerable advantage as incident handling teams, processes, and technologies are institutionalized into organizational routines and do not have to be set up reactively after the incident has already occurred. Little is known about the structure, processes and practices of SOCs in organizations as there are no standardized frameworks and very few case studies of practice (Schinagl et al. 2015). SOCs increasingly use adversary models of the cyber-attack lifecycle (e.g. Lockheed Martin's Cyber Kill Chain (Hutchins et al. 2011) and Mitre's ATT&CK (The Mitre Corporation 2017)) for Situation Awareness in the IR process (Ahmad et al. 2019). The use of attack lifecycles enables SOC analysts to engage more directly with the objectives of the attacker (i.e. to investigate how far attackers have progressed towards their objectives and to interrupt or delay the attacker from further progression). However, for these actions to be effective, organizations need significant Situation Awareness of the threat environment as well as the attack surface (organizational assets and operations).

Incident response has been conceptualized as linear and plan-driven process models consisting of sequential stages (Cichonski et al. 2012; West-Brown et al. 2003). According to the traditional IR process model (figure 1), IR teams prepare for incidents by building the requisite technological toolkits, response processes, and governance structures (e.g. policies, accountability). Once an incident has been identified, IR teams diagnose the circumstances and the type, nature, and scope of the incident. The next step is to contain the incident from causing further impact to the organization. In the case of high severity incidents, this step may involve taking mission critical systems offline. Eradication requires the IR team to identify and remove the root cause of the incident (e.g. malware in organizational networks and systems). In the recovery phase, the IR team restores IT services to their routine operations. Finally, the follow-up phase allows for reflection on the incident handling experience where 'lessons learned' are incorporated into standard operating procedures.

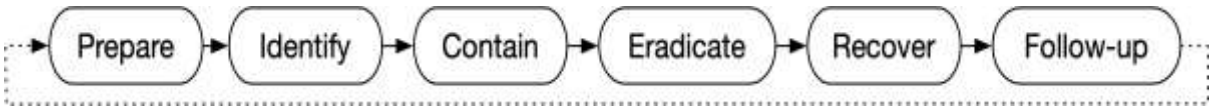

Figure 1: Traditional Incident Response Process Model

2.2 Situation Awareness in Cybersecurity Incident Response

Effective response to a cyber-attack requires incident response teams to develop Situation Awareness of a complex, evolving and dense socio-technical environment (Franke and Brynielsson 2014). Cyber-Situation Awareness is a specific kind of Situation Awareness which is directed at the digital environment and involves the integrated use of digital technology (henceforth we will refer to Cyber-Situation Awareness as Situation Awareness). Although there has been considerable research on Situation Awareness from a technological perspective, there has been comparatively less research focusing on the practice perspective.

Best-practice industry standards are presented from an operational and technology-centered perspective. The focus is on explaining how front-line personnel can detect, contain, eradicate, and recover from cybersecurity incidents. In some cases (e.g. NIST SP 800-61 - Cichonski et al. (2012)), very brief and general advice is provided on organizing an incident response capability which touches on the need for an incident response plan and procedures and establishing a team with select personnel to carry out the responsibilities. In the case of the NIST SP 800-61, the technology dimension of situation awareness appears as directives to compile, process, communicate and fuse incident-related information: (1) establish alerts by identifying precursors and indicators, (2) create channels of communication with outside parties, (3) implement logging and auditing of systems, and (4) profile networks and systems, (5) understand the normal behaviors of networks, systems and applications, (6) increase storage of information/evidence once an attack is suspected, and (7) correlate information across multiple sources of information.

The research literature acknowledges that Situation Awareness is a complex and multi-faceted attribute of humans that is developed through a cognitive process. There have been at least two comprehensive and systematic reviews of Situation Awareness (see Franke and Brynielsson (2014) followed by Jirsík (2018)). Both argue that Situation Awareness has been studied from technological and cognitive perspectives. As this paper is on the practice of incident response, we only provide a brief overview of the technology and cognitive research in the broad area of Situation Awareness.

From a technological perspective, Situation Awareness is framed as a problem of collecting relevant and useful information (i.e. ‘collect the dots’), fusing together key elements of the information (i.e. ‘connect the dots’) and deriving insights from the fused information (‘project from the dots’). Jirsík (2018) profiles key contributions and hubs of activity in Situation Awareness research. He points to active research teams at George Mason University (specializing in modeling, predicting and visualizing attacks as well as modeling to explain and measure Situation Awareness), US Army Research Laboratory (modeling risk and simulating cyber defense scenarios particularly in industrial control systems), Swedish Defense Research Agency (using attack personas to model attacker behavior among other contributions), Rochester Institute of Technology (also researching attack modeling and prediction with particular interest in multi-stage attacks) and the Austrian Institute of Technology (Situation Awareness in smart grids, network anomaly detection and decision support models in security operations centers).

From the human-centered perspective, Situation Awareness is seen as a dynamic cognitive process where the human operators need to acquire and continuously renew Situation

Awareness with new IR-related information from the incident environment (Rajivan and Cooke 2017). Here the focus has been on studying how operators (and teams of operators) acquire and maintain certain levels of Situation Awareness in IR by drawing insights from the IR-related data. A focal topic of interest has been team cognition in cyber defense (Cooke et al. 2013). Researchers have studied knowledge structures and conducted cognitive task analysis to study team effectiveness and mental models (Chen et al. 2014) as well as diagnostic work processes (Werlinger et al. 2010). Multi-disciplinary methods such as human-in-the loop experiments, agent-based modeling, and root cause analysis have been employed to study and interpret team interactions and cognitive biases in cyber defense tasks such as triage and correlation of incident-related information (Rajivan and Cooke 2017).

Incident response has recently been the subject of case study research. These studies have examined broad challenges (Bartnes et al. 2016; Hove et al. 2014) organizational learning (Ahmad et al. 2015), the applicability of safety management (Line and Albrechtsen 2016), integration of pro-active learning and socio-technical perspective in management models (Jaatun et al. 2009), the strategic balance between prevention and response (Baskerville et al. 2014) as well as broad sector-specific studies (Catota et al. 2018; Line 2013). However, to the best of our knowledge, Situation Awareness in incident response has not been the focus of any practice studies. The limited body of literature relevant to this perspective states that the IR function has been traditionally constrained by organizational structure, policy, and maturity due to its positioning in IT support operations (Ahmad et al. 2020; Nyre-Yu et al. 2019). Further, that personnel lack sufficient authority to carry out their responsibilities and grow the role and function of the team (Nyre-Yu et al. 2019). From a resourcing perspective (in non-IT firms), IT is seen as a cost-center rather than a revenue generator (Peppard 2018). Therefore, IR's activities are subject to the same constraints as IT, which constrains its ability to carry out enterprise-level response to cyber-attacks (Nyre-Yu et al. 2019). This is a key reason why IR in many organizations focuses on the operational objective of maintaining IT continuity rather than the strategic objective of actively defending organizational information resources (Ahmad et al. 2019).

Where IR is implemented in a strict hierarchical structure (e.g. a SOC), uneven distribution of expertise becomes a barrier to knowledge sharing between analysts (Nyre-Yu et al. 2019). Organizational Situation Awareness is 'brittle', confusing and unreliable because it is based on loosely connected analysts rather than a genuine team-based activity (Cooke et al. 2013). This is primarily because individual achievement and knowledge 'hoarding' is rewarded over and above team success and knowledge sharing, a by-product of the way reward structures and personnel selection practices work in organizations (Cooke et al. 2013). This lack of shared awareness extends to stakeholders, particularly with mid and senior level managers, CISOs and other security personnel that liaise with other divisions and groups that must be notified to create shared situation awareness with management (Nyre-Yu et al. 2019).

