A FRAMEWORK OF DYNAMIC CYBERSECURITY INCIDENT RESPONSE TO IMPROVE INCIDENT RESPONSE AGILITY

Humza Naseer

Submitted in fulfilment of the requirements of the degree of

Doctor of Philosophy

October 2018

School of Computing and Information System

The University of Melbourne

ABSTRACT

The modern enterprise uses risk-driven and control-centered security management systems to protect information resources and sustain competitive advantage. Such systems have proven to be quite effective in the *prevention* of threats such as those exploiting common vulnerabilities. However, they are not very well suited to *response* against threats that are unpredictable, complex and evolving such as Advanced Persistent Threats. The complex and dynamic nature of these threats demands a sophisticated, timely and agile response capability to collect, integrate and analyse information to direct strategic and operational security measures. Real-time analytics is a specialized business analytics capability that helps organizations to collect, integrate, and analyse business events as they occur. While the ability of real-time analytics to deliver instant business insights has gained much attention in the literature, there has been limited research on how it can help enterprises improve agility in their cybersecurity incident response.

This study addresses the aforementioned research gap through investigating the research question: *How can organizations improve agility in their cybersecurity incident response process using real-time analytics?* Drawing from dynamic capabilities theory, the study collected qualitative data from three large financial organizations and used a process of data comparison that engages in simultaneous analysis and exploration. The results informed a framework of *dynamic cybersecurity incident response* that explains how organizations using real-time analytics are able to develop higher order *real-time analytics-enabled dynamic capabilities* in incident response such as *real-time situation awareness*, *dynamic risk assessment*, and *cyber threat intelligence generation*. These dynamic capabilities help organizations to execute dynamic incident response strategies including *active defence*, *continuous monitoring*, and *active reconnaissance*. The *real-time analytics enabled dynamic capabilities* together with *dynamic incident response strategies* infuse agile characteristics such as *swiftness*, *flexibility* and *innovation* in the cybersecurity incident response process, which in turn, lead to positive outcomes in enterprise security performance and delivers both strategic and economic benefits. The framework also provides a comprehensive view of the factors that support and hinder the development of dynamic capabilities in the *cybersecurity incident response process* and execution of *dynamic incident response strategies*. The details of the framework contribute to the literature on business analytics capabilities, dynamic capabilities, cybersecurity incident response strategies, and business process agility. The findings of the study provide a useful stepping stone for future studies on how to improve agility in cybersecurity incident response process.

DECLARATION

This is to certify that:

i. the thesis comprises only my original work towards the PhD,

ii. due acknowledgement has been made in the text to all other material used,

iii. the thesis is less than 100,000 words in length, exclusive of tables, maps, bibliographies, and appendices.

Humza Naseer

15 October 2018

Publications and Awards

This section includes the list of peer-reviewed academic articles that I have published and the awards that I have received during my PhD research. Elements of these articles are included in this thesis particularly in Chapter 2. The inclusion of the papers is highlighted in the relevant section within the thesis.

Publications from the PhD Research

Naseer, H., Ahmad, A., Maynard, S., Desouza, K.C., and Shanks, G., 2018, "**A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility Using Real-time Analytics: An Empirical Investigation**" Under review in *The Journal of Strategic Information Systems*.

Naseer, H., Ahmad, A., Maynard, S., and Shanks, G., 2018, "**Cybersecurity Risk Management Using Analytics: A Dynamic Capabilities Approach**" in *Thirty Ninth International Conference on Information Systems (ICIS)*, San Francisco, USA.

Naseer, H., Shanks, G., Ahmad, A., and Maynard, S., 2017, "**Towards an Analytics-Driven Information Security Risk Management: A Contingent Resource Based Perspective**" in *Twenty-fifth European Conference on Information Systems (ECIS)*, Guimarães, Portugal.

Naseer, H., Shanks, G., Ahmad, A., and Maynard, S., 2016, "**Enhancing Information Security Risk Management with Security Analytics: A Dynamic Capabilities Perspective**" in *Australasian Conference on Information Systems (ACIS)*, Wollongong, Australia.