3.0 Theoretical Lens

There are four main theories or approaches in the study of situation awareness. The most dominant theory is that of Endsley (1995) that takes an information processing approach. Others as discussed in Neville and Salmon (2016) are situation awareness as knowledge state which adopts a human workload perspective, Ecological Theory focusing on action-perception and Activity Theory which also takes an information processing perspective. We selected Endsley's theory of Situation Awareness as the theoretical lens for this study (Endsley 1995). Our rationale is that it (1) frames Situation Awareness as a decision-support process for a single operator which corresponds to our objectives of understanding a single organization's decision-support, (2) contains arguably the simplest conceptualization of

Situation Awareness centered on three broad theoretical constructs (perception, comprehension, projection) making it practically useful as an analytical lens for an in-depth case study, (3) has been the theory of choice for cybersecurity researchers studying incident response as we deduced from our literature review, (4) is the most empirically validated model among the descriptive models in the literature, and (5) has been applied to the wider socio-technical environment (see Endsley (1995) for examples of applications).

Endsley defines Situation Awareness as: "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future". We therefore define Situation Awareness in IR as "*perception of incident-related elements within the organizational environment over the course of the incident, comprehension of their meaning within the context of the organization's cybersecurity mission and objectives, and the projection of their status in the near future*". Note we interpret 'space' to be all elements related to the incident, 'time' to be the duration of the incident, and 'meaning' to be interpreted in the context of the organization's mission and objectives.

Endsley conceptualizes Situation Awareness as part of a broader process model for human cognition that is framed from an information-processing perspective. Situation Awareness is an operator's 'state of knowledge' that can exist at three different levels – perception, comprehension, projection. The three states of Situation Awareness collectively lead to decision and action. The interaction of the operator with the real-world environment results in further modification of the operator's mental model which directs further actions (see figure 2).

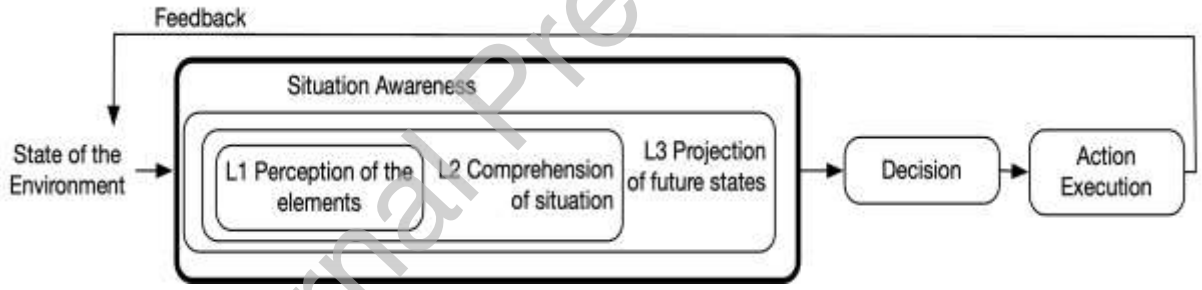

Figure 2: Situation Awareness of the Environment (adapted from Endsley (1995)**)**

Perception is a state-of-knowledge that reflects the operational picture of the environment. Perception results from the collection of raw information through activities such as sensing the environment, receiving messages about the environment, or even interacting with the environment. It is important to note that the operator does not integrate key elements of the raw information to draw meaning as this takes place in other levels. *Comprehension* is a higher order state-of-knowledge resulting from the operator 'connecting the dots', i.e. integrating key elements in the operational picture into their mental model so their significance to the operator's objectives and mission become apparent. *Projection* is the third and highest order state-of-knowledge of Situation Awareness that results from the agent extrapolating from their existing mental model to generate alternative states of the system and environment in the future. *Projection* is purposeful and supports goal-oriented decision-making - the operator assesses the situation and interprets what will happen in the future in the context of its goals and objectives as a basis for future decision-making.

Decision and action execution are separate stages that are distinct from Situation Awareness but follow from it. Situation Awareness therefore exists in a support role for decision-making and execution rather than part of it. *Decision* is where the operator selects a course of action

among the possibilities identified in Projection. *Action Execution* is where the operator implements the course of action previously selected in the Decision stage of the Situation Awareness framework to change the real-world environment. The final stage of action impacts the real world which is ultimately perceived by the operator through its Situation Awareness.

4.0 Research Approach

To explore how organizations can improve their Situation Awareness when responding to cybersecurity attacks, we undertook a qualitative research approach. Qualitative methods allow us to develop a rich picture of phenomena within an organization and allow us to investigate aspects that may not be obvious at the outset of the research project (Boudreau and Robey 2005; Eisenhardt 1989; Klein and Myers 1999; Yin 2018). The empirical data in our paper comes from a single in-depth, revelatory case. Single case studies are particularly useful in research where there are few cases to report and an in-depth understanding of the phenomena is required. Scholars have argued that when a single case study is used, the researcher is better able to question old theoretical relationships and explore new ones (Yin 2018). Our case study is revelatory for two reasons. First, the case is of a unique phenomenon, that being an IR function that has developed a high-level of situation-awareness as a result of learning from past responses to cybersecurity incidents. Second, there are very few case studies of IR in the literature primarily because gaining access to an organization to investigate cybersecurity is extremely difficult due to the sensitivity of the operations in question. This is well known among cybersecurity researchers in this area (Kotulic and Clark 2004; Paul and Whitley 2013).

FinanceCentral (pseudonym) is a large multinational finance organization with a market capitalization equivalent to forty-four billion US dollars. The firm operates in 34 countries, serves over nine million customers worldwide and employs over fifty thousand personnel. The firm has two strategic-level cybersecurity objectives: to maintain IT service availability and to protect confidentiality of customer data. The firm recently underwent a significant structural and process transformation to break down silos, flatten its hierarchical structure and improve its decision-making agility. As a result, the firm is being driven by smaller teams that are more collaborative and self-directed. We selected this firm as it: (1) has an in-house, well-resourced and permanent 24 x 7 IR function that is mature and relatively stable for the last five years, (2) evolved 'best practice' IR from experiences of highly sophisticated cyber-attacks, and (3) allowed the researchers unfettered access to the relevant stakeholders.

Data was collected using semi-structured interviews which lasted between one and three hours each. The first set of questions established the interviewee's role and responsibilities in the IR function. The second set asked the interviewee to walk the researchers through the organization's response to a 'high severity' cyber-attack while describing the organizational structure, coordination among teams, team dynamics, routine behaviors, reporting structure and communication protocols. The third set of questions was prefaced by a brief explanation of Situation Awareness. The interviewees were then asked to walk through the response a second time while explaining how the firm acquired its perception, comprehension, and projection. Interview data was transcribed verbatim and coded using open, axial and selective coding (Neuman 2014). Multiple passes were performed through the data to cluster the quotes and identify recurring themes that addressed the research question. Table 1 lists the interviewees at *FinanceCentral*. Whilst we were able to interview participants at each level of the IR process in *FinanceCentral*, we were limited to one representative for each stakeholder group (Level 2 SOC analysts were covered by a combination of Level 1 and Level 3) due to the sensitive nature of IR operations and because staff were handling a large volume of

incidents at the time. The only exception was *Lead_CyberStrategy*, who we interviewed three times. The purpose of the subsequent interviews was to refine and subsequently validate the final process model.

Table 1. Interviewee Profiles

Pseudonym	Role	Years in Role
Lead_CyberOperations	Lead - Cybersecurity Operations	5 years
Lead_SOC	Lead - Security Operations Centre and Level 3 Analyst	4.5 years
Lead_CyberStrategy	Lead – Cybersecurity Strategy	3 years
Liaison_ThreatIntel	Senior Threat Intelligence Analyst	1 year
L1Analyst_SOC	Security Operations Centre – Level 1 Analyst	1 year
CISO	Chief Information Security Officer	3 years

5.0 *FinanceCentral*: A Case Study of Exemplar Situation Awareness in Incident Response

FinanceCentral's cybersecurity operations team is responsible for the protection of information resources. The function manages twenty billion data events each day that are generated from across the firm's heterogeneous technology estate. *FinanceCentral*'s IR capability is driven by its 24x7 SOC. The SOC employs 25 personnel with the greatest number involved in daily incident management, a much smaller number of 3-4 personnel at Level 2, and only 1-2 at Level 3 including the SOC leader. A separate threat intelligence team consists of an additional 4-6 personnel. A security leadership team (*SecurityLT*) is formed on-the-fly to address high severity incidents. The *SecurityLT* consists of the cyber operations leader (*Lead_CyberOperations*) and the SOC leader (*Lead_SOC*) but may also include others such as the cybersecurity strategy leader (*Lead_CyberStrategy*), a designated liaison with the cyber threat intelligence team (*Liaison_ThreatIntel*) and the other Level 3 SOC Analyst. The firm's *CISO* has oversight over the entire cybersecurity operations and acts as the communication conduit with the firm's senior executive. The information flow and communication pathways are illustrated in Figure 3.