Naseer, H., Maynard, S., and Ahmad, A., 2016, "**Business Analytics in Information Security Risk Management: The Contingent Effect on Security Performance**" in *Twenty-fourth European Conference on Information Systems (ECIS)*, İstanbul, Turkey.

Awards

Google Australia Best Paper Award at 4th School of Computing and Information Systems Doctoral Colloquium, 2016, The University of Melbourne, to paper entitled "**Business Analytics in Information Security Risk Management: The Contingent Effect on Security Performance**".

ACKNOWLEDGEMENTS

I would like to thank:

the participants of the study for their invaluable insights, making this research possible,

my supervisors, Dr. Sean Maynard, Dr. Atif Ahmad and Prof. Graeme Shanks, for their unwavering support, guidance, and encouragement throughout the project,

other members of the professional community who have been most kind to offer their thoughts and advice, in particular Dr. Rod Dilnutt for the many enjoyable and insightful discussions in the course of this study,

and my family and friends for their warm support throughout this process, in particular my father, Naseer Ahmed, and mother, Ishrat Ara for encouraging me to study at an outstanding university and for making it possible, and my wife, Samarah Shahid, for regularly distracting me from work in my own best interest!

DEDICATION

To my wife, and my wonderful daughter - Zunnoraen

To those who raised me personally (my parents), professionally (my supervisors), and patiently (my wonderful wife) - Samarah

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1

“We have to keep on remembering that the attacks are going to come. The attackers are continuously innovating. We have to be agile in our response, and that requires sharing the right information with the right people at the right time to be able to respond in the right manner.

(General manager of cybersecurity risk management, FinBank)

CHAPTER 1. INTRODUCTION

Cybersecurity incident response is a continuous process in which designated teams identify, investigate, respond and learn from potential cybersecurity incidents in a timely and cost-effective manner. This process is crucial for enterprises because they cannot always prevent a breach and therefore a swift incident response to a cybersecurity attack can help them to avoid any financial damage and most importantly, protect their business, reputation and competitive advantage. In an effort to deal with cybersecurity attacks and data breaches, organisations engage their cybersecurity incident response teams (ad-hoc or dedicated) to detect, examine and respond to cybersecurity incidents efficiently and effectively (Grispos et al. 2014; Ruefle et al. 2014). However, in order to effectively detect and respond to cybersecurity incidents, incident response teams need to quickly collect, integrate and analyse all data related to a cybersecurity incident that has happened or is happening in their organizations (von Solms and van Niekerk 2013; Tøndel et al. 2014).

Business analytics (BA) is an organizational capability to collect, store and analyse business data to generate insights that helps business executives in making informed decisions (Chen et al. 2012; Sharma et al. 2014; Wixom et al. 2013). Building on BA capability, BA scholars have proposed *real-time analytics capability* - a specialized BA capability that helps organizations to carry out BA in real-time and proactively make informed decisions (Dobrev and Hart 2015; Phillips-Wren et al. 2015; Watson et al. 2006).

This study is about improving agility in cybersecurity incident response process by employing real-time analytics. Agility in cybersecurity incident response process refers to how swiftly and efficiently organizations can alter their incident response process to detect and respond to creative and unpredictable cybersecurity threats. Agility is critical to the success of cybersecurity incident response process, since an organization's capability to achieve superior security performance depends on its response to cybersecurity incidents within an unpredictable threat environment (Baskerville et al. 2014; Grispos et al. 2014; Jalali et al. 2018). The following sections explain the importance of this research topic, the focus of the study, provide an overview of the research design, present a summary of the contributions of the study and discuss the organisation of the thesis.