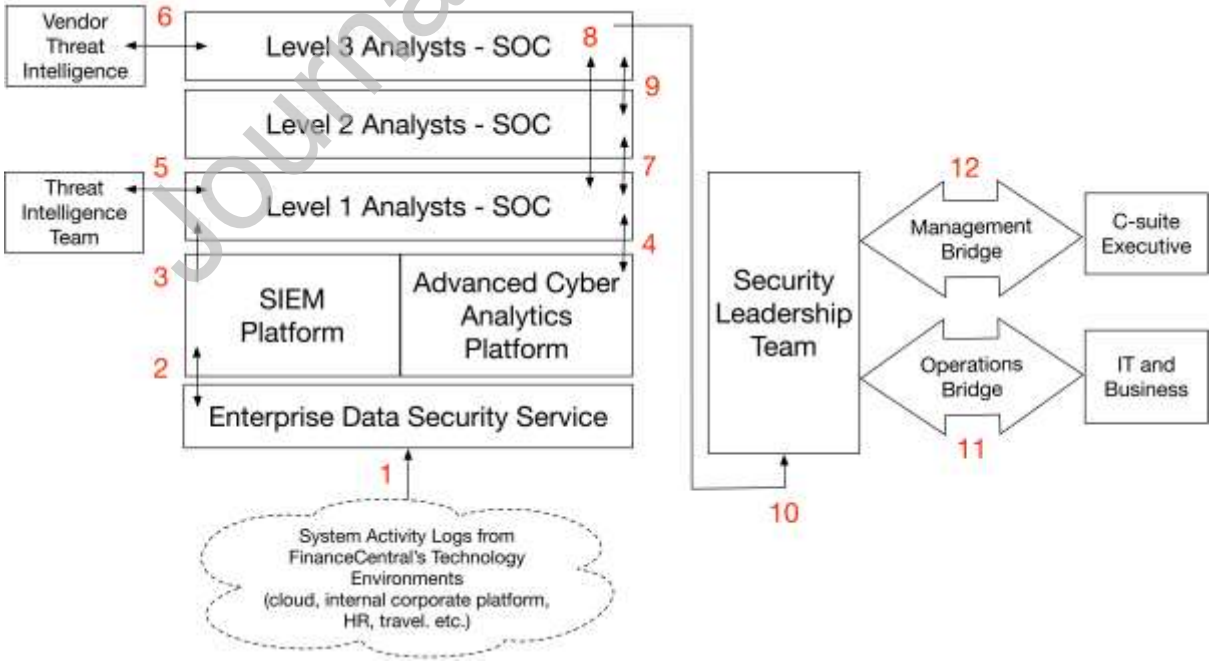

Figure 3: Information Flow and Communication Pathways at *FinanceCentral*

5.1 Cybersecurity Operations at *FinanceCentral*

FinanceCentral has invested in a cyber defensive system that acts as a preventative 'shield' comprising a sophisticated configuration of security technologies incorporating multiple layers of control (firewalls, intrusion detection systems, anti-virus software, and specialized security tools purchased from various vendors). *FinanceCentral*'s cyber defense system is the subject of significant ongoing investment in continuously configuring, testing, and customizing these technologies with bespoke code to mitigate cybersecurity risks in their threat environment. A key objective of the cybersecurity function is to continuously uplift the capability of the protective shield to defend the firm against increasingly sophisticated forms of cyber-attack. In support of this objective, SOC analysts investigate cyber-attacks to reverse engineer Tactics, Techniques and Procedures (TTPs) to develop solutions that can be patched back into the cyber defensive system to uplift the shield's protective capability.

This is supported by *Lead_CyberOperations* who states:

> *"So, within our environment we're very much dependent on what we call layers of security control. So, some of what we do again may not necessarily be deemed as unique but it's in how we manage those layers of control. So when you think about denial of service capability, when you think about our Web application firewalls, whether it's through threat intel, or through what we're seeing through our security partners or security tools, it's how we uplift them. How we put in place bespoke detections, how we uplift that capability. So that's a big part of what we do, how we respond, and how we are agile in the context of the changing threat landscape."*

Referring to how *FinanceCentral* handled two specific incidents, the *Lead_CyberOperations* stated:

> *"What we did specific to both of those incidents, both of those vulnerabilities, is we were able to reverse engineer the exposure. We then built specific new detection rules both on our Web application firewalls for our Internet facing services but also on things like our IPS/IDS, intrusion prevention systems, and therefore lifted our barriers, strengthened our barriers to protect our environment."*

5.2 Incident-related Data Collection

FinanceCentral's Situation Awareness of the environment comes from multiple channels of information collection. The primary avenue is system activity logs from their internal corporate networks, human resources platforms, travel systems, and cloud environments. These are channeled into the 'Enterprise data security service' (arrow 1 in figure 3) and then subsequently into the Security Information and Event Management (SIEM) platform (arrow 2 in figure 3) which correlate and aggregate the data. The SIEM performs real-time analysis of data using a combination of vendor-issued standard detection rules as well as custom detection rules engineered by SOC analysts to report security alerts (arrow 3 in figure 3). *Lead_CyberOperations* describes this:

> *"So, all of this data that I'm talking about, whether it be from third party service, a cloud platform, an internal corporate network, our security tools, our HR system, our travel system, all comes into this environment as raw data. We then have a layer of abstraction so that we can use it for our own security purposes. So, we do that that translation here but then we use it to help us drive what we do from the monitoring, detection and response perspective… the SIEM does additional aggregation and correlation of the data which then helps us drive incidents and the response to that within the security operations team."*

Another important source of information is a custom behavioral analytics platform that reports anomalous staff activity (arrow 4 in figure 3) as described by *Lead_CyberOperations*:

> *"... the other component is around our advanced cyber analytics platform. So, we're probably I think the only financial institution in this region to have built this. It's really best to give you an example. So, we profile every staff member. Well, look at me - as just a just a typical general manager within the organization, over a period of six months, if all of a sudden, I upload data to Dropbox or to GitHub or something like that, then we'll pick that up as anomalous behavior."*

5.3 Threat intelligence

FinanceCentral also receives threat intelligence that helps to direct their Situation Awareness of the threat environment. A key source is *FinanceCentral*'s dedicated team (arrow 5 in figure 3) that collects intelligence from a close-knit network of insiders among financial institutions, law enforcement and intelligence agencies, and specialist vendors such as FireEye. Another key source are referrals from the IT helpdesk and emails from staff reporting email, SMS, and phone phishing attacks. This threat intelligence function is described by *Lead_CyberOperations*:

> *"Threat intel is a dedicated team. And in summary that's the group that has a finger on the pulse of the threat intelligence community. So, they are connected with intelligence agencies, various government bodies, law enforcement, both local and national."*

The team provides operational, tactical, and strategic intelligence to stakeholders in *FinanceCentral*. At an operational level, the team proactively monitors the threat landscape feeding actionable intelligence to L1 SOC analysts (e.g. blocking IP addresses, interpretation of security alerts, possible avenues of investigation). The *Liaison_ThreatIntel* states:

> *"... we're monitoring the broader threat landscape and we want to pass intelligence to the operations team to uplift their existing platforms. We uplift their existing toolset using intelligence. It could be a simple list to block these potential IP addresses. Right? But it could be more along the lines of writing detection rules based on this hunt, this hypothesis, this piece of intelligence where another financial institution was targeted."*

Tactical intelligence involves hypothesizing about threat activity impacting *FinanceCentral* and validating that against the observations of the L3 SOC analysts.

> *"If you're looking at what threat intel does on a day-to-day basis, we're basically creating hypotheses, and then to validate the hypotheses you basically go to the Incident Response, and this is where the reactive - proactive component comes in, right? We pass on to the threat hunters to validate the hypotheses and then the hypotheses generates results and then you deploy the controls proactively even before the attack happens, we are running that whole loop and deploying our controls because we know the potential actor is operating in our geography based on the intel." Liaison_ThreatIntel*

Strategic-level intelligence is about identifying new threat-actors and their TTPs to identify gaps in the firm's cyber defenses that might be exposed and proactively deploy controls into cyber defenses before the exposure is exploited.

> *"Strategic intelligence is identifying what the actors are targeting, what are their TTPs? And then out of those TTPs, once you get the TTPs, it very clearly gives you an overall picture of what are your gaps right now? What are the controls, and what are the gaps?" Liaison_ThreatIntel*

FinanceCentral also benefits from threat intelligence (particularly indicators of compromise or IoCs) embedded in specialized security tools purchased from market leader FireEye and available through the vendor's knowledge portals that they routinely monitor. The SOC leader (*Lead_SOC*) talks about learning from the incident response experiences or engagements of the market leader in threat intelligence:

> *"…they collect IOCs or indicators of compromise from those engagements and feed those directly into their tools. So that's something that happens automatically that helps protect us… they have an intel arm [Mandiant] that can help us prioritize and map out those threats… and what tactics are they using. We then use [that] to prioritize whether we've got detections in place for those, and in many cases, we may need to write custom detections… they already have a portal where we can get lots of reporting around… the financial area in particular and what we'll then do, is monitor [the portal] for those…"*

FinanceCentral has a contract with FireEye's intelligence arm which gives them a direct line to the vendor's threat intelligence and monitoring specialists. For example, these experts will routinely analyze security reports from *FinanceCentral*'s security tools and occasionally place a phone call to the SOC leader directing his attention to specific threat activity on the firm's systems (arrow 6 in Figure 3).

> *"…if they do get a specific hit…I might get a phone call even, and they'll say, hey this particular alert in here, pay attention to this, this actually relates to this particular threat-actor that's been doing X in your area." Lead_SOC*

5.4 SOC operations: Incident Triage and Handling Low-Severity Incidents

Developing the operational picture from multiple fragments of information is a key hurdle for SOC analysts. Security alerts must be interpreted, and the broader context must be pieced together from diverse sources of information (i.e. *FinanceCentral*'s myriad platform environments that span IT and business management). Threat intelligence plays an important role in directing the attention of SOC analysts to specific system activity and forms much of the background context through which security alerts are perceived. Level 1 analysts are responsible for the triage of all security alerts and the handling of low-severity incidents which number approximately 600 to 800 per month. The triage process requires analysts to follow guidelines or 'playbooks', draw on threat intelligence, and apply their training, skills and experience to piece together and make sense of the unfolding incident situation. L1 analysts monitor, prioritize, investigate, and respond to security alerts. This involves assessing risk and building incident context using problem-solving questions in playbooks, escalating high-severity alerts to senior analysts, and coordinating containment, eradication, and recovery for low-severity incidents.

> *"I handle phishing and malware incidents that are usually fairly low priority incidents. So just your day-to-day commodity malware or commodity phishing emails a lot of the time. If I do encounter anything that's more serious, I escalate it to level two. I'm like the frontline, the human frontline defense for FinanceCentral as an organization. We have, obviously, defenses around the perimeter which are our tools and things but I'm the first person who receives the alerts that are generated by those tools and review them and triage them basically." L1Analyst_SOC*

Level 1 analysts (less than 3 years of experience) may seek assistance with these tasks from Level 2 analysts (3 to 5 years of experience) (for example if it's unclear that an incident trigger is a false positive) (arrow 7 in figure 3). Level 3 analysts (5 or more years of experience) develop the playbooks to be followed by junior analysts and mentor them in their

use. They spend 90% of their time on capability uplift and 10% of their time handling (high severity) incidents. L2 analysts spend roughly 50% of their time on capability uplift and the other 50% of their time handling incidents. L1 analysts spend almost 100% of their time handling tickets. They also provide feedback on the utility of the playbooks for low-severity incident handling.

A key challenge when making sense of the operational situation is coping with poor 'visibility' for example due to contradictions and gaps in incident-related information. Junior analysts have less developed mental models, so they are data-driven in that they rely on the processing of the raw data collected through the firm's sensors (e.g. the SIEM). Senior analysts rely heavily on their existing mental models to map out threats and identify gaps in visibility that need to be filled to better understand the operational picture, so they are more goal-directed. This is evidenced by *Lead_SOC*:

> *"…that's part of the experience we're trying to build into the analyst's everyday job, that's one of the major reasons why you need a human analyst rather than being able to automate it. So, their day to day job is really to handle… how do I work with imperfect data? How do I work with data where there's weird contradictions? How do I troubleshoot those contradictions and figure out through experience - if I see this data from this control and this is contradictory data from this control, which one actually makes more sense? Which ones the real thing? Which ones less reliable? How do you marry those two things? In terms of the visibility, that tends to be something that, more the management and L3 layer is much more aware of."*

5.5 Enterprise Response to High Severity Incidents

Low-severity incidents are completely managed by L1 analysts without the need for escalation. High severity incidents such as a confirmed compromise of one or more systems (the specific criteria are confidential) are immediately escalated to L3 analysts by L1 or L2 analysts (arrows 8 and 9 respectively in Figure 3). Suspected sophisticated attacks trigger the formation of the previously described *SecurityLT* (arrow 10 in Figure 3). The *SecurityLT*'s responsibilities in such situations, which tend to be executed in parallel, is to assess the situation, open communication channels to all relevant stakeholders, and direct the enterprise response.

To execute these responsibilities the *SecurityLT* initiates a formal 'managed incident' process which comes with a dedicated technical incident recovery manager. The formal process incorporates two communications platforms or "bridges". As *Lead_SOC* states:

> *"So typically, we've got two paths. Typically, using our technology operations group, we use the major incident management process and through that we've got a platform, we've got mechanisms, we've got a framework in which we can bring everyone together. So, we use that but in parallel, if it's [the incident] big enough, we also use the management bridge and our CISO will help coordinate that. We've got two avenues to bring everyone together."*

Using the operational bridge, the *SecurityLT* can leverage formal communications protocols to compel all twelve technology domain heads of IT as well as the heads of business domains to engage with the incident response process (arrow 11 in figure 3). They will embark on a sensemaking process which will involve more context-building and discussion of the incident approach with stakeholders. Critical decisions will be made swiftly, and tasks will be delegated to contain, eradicate, and recover from the incident. The *SecurityLT* will engage with *FinanceCentral*'s *CISO* and senior executive through the management bridge (arrow 12 in Figure 3). Through this bridge they will conduct regular situation briefings and obtain

signoff on significant decisions (e.g. suspending mission-critical services in a specific part of the world). On-demand communication between the two bridges is critical to *FinanceCentral*'s rapid decision-making and coordination as well as its comprehension of the unfolding situation as it enables the *SecurityLT* to engage in knowledge sharing about the incident and its changing context.

On the sensemaking process, *Lead_SOC* states:

> *"This could be a major incident. And then at that point yes, we'll have a meeting, we'll start drawing on whiteboards what could have been affected, we'll start bringing in the people that we need. So that happens at the point that is triggered".*

The *SecurityLT* will present the senior executive with a risk and impact assessment of the incident. As *Lead_SOC* points out below: the firm's executive is particularly concerned about risk to business management, reputational damage and disclosure of intellectual property and customer data resulting in the obligation to disclose serious security incidents to regulators and the public.

> *"So, they're worried about things like reputational damage, customer information being breached, having to tell the regulators, having to tell the public. So yes, data is a really big one. And I think availability is key as well. But yeah it tends to be, is there a risk to customer data." Lead_SOC*

Communication between the senior executive and the *SecurityLT* is bi-directional. The senior executive may initiate contact with *Lead_CyberOperations* requesting controls to explored to mitigate the risk of a specific scenario.