1.1 Motivation for the Study

Today's highly dynamic and fast-paced business environment shapes the way in which enterprises use their assets such as digital processes, data, and systems in gaining a competitive advantage. While modern enterprises perform their daily business operations, these assets are increasingly exposed to complex and evolving security threats, both external and internal, such as theft, fraud, sabotage, embezzlement, and industrial espionage. It is therefore critical for organizations to protect these assets in order to sustain their competitive advantage and successfully operate in today's dynamic cyber threat environment (Weishäupl et al. 2015a). To do so, organizations employ the process of cybersecurity incident response that helps them to identify, investigate and respond to potential cybersecurity incidents in a manner that minimizes impact and supports rapid recovery.

Strategically, enterprise cybersecurity in organizations has long been centered on addressing threats with a comprehensive regime of controls (Ahmad, Maynard, et al. 2014; Baskerville et al. 2014; Maynard et al. 2018; Onibere et al. 2017; Park et al. 2012; Tan et al. 2010, 2017). The method of selection of controls has evolved from industry-endorsed checklists to a more sophisticated risk management process that requires the enterprise to: (1) identify sensitive assets, (2) prioritize risk scenarios according to severity, and (3) determine the most cost-effective means of controlling exposure (Shedden, Ruighaver, et al. 2010; Shedden et al. 2016; Webb et al. 2014).

According to a seminal paper by Baskerville et al. (2014), risk-driven and control-centered security management systems have proven to be quite effective in the static prevention of predictable threats (exploits of common vulnerabilities, IT accidents, internal threats of theft, fraud, etc.) but not very well suited to dynamic response against unpredictable, evolving and complex threats such as Advanced Persistent Threats (APTs). Perpetrators of APTs are knowledgeable, well-trained, and organized attackers that use customized and innovative operational techniques to circumvent organizational security defences (Chen et al. 2014; Friedberg et al. 2014). The frequency of this more sophisticated form of attack is expected to rise significantly in the coming years (Lemay et al. 2018). The complex and dynamic nature of such threats demands a high degree of situation-awareness to counter the evolving vectors in the attack. This requires organizations to develop a sophisticated capability to collect, integrate and analyse information to direct strategic and operational security measures to be taken in a timely manner.

Although most organizations retain cybersecurity incident response (IR) teams, their traditional role is largely operational and technology-centered, with the primary objective of facilitating organizational recovery to routine business operations. To combat APTs, as Baskerville et al. (2014) argue, a paradigm shift is required centered on a whole-of-organization response. In the 'response paradigm', IR becomes a more strategic-level function, engaging with the threat environment more directly by addressing the threat and consequences of attacks within the strategic business context (Baskerville et al. 2014; Pierazzi et al. 2016). Critical to the success of the more strategic-level IR function is the organization's ability to generate security insights or 'intelligence' about the threat and adapting the IR process to leverage said intelligence in a timely manner to defend against APTs. Consequently, this requires the IR function to have tools, processes and skills that enable enterprise wide collection, integration and analysis of all relevant data related to cybersecurity incidents especially data about the strategic business context.

Business analytics (BA) is an organizational capability integrating people, process, and technology to generate insights empowering business executives to make informed and timely decisions (Chen et al. 2012; Holsapple et al. 2014; Wixom et al. 2013). This capability is suited to the collection, integration and analysis of large sets of disparate organizational data. A specialized BA capability, "real-time analytics" focuses on streaming data thereby enabling organizations to carry out BA in real-time and proactively make informed decisions (Phillips-Wren et al. 2015; Watson et al. 2006). Therefore, real-time analytics provides organizations with a unique opportunity to achieve the aforementioned paradigm shift by developing a response function that collects, integrates and analyses both business and security data sets in real time to mitigate the risk of APT within the strategic business context.