> *"So, when an event occurs, Lead_CyberOperations typically at some point reports to the CISO or head of cyber-defense or something, and usually at some point after that without a formalized process the CISO will come to us and say, we've had this event. Articulated, it looks like these series of events. What mechanisms can we put in place at the organizational level to stop that? Or control that in some way?" Lead_CyberStrategy*

The senior executive provides the critical ingredient of strategic business context into the sensemaking process, as the *CISO* points out:

> *"If there is motive to be established, it may originate elsewhere in the business, especially if they are intangible — an attack on corporate IP, or an essential asset will rarely originate on the asset itself. Senior executives can provide a broader view to allow operational teams to make sense of a kill-chain and its potential path. The same is true in reverse, being able to trace malicious activity occasionally requires context beyond the technical current state. For example, a machine is compromised containing only an empty datastore — this machine may be earmarked to support a new service offering for analysis of fraudulent transactions. This information isn't always technically obvious, and occasionally only known to the business units with direct ties to the platform. We can close that gap."*

As previously mentioned, the *SecurityLT* uses the operational bridge to consult with, recruit and delegate response activities with the domain heads of IT and Business. Standard response protocols are followed to contain the incident from escalating, eradicating the root cause of the incident and recovering operations to routine function. This involves recruiting personnel from across the organization to engage with the incident response process and directing the critical response phases while keeping the senior executive apprised of progress. A key factor

in *FinanceCentral*'s agility in responding to cyber-attacks is the firm's recent transformation to incorporate flexible organizational structures and processes:

> *"... it's about taking out middle management... so the CISO is the domain lead for the security domain but I am empowered to go directly to the domain leads of all the other twelve domains and engage them at any point in time. So, our new organization structure is about empowering people. There's a whole range of people that we can bring in. But predominantly it's the service owners, the platform owners, the application owners, and the relevant domain leads who ultimately own that environment, who are brought into the discussion." Lead_CyberOperations*

5.6 *FinanceCentral*'s Situation Awareness in Incident Response

FinanceCentral addresses the two key Situation Awareness deficiencies in 'best practice' IR identified in our literature (Situation Awareness of the cyber-threat landscape and Situation Awareness of the broad organizational context) by: (1) acquiring threat intelligence from a number of sources and integrating insights into the response process at operational, tactical and strategic levels (see section 5.3), and (2) knowledge sharing between a specialized security leadership team and stakeholders across the IT, business and senior executive using operational and management bridges (see section 5.5).

Poor Situation Awareness arising from structural and policy limitations of positioning IR in an operational IT unit is overcome by complementing the SOC with a strategic-level leadership team (*SecurityLT*) that has a flexible command and control structure augmented with the requisite authority and communications protocols to implement its decisions (management and operational bridges). This mechanism addresses the need for shared awareness between the IR function and other organizational stakeholders. Shared awareness within the SOC is addressed through the provision of knowledge management platforms as well as a culture of communication and mentoring. Uneven distribution of expertise is addressed by using playbooks and by blurring the boundaries separating the roles and responsibilities between the three levels of the SOC. These initiatives help to increase connectedness among SOC analysts and organizational stakeholders towards more reliable and coherent Situation Awareness.

The case study also shows how the challenges facing SOC analysts can be addressed. The firm converted its proceduralized playbooks to problem-centered ones to reduce manual and repetitive work and to increase investigative work. To improve engagement with the attacker's intent, the firm integrated the attack lifecycle (the kill-chain) into its playbooks. Information and cognitive overload are addressed at multiple levels starting from correlation and aggregation using the firm's enterprise data service and SIEM to the SOC's large contingent of level 1 analysts backed up by advanced skills and experience at levels 2 and 3.

6.0 Situation Awareness in Incident Response: A Process Model

We answer our research question by proposing a process model of Situation Awareness in Cybersecurity IR or SA-CIR (figure 4). To construct the model, we determined how *FinanceCentral*'s Situation Awareness is implemented through processes that vertically and horizontally integrate stakeholders within IT and also across the broader enterprise. From the interviewees' description of the processes we identified the key ingredients required for a process model: (1) the stakeholders integral to the response process, (2) process inputs (mental models, playbooks, threat intelligence, strategic, business and IT context), and (3) process outputs (perception, comprehension, projection). We subsequently cycled recursively

among the exemplar Situation Awareness practices of *FinanceCentral* and Situation Awareness theory using the logic of Eisenhardt and Graebner (2007).

The process model is modelled as a two-dimensional artifact. Cybersecurity stakeholders (green boxes) are modelled across the horizontal dimension. The vertical dimension models Situation Awareness as the three states of knowledge defined in Endlsey's theory (perception, comprehension, and projection). The process model features two kinds of dynamic behavior. The first is information processing behavior (data-driven vs goal-driven) and the second is task behavior (escalation vs investigation).

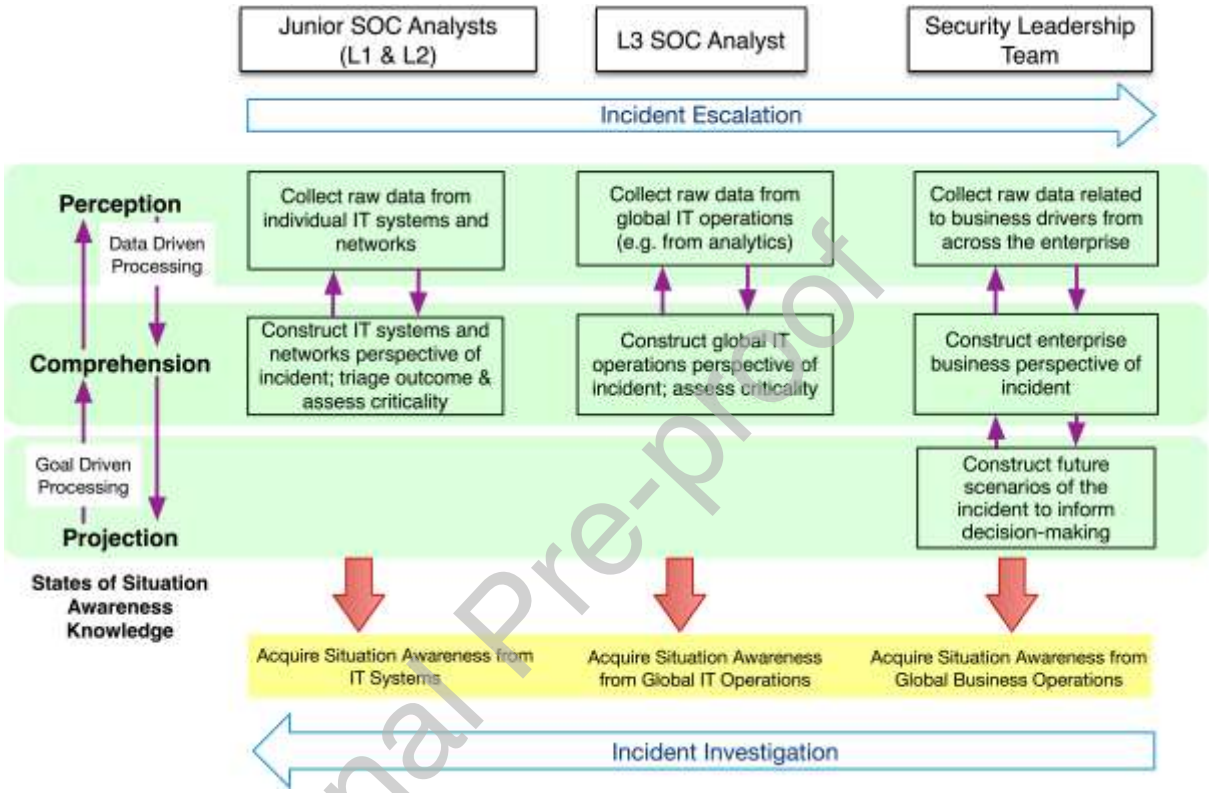

Figure 4: Situation-Awareness in Cybersecurity Incident Response

Information processing behavior is modelled using the purple arrows in figure 4 that allow progression through the 3 states of Situation Awareness knowledge. The downward pointing purple arrows reflect that organizations can acquire increasingly higher levels of Situation Awareness from data-driven processes (moving from perception to comprehension to projection). The upward pointing purple arrows between the states reflect that goal-driven processing such as attention-focusing using existing mental models can improve lower levels of Situation Awareness (moving from projection to comprehension to perception).