The concept of real-time analytics exists in BA literature and BA practice for more than a decade, however the understanding of this concept is still limited (Dobrev and Hart 2015; Phillips-Wren et al. 2015). As real-time analytics is still an emerging phenomenon, most enterprises are using it to enhance their operational competencies. However, some enterprises have recognised that specialized BA capabilities such as real-time analytics enables a fundamental shift in the way IT capabilities are delivered and it can be used to improve business process agility by developing dynamic capabilities (Park et al. 2017). Dynamic capability is defined as 'the firm's ability to integrate, build, and reconfigure internal and external competences to address rapidly changing environments' (Teece et al. 1997, p. 516). Baskerville et al. (2014) have called for the development of dynamic capabilities in cybersecurity environments that face dynamic and sophisticated attacks. While the ability of real-time analytics to enhance operational competencies has gained much attention in the literature, research on how real-time analytics can improve business process agility through dynamic capabilities is limited. Furthermore, with real-time analytics gaining widespread attention as an evolving BA capability, the focus on using real-time analytics to improve incident response process agility has significant implications for overall enterprise security performance.

Agility in IR refers to *how swiftly and efficiently cybersecurity incident response teams can alter their IR process to detect and respond to unpredictable cybersecurity threats* (Tallon 2008). Agility is critical to the IR process, since an organization's capability to achieve superior enterprise security performance depends on its reaction to cybersecurity incidents that have happened or are happening in an unpredictable threat environment (Baskerville et al. 2014). Even though organizations are paying increasing attention in improving agility in their cybersecurity incident response, not enough is known about how agility can be improved in incident response process (Grispos et al. 2014). Thus, how organizations improve agility by developing dynamic capabilities in their incident response critically impacts an enterprise's cybersecurity success yet remains relatively unexamined.

1.2 Focus of the Study

In order to address the knowledge gap described above, the key research question that guides this study is:

How can organizations improve agility in their cybersecurity incident response process using real-time analytics?

There are several related issues that need to be considered in order to address this fundamental question. First, what are they key *features* of real-time analytics in cybersecurity incident response process? Second, what are the specific *dynamic capabilities* that are enabled by the use of real-time analytics in cybersecurity incident response process? Third, what are the underlying *mechanisms* through which real-time analytics improves agility in cybersecurity incident response? Fourth, what are the *factors* that facilitate or hinder the development of dynamic capabilities? And Fifth, how does the use of real-time analytics in cybersecurity incident response impact overall enterprise security performance? Therefore, five sub-themes need to be considered in relation to address the aforementioned research question:

1) **Key features of real-time analytics capability.** *What* are the key features of real-time analytics capability in the process of cybersecurity incident response?
2) **Real-time analytics enabled dynamic capabilities.** *What* are specific dynamic capabilities that real-time analytics enable in the process of cybersecurity incident response?
3) **Cybersecurity incident response agility.** *What* are the underlying mechanisms through which real-time analytics improves agility in cybersecurity incident response process? In other words, *how* and *why* does real-time analytics improve agility in cybersecurity incident response?
4) **Facilitating and challenging factors.** *What* are the factors related to cybersecurity incident response process and analytical capability that need to be most carefully monitored and managed in order to increase the likelihood of improving agility in incident response? *How* do these factors facilitate or hinder the development of dynamic capabilities? *Why* are these factors important?
5) **Enterprise security performance.** *How* does the use of real-time analytics in cybersecurity incident response impact overall enterprise security performance?

Although most of the five themes begin with the identification of the relevant concepts (the "what?"), the primary focus and weight of this study is on the underlying mechanisms, explanations, and the justification for the importance of each identified concept in relation to how cybersecurity incident response agility is improved using real-time analytics (i.e., the "how?" and "why?").

1.3 Overview of the Research Design

The first step towards a better understanding of the five themes listed in the previous section was a careful integration, synthesis and analysis of interdisciplinary IS literature on business analytics, dynamic capabilities, business process agility and cybersecurity incident response. Dynamic capabilities theory (Teece et al. 1997) was used to integrate and synthesize the literature conceptually.