Task behavior is modelled using the blue outline arrows. The arrow pointing to the right represents situations where priority incidents are escalated from junior analysts to senior analysts and ultimately to the security leadership team. The precise types of cyber events that might result in escalation are confidential. However, an example cited by *Lead_CyberOperations* is loss of control over significant parts of the firm's IT infrastructure from the rapid spread of malware. The arrow pointing to the left represents situations where a senior analyst or the security leadership team require internal incident context to be developed by junior analysts having been alerted to a potential incident by IT & Business Management and/or the C-suite Executive.

The contributions of each category of stakeholder to situation awareness are defined in terms of their frame of reference (yellow bar). Junior SOC analysts have a narrow frame of reference compared to senior SOC analysts. Their activities focus on individual IT systems and networks across the organization. L3 SOC analysts have a broader frame of reference which encompasses the firm's global IT operations. The broadest frame of reference sits with the Security Leadership Team which encompasses the whole enterprise. An important further point of distinction is that the Security Leadership Team's perspective is business-centered rather than technology-centered.

In general, to acquire Situation Awareness organizations must (1) 'collect the dots', i.e. collect alerts and raw details of the incident-related environment (perception), (2) 'connect the dots', i.e. synthesize elements of the incident with existing knowledge, and assess criticality and overall significance of the incident in the context of cybersecurity objectives (comprehension), and (3) 'project from the dots', i.e. construct possible incident scenarios in the immediate future to inform appropriate response (projection). The processes of Situation Awareness run continuously, in parallel, and can be data-driven and goal-driven at the same time. In the following sections we describe the activities of all stakeholders or sources of information that contribute to the firm's Situation Awareness. These are summarized in Table 2. The unshaded stakeholders in Table 2 (that also appear in Figure 3) execute the response process, whereas the shaded stakeholders / information sources inform the response process.

Table 2. All Stakeholder Activity in Situation Awareness

Stakeholder	**Perception**	**Comprehension**	**Projection**
Sensor Data	Generate security alerts from aggregated and correlated security log entries and other sources for *L1 SOC Analysts*	None	None
Threat Intelligence	Collect, analyze, and disseminate raw intelligence data and alerts for *SOC Analysts* and *Security Leadership*	Provide advice (including hypotheses) for *SOC Analysts* and *Security Leadership*	Provide advice (including hypotheses) for *Security Leadership*
Junior SOC Analysts (L1 and L2)	Apply playbooks, mental models, and operational threat intelligence to collect alerts and raw data using a case management system for later analysis	Apply playbooks, mental models, tacit knowledge about the organization and incident, and operational threat advice to synthesize incident-related elements with existing knowledge for triage and criticality assessment	None
L3 SOC Analysts	Draw on analytics-driven reporting from Global IT Operations to collect alerts and raw data using a case management system for later analysis	Apply mental models, tacit knowledge about the organization and incident, and threat advice to synthesize incident-related elements with existing knowledge for understanding and criticality assessment	None, however, some *L3 SOC Analysts* will be part of *Security Leadership*
Security Leadership	Collect alerts and raw data from *C-suite Executive* and *IT & Business Management;* document in case management system; Direct alerts to junior analysts for investigation	Apply mental models, tacit knowledge, and input about strategic business context to synthesize incident-related elements with existing knowledge for the purposes of understanding	Apply mental models, strategic threat advice, to generate future scenarios of the incident
IT & Business Management	Provide alerts and raw data related to incident elements to *L3 SOC Analysts* and *Security Leadership Team*	Provide business and IT context related to incident elements to *L3 SOC Analysts* and *Security Leadership Team*	None

Table 2. All Stakeholder Activity in Situation Awareness			
Stakeholder	**Perception**	**Comprehension**	**Projection**
C-suite Executive	Provide alerts and raw data related to incident elements to *Security Leadership*	Provide context related to incident elements to *Security Leadership*	None

6.1 Perception

Perception requires organizations to collect the alerts and raw details that will be later used to construct the incident-related operational picture. Figure 4 shows alerts and raw data collected using three different frames of reference. Junior SOC analysts focus their collection on individual IT devices, L3 receive analytical information that summarizes trends across the IT domain which they draw upon for raw data collection. Security Leadership Team's collection comes from direct human contact from *IT and Business Management* as well as from the *C-suite Executive* (rather than IT tools).

Sensor data is a critical source of alerts and raw data about incident-related elements in the organizational environment. This data may include real-time data generated from SIEM platforms that aggregate and correlate security logs but may also include behavioral analytics, internally generated alerts about email, SMS and phone phishing, and data generated by third party threat intelligence tools. Sensor data informs the perception of L1 analysts.

Threat intelligence is a second key source of alerts and raw data. The threat intelligence team collects and disseminates operational-level alerts and raw data to junior SOC analysts, tactical-level alerts to L3 SOC analysts, and strategic-level alerts to the SecurityLT

Incident alerts and raw data may come from outside the IT operations unit. There are two key sources in organizations, namely *IT and Business Management* and the *CISO and C-suite Executives*. As Figure 4 shows, the former comes from domain heads and are likely to be communicated to their equivalent peer in IT operations (i.e. L3 SOC analysts). Whereas in the case of the latter, such information is likely to be communicated to the Security Leadership Team directly.

6.2 Comprehension

Comprehension requires organizations to build the operational picture of the incident and understand its significance in the context of cybersecurity objectives. The key stakeholders in the response process are SOC analysts and the SecurityLT. They integrate the raw details of the incident with: (1) their existing mental models, (2) their tacit knowledge of the organization, (3) their knowledge of the incident, and (4) advice from threat intelligence.

Threat intelligence play a key role in collecting, analyzing, and disseminating advice on the intent of threat-actors and the implications for organizations. For example, they can provide hypotheses about threat activity (including advice on threat-actor objectives and patterns of attack) to SOC analysts. Specifically, then can provide operational threat intelligence to L1 SOC analysts (e.g. blocking internet addresses, directing analysts on where to find evidence and context that helps to piece together operational-level fragments), tactical threat intelligence to L3 SOC analysts (e.g. explaining patterns of attack across IT operations) and strategic threat intelligence to the SecurityLT (i.e. identifying threat-actors and their intentions).

Junior SOC analysts are directed by playbooks to synthesize elements of the raw data to construct and triage the operational picture of the unfolding incident. If the incident criticality is low, then they may manage the full response themselves. However, if the incident is

deemed to be critical, they will escalate the incident to an L3 SOC analyst or directly to the Security Leadership Team. L3 SOC analysts will engage in the same comprehension activity within their frame of reference which is Global IT Operations. In making sense of the operational picture, *SOC analysts* will assess how far the attack has progressed in the kill-chain, the scope of the threat-actor's activities inside the firm, the extent to which the threat-actor has acquired authority and resources to carry out their mission objectives and the risk exposure to the organization's operations and sensitive information assets. A key consideration is the timing and nature of interventions in an unfolding attack scenario. There is a clear trade-off between cutting off a threat-actor to contain the impact of an attack and allowing the attack to continue to scope the attacker's activities and ascertain intent.

The Security Leadership will apply its shared mental models of the enterprises' cybersecurity risk environment, strategic threat intelligence, and its knowledge of the firm's cybersecurity mission and objectives, to the operational picture constructed by *SOC analysts* to make sense of the unfolding incident. Most such teams will engage in sensemaking, if necessary using a 'war room' where members can debate the facts of the case and use interactive learning technologies like whiteboards to develop a shared mental model specific to the incident within the model of the attack lifecycle. Engaging the operational units of the organization is critical for communication, consultation, and swift response. Through prefabricated and formal mechanisms such as an operational bridge, personnel from the *IT and Business Management* domains and *C-suite Executive* can be brought in as needed to provide additional context that assists with sensemaking but also for delegation of tasks (blue arrows).

6.3 Projection

Projection requires organizations to continuously extrapolate from the operational picture to generate alternative future scenarios of the incident-related organizational environment. Projection is the sole responsibility of the *Security Leadership*. The generation of plausible and likely scenarios requires several critical inputs. These are the mental models of the enterprises' cybersecurity risk environment and strategic-level threat intelligence about threat-actors, their objectives and anticipated behavior. Projection feeds into decision-making for the purpose of incident response. Major incident response is likely to be executed by a cross-functional team made up from members from across Business and IT Operations.