Because of the heavy focus on the "how?" and "why?" questions in this study, a qualitative research approach was adopted. To answer the overarching research question of this study empirically, an exploratory field study was conducted using a multiple case study design. In-depth data from three large financial organizations was analysed to explore their use of real-time analytics in the process of cybersecurity incident response. Specifically, the selected organizations were facing dynamic environment in which the cyber threat landscape changes rapidly and had reportedly identified business intelligence and analytics as an important component of their cybersecurity incident response strategy. The unit of analysis for the case study was chosen to be 'cybersecurity incident response teams' as their primary responsibility is to identify, investigate, respond and learn from potential cybersecurity incidents in a timely and cost-effective manner. Integrating insights from these data with the existing literature informed a theoretical framework that depicts how organizations improve agility in their cybersecurity incident response by developing dynamic capabilities using real-time analytics. The overall research design is presented in Figure 1-1. For theory building, this study follows the steps that Gioia et al. (2013) outlines for building a theory which is grounded in the empirical data. Chapter 3 discusses the research design in more detail.

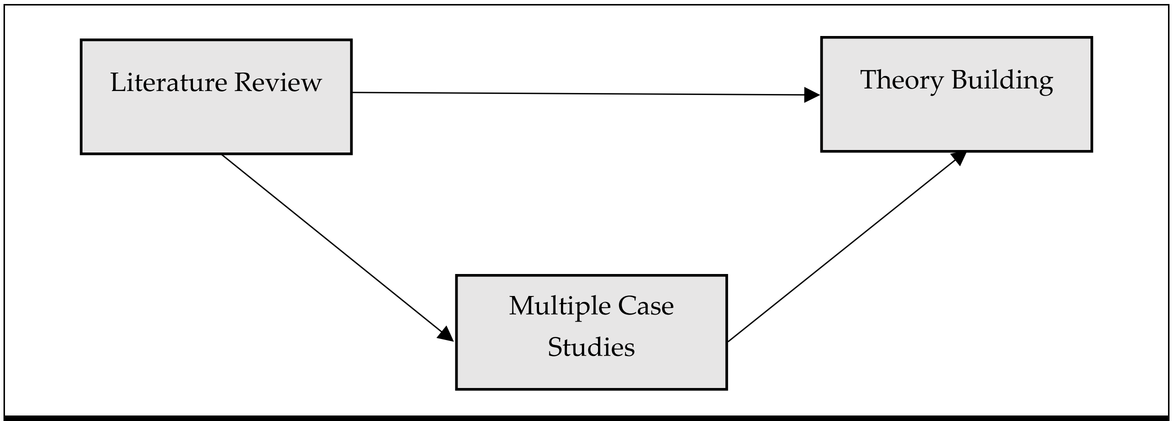


Figure 1-1. Research Design Overview

1.4 Key Findings

To answer the research question outlined in Section 1.2, this study proposes a framework of dynamic cybersecurity incident response to improve incident response agility shown in Figure 1-2. The insights captured by the framework are informed by the extant literature, grounded in dynamic capabilities theory, and have been built through analysis of a considerable body of empirical data. The details of the framework suggest the following regarding the five themes outlined in Section 1.2.