6.4 Limitations and Research Directions

Our case study of FinanceCentral is not without limitations. First, we were not able to interview more personnel - junior SOC analysts, threat intelligence personnel and helpdesk support staff - as the firm was experiencing a high number of low-criticality incidents at the time. Second, given more time we would have broadened the scope of enquiry to include non-IT personnel in order to develop a more holistic understanding of Situation Awareness of FinanceCentral and study the interplay between cybersecurity and non-cybersecurity personnel at both strategic and operational levels of the firm during incident response. In particular we would have liked to study the potential disconnect between IT and non-IT personnel to confirm or disconfirm Peppard's observations regarding the Business-IT disconnect (Peppard 2018). Third, although our study was grounded in theory (i.e. interview questions were developed from the constructs of Endsley's theory of Situation Awareness), there are other theories of Situation Awareness that could have been consulted in order to enhance the quality of the theoretical contribution.

Single in-depth case studies impose their own limitations (Yin 2018). Notwithstanding the challenges of building sufficient trust to enable deep access to multiple organizations, and the tremendous cost incurred in time and resources, a multiple-case study would have allowed:

(1) literal and theoretical replication logic when analysing results of the study, (2) better generalizability of our process model, (3) stronger theory building due to greater reliablility of evidence, (4) comparison and contrast of the SA processes of the firms in terms of their organizational structure, coordination among teams, team dynamics, routine behaviors, skillbase of personnel, technologies used and their integration, reporting structure and communication protocols.

Our reason for adopting a case study approach to developing and refining the process model is that the method allows us to investigate incident response in its real-life context and compile comprehensive systematic and in-depth information about the incident response capability of an organization. Focus groups with experienced industry practitioners in incident response can also help to further refine and validate the process model as they: (1) provide an open format to discuss a wide range of opinions, (2) allow contrasts and similarities of opinions to be highlighted, (3) allow industry experts to directly interact with the researchers to clarify issues, and (4) allow industry experts to build on each other's expertise (Tremblay et al. 2010). These will add depth to the research by providing rich insights on factors that enable or hinder the development of Situation Awareness in IR, the skills and knowledge required by cybersecurity IR teams to build Situation Awareness capabilities, and conditions which affect the utility of Situation Awareness in IR.

7.0 Conclusion

The cybersecurity threat landscape has shifted due to the rise of organized, well-resourced, and persistent threat-actors that target individual organizations for financial and/or political benefit. To respond to the threat, organizations must develop situation awareness in their incident response practices. Our study provides several contributions to both theory and practice.

First, we contribute to the literature on cybersecurity incident response by developing a process model that explains the role of management practice in developing situation awareness of cybersecurity incidents. Past research on situation awareness has focused on the technology and cognitive perspective, whereas management practice has received comparatively less attention. Adopting a case study approach enabled us to explain how situation awareness is developed through a three-step process – perception, comprehension, and projection in terms of management practice. The model can be used to develop and/or evaluate the response function of response teams in large and well-resourced organizations that perceive a high risk of cyber-attack from sophisticated threat-actors.

Second, through the identification of sources of information and knowledge and the construction of communication pathways and relationships between stakeholders (individuals and teams), we have developed an information processing network and explained how organizations can control information flow to develop situation awareness. We hope to attract experts in information processing theory to further develop our information processing perspective towards improved situation awareness.

The *FinanceCentral* case explains how Situation Awareness can be acquired in large organizations using the combination of a SOC and a flexible command and control leadership team. We believe organizations looking to develop their incident response practice to address organized and sophisticated cyber threat agents will find the process model and the case study useful. Our discussion of the practices of each stakeholder in the response process provides a basis for developing selection and training requirements for incident response personnel. This is particularly the case for level 1 SOC analysts as they need to be trained in investigative approaches to incident handling. Our case study confirms the critical relationship between

organizational structure and incident response outcomes and shows how structural limitations can be overcome in mature and sophisticated response capabilities.

8.0 Acknowledgements

This work is supported by the Australian Research Council through the Discovery Projects scheme (DP160102277) “Enhancing Information Security Management through Organisational Learning”.

9.0 References

Agyepong, E., Cherdantseva, Y., Reinecke, P., and Burnap, P. 2019. "Challenges and Performance Metrics for Security Operations Center Analysts: A Systematic Review," *Journal of Cyber Security Technology*), pp. 1-28.

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., and Baskerville, R. L. 2020. "How Integration of Cyber Security Management and Incident Response Enables Organizational Learning," *Journal of the Association for Information Science and Technology* (71:8), pp. 939-953.

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

Ahmad, A., Maynard, S. B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," *International Journal of Information Management* (35:6), pp. 717-723.

Ahmad, A., Webb, J., Desouza, K. C., and Boorman, J. 2019. "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security* (86), pp. 402-418.

Alshaikh, M., Ahmad, A., Maynard, S. B., and Chang, S. 2014. "Towards a Taxonomy of Information Security Management Practices in Organisations," *25th Australasian Conference on Information Systems*, Auckland, New Zealand, p. 10.

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 & 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 & Management* (51:1), pp. 138-151.

Boudreau, M.-C., and Robey, D. 2005. "Enacting Integrated Information Technology: A Human Agency Perspective," *Organization science* (16:1), pp. 3-18.

Catota, F. E., Morgan, M. G., and Sicker, D. C. 2018. "Cybersecurity Incident Response Capabilities in the Ecuadorian Financial Sector," *Journal of Cybersecurity* (4:1), p. tyy002.

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

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. "Nist Special Publication 800-61, Revision 2: Computer Security Incident Handling Guide," NIST, US Department of Commerce.

Cooke, N. J., Champion, M., Rajivan, P., and Jariwala, S. 2013. "Cyber Situation Awareness and Teamwork," *EAI Endorsed Transactions on Security and Safety* (1:2).

Dhillon, G. 2018. "Principles of Information Systems Security," B.L. Golub (ed.). Burlington, Vermont: Prospect Press, pp. 1-559.

Eisenhardt, K. M. 1989. "Building Theories from Case Study Research," *Academy of management review* (14:4), pp. 532-550.

Eisenhardt, K. M., and Graebner, M. E. 2007. "Theory Building from Cases: Opportunities and Challenges," *Academy of management journal* (50:1), pp. 25-32.

Endsley, M. R. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems," *Human factors* (37:1), pp. 32-64.

Franke, U., and Brynielsson, J. 2014. "Cyber Situational Awareness–a Systematic Review of the Literature," *Computers & Security* (46), pp. 18-31.

Gartner. 2020. "Gartner Forecasts Worldwide Security and Risk Management Spending Growth to Slow but Remain Positive in 2020." from https://www.gartner.com/en/newsroom/press-releases/2020-06-17-gartner-forecasts-worldwide-security-and-risk-managem

Hove, C., Tarnes, M., Line, M. B., and Bernsmed, K. 2014. "Information Security Incident Management: Identified Practice in Large Organizations," *IT Security Incident Management & IT Forensics (IMF), 2014 Eighth International Conference on*, pp. 27-46.

Hutchins, E. M., Cloppert, M. J., and Amin, R. M. 2011. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Leading Issues in Information Warfare & Security Research* (1:1), p. 80.

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* (2:1-2), pp. 26-37.

Jirsík, T. 2018. "Cyber Situation Awareness Via Ip Flow Monitoring." Faculty of Informatics: Masaryk University, p. 193.

Klein, H. K., and Myers, M. D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Fields Studies in Information Systems.," *MIS Quarterly* (23:7), pp. 67-94.

Komárková, J., Husák, M., Laštovička, M., and Tovarňák, D. 2018. "Crusoe: Data Model for Cyber Situational Awareness," *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-10.

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

Lemay, A., Calvet, J., Menet, F., and Fernandez, J. M. 2018. "Survey of Publicly Available Reports on Advanced Persistent Threat Actors," *Computers & Security* (72), pp. 26-59.

Line, M. B. 2013. "A Case Study: Preparing for the Smart Grids - Identifying Current Practice for Information Security Incident Management in the Power Industry," *IT Security Incident Management and IT Forensics (IMF), 2013 Seventh International Conference on*, pp. 26-32.

Line, M. B., and Albrechtsen, E. 2016. "Examining the Suitability of Industrial Safety Management Approaches for Information Security Incident Management," *Information & Computer Security* (24:1), p. 20.

Line, M. B., Zand, A., Stringhini, G., and Kemmerer, R. 2014. "Targeted Attacks against Industrial Control Systems: Is the Power Industry Prepared?," *Proceedings of the 2nd Workshop on Smart Energy Grid Security*, pp. 13-22.

Macabante, C., Wei, S., and Schuster, D. 2019. "Elements of Cyber-Cognitive Situation Awareness in Organizations," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*: SAGE Publications Sage CA: Los Angeles, CA, pp. 1624-1628.

Neuman, W. L. 2014. *Social Research Methods: Qualitative and Quantitative Approaches*, (Seventh ed.). London: Pearson Education Ltd.

Neville, T. J., and Salmon, P. M. 2016. "Never Blame the Umpire–a Review of Situation Awareness Models and Methods for Examining the Performance of Officials in Sport," *Ergonomics* (59:7), pp. 962-975.

Nyre-Yu, M., Gutzwiller, R. S., and Caldwell, B. S. 2019. "Observing Cyber Security Incident Response: Qualitative Themes from Field Research," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*: SAGE Publications Sage CA: Los Angeles, CA, pp. 437-441.

Paul, C. L., and Whitley, K. 2013. "A Taxonomy of Cyber Awareness Questions for the User-Centered Design of Cyber Situation Awareness," *International Conference on Human Aspects of Information Security, Privacy, and Trust*: Springer, pp. 145-154.

Peppard, J. 2018. "Rethinking the Concept of the Is Organization," *Information Systems Journal* (28:1), pp. 76-103.

Rajivan, P., and Cooke, N. 2017. "Impact of Team Collaboration on Cybersecurity Situational Awareness," in *Theory and Models for Cyber Situation Awareness*. Springer, pp. 203-226.

Schinagl, S., Schoon, K., and Paans, R. 2015. "A Framework for Designing a Security Operations Centre (Soc)," *2015 48th Hawaii International Conference on System Sciences*: IEEE, pp. 2253-2262.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., Zaccaro, S. J., Dalal, R. S., and Tetrick, L. E. 2015. "Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research," *IEEE Security & Privacy* (13:4), pp. 20-29.

Sveen, F. O., Torres, J. M., and Sarriegi, J. M. 2009. "Blind Information Security Strategy," *International journal of critical infrastructure protection* (2:3), pp. 95-109.

The Mitre Corporation. 2017. "Threat-Based Defense - Understanding an Attacker's Tactics and Techniques Is Key to Successful Cyber Defense." Retrieved 18th Sept 2020, from https://www.mitre.org/capabilities/cybersecurity/threat-based-defense

Tremblay, M. C., Hevner, A. R., and Berndt, D. J. 2010. "Focus Groups for Artifact Refinement and Evaluation in Design Research," *Communications of the association for information systems* (26:1), p. 27.

Verizon. 2020. "2020 Data Breach Investigations Report." Retrieved 26/8/2020, from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44), pp. 391-404.

Weishäupl, E., Yasasin, E., and Schryen, G. 2018. "Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning," *Computers & Security* (77), pp. 807-823.

Werlinger, R., Muldner, K., Hawkey, K., and Beznosov, K. 2010. "Preparation, Detection, and Analysis: The Diagnostic Work of It Security Incident Response," *Information Management & Computer Security* (18:1), pp. 26-42.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., and Ruefle, R. 2003. "Handbook for Computer Security Incident Response Teams (Csirts)," Carnegie Mellon University.

Yin, R. K. 2018. *Case Study Research and Applications: Design and Methods*. Sage publications.

CReDiT Author Statement

Atif Ahmad - Funding Acquisition, Conceptualization, Methodology, Investigation, Writing - Original Draft. **Sean B. Maynard -** Project Administration, Methodology, Writing - Review & Editing, Validation. **Kevin C. Desouza -** Writing - Review & Editing. **James Kotsias –** Investigation, Data Analysis, Resources (access to organization, interview management). **Monica T. Whitty -** Writing - Review & Editing. **Richard L. Baskerville - Writing - Review & Editing**

Declaration of interests

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

Atif Ahmad is an Associate Professor at the University of Melbourne's School of Computing & Information Systems. Atif leads Cybersecurity Management research and currently serves as the Deputy Director for the Academic Centre of Cyber Security Excellence. His main areas of expertise are in security strategy, risk management, incident response and intellectual property protection. Atif has authored over eighty scholarly articles in cybersecurity and received over $3M in grant funding. He is a member of the editorial board for the journal Computers & Security. His research has been published in high-impact journals such as the Journal of the Association for Information Science and Technology, Computers & Security and the International Journal of Information Management as well as leading conferences such as

the International Conference on Information Systems. Atif has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. He is a Certified Protection Professional with the American Society for Industrial Security. For more information, see https://www.atifahmad.me/

Sean B. Maynard is an academic based at the School of Computing and Information Systems, University of Melbourne, Australia. Sean has over 25 years of teaching experience at the undergraduate, postgraduate and executive training levels. His teaching specialities include: Information Systems, Information Systems strategy and governance, database, and data warehousing. He received his Ph.D. in Information Security from the University of Melbourne in 2010. His research interests are in the management of information security specifically relating to security policy, security culture, security governance, security strategy, security analytics, and incident response. He has also published in the area of decision support systems, and business analytics, particularly in capability maturity. He has over sixty publications. His research has been published in high-impact journals such as Computers & Security, the Journal of the Association for Information Science and Technology and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems. For more information, please visit https://www.seanmaynard.me/

Kevin C. Desouza is a Professor of Business, Technology and Strategy in the School of Management at the QUT Business School and in the Centre for Future Enterprise, Queensland University of Technology. He is a Nonresident Senior Fellow in the Governance Studies Program at the Brookings Institution and is a Distinguished Research Fellow at the China Institute for Urban Governance at Shanghai Jiao Tong University. He has held tenured faculty appointments at the University of Washington, Virginia Tech, and Arizona State University. He has published more than 130 articles in journals across a range of disciplines including information systems, information science, public administration, and political science. For more information, see http://www.kevindesouza.net

James Kotsias is a Cyber Security Leader and Research Advisor. He holds a Master's Degree in Information Systems from The University of Melbourne. He leads an offensive security and operations function, and advises long-term cyber security and threat strategy for a number of organisations. James also sits on the Cyber Executive Advisory Board at Deakin University; providing input to the Cyber Security Research and Innovation Centre (CSRI) and its extended intelligent systems research. His current research interests are the expanding theatre of cyber warfare, the evolution of corporate espionage, the weaponisation of defensive systems, and kinetic incident response structures. James bluescreened his first PC at the age of 7.

Professor Monica Whitty is the Director of Research (Cyber) at the UNSW (Canberra), where she also holds a Chair in Human Factors in Cyber Security. She is a member of the World Economic Forum Cyber Security Centre. She is also a visiting Professor in Cyber Security at Royal Holloway, University of London. Her work, in particular, examines identities created in cyberspace, online security risks, behaviour in cyberspace, insider threat, as well as detecting and preventing deception, such as cyberscams and mis/disinformation (drawing from psychological and linguistic tools). Monica is the author of over 100 articles and 5 books, the latest being: 'Cyberpsychology: The study of individuals, society and digital technologies' (Wiley, 2017, with Garry Young).

Richard Baskerville is Regents' Professor and Board of Advisors Professor in the Department of Computer Information Systems, J. Mack Robinson College of Business at Georgia State University. His research specializes in security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. Baskerville is the author of more than 300 articles in scholarly journals, professional magazines, and edited books. He is Editor Emeritus and past Editor-in-Chief for The European Journal of Information Systems and serves on the editorial boards of the Information Systems Journal and the Journal of Information Systems Security.
Baskerville's practical and consulting experience includes advanced information system designs for the U.S. Defense and Energy Departments. He is past president of the Information Systems Academic Heads International, past chairman of the Information Systems Department at Georgia State, past chair of the IFIP Working Groups 8.2 (Information Systems and Organizations) and 8.11/11.13 (Information Systems Security

Research). Baskerville was awarded The LEO Award for Lifetime Exceptional Achievement by the Association for Information Systems in 2016 and the Silver Core by the International Federation for Information Processing in 1998.