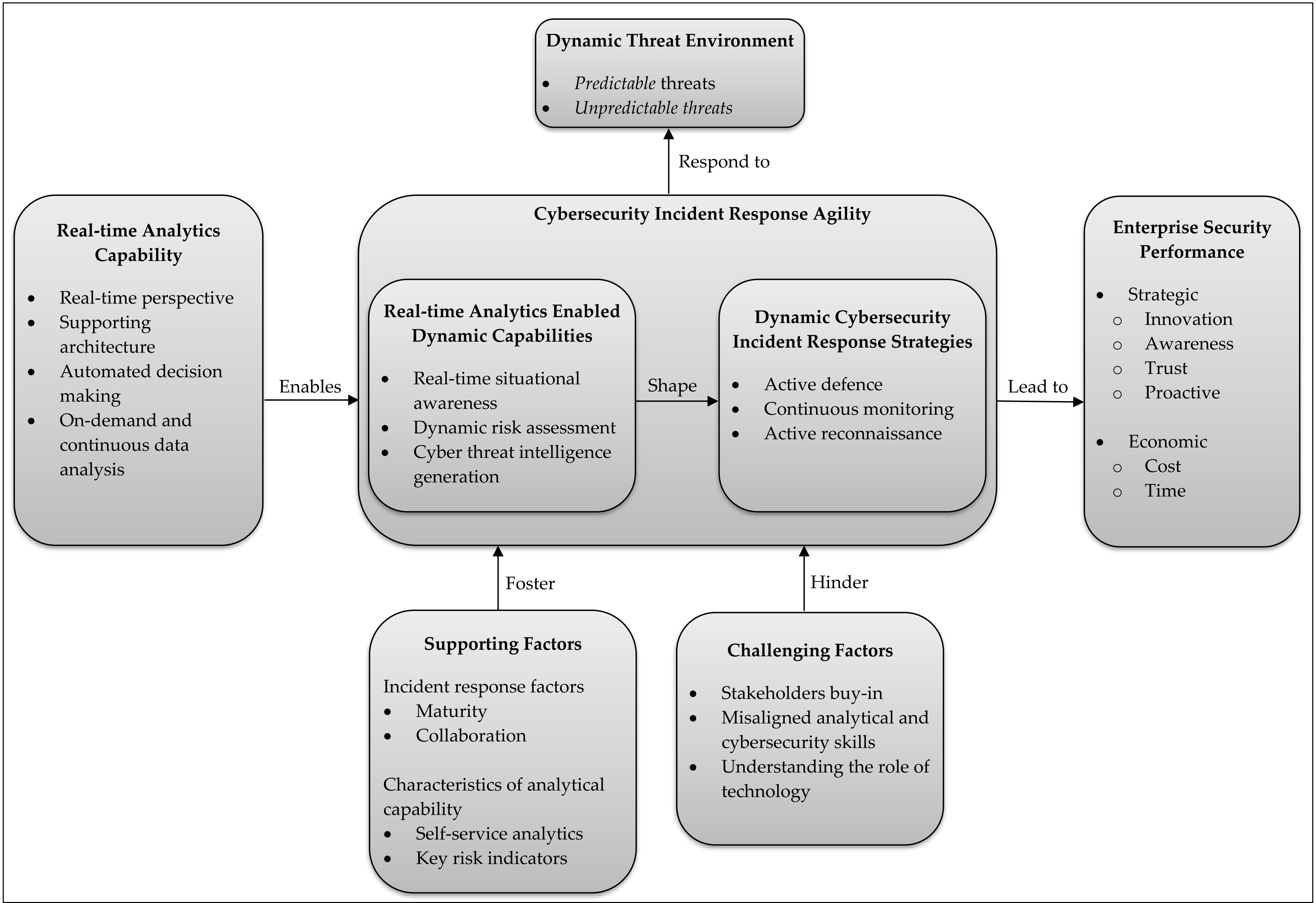

Dynamic Threat Environment
• *Predictable* threats
• *Unpredictable threats*
Respond to
Real-time Analytics Capability
• Real-time perspective
• Supporting architecture
• Automated decision making
• On-demand and continuous data analysis
Enables
Cybersecurity Incident Response Agility
Real-time Analytics Enabled Dynamic Capabilities
• Real-time situational awareness
• Dynamic risk assessment
• Cyber threat intelligence generation
Shape
Dynamic Cybersecurity Incident Response Strategies
• Active defence
• Continuous monitoring
• Active reconnaissance
Lead to
Enterprise Security Performance
• Strategic
○ Innovation
○ Awareness
○ Trust
○ Proactive
• Economic
○ Cost
○ Time
Foster
Hinder
Supporting Factors
Incident response factors
• Maturity
• Collaboration
Characteristics of analytical capability
• Self-service analytics
• Key risk indicators
Challenging Factors
• Stakeholders buy-in
• Misaligned analytical and cybersecurity skills
• Understanding the role of technology

Figure 1-2. A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility

1) **Key features of real-time analytics capability.** This study identifies four key features of real-time analytics capability including real-time perspective, supporting architecture, automated decision making, and on-demand and continuous data analysis. These key features help organizations to integrate, build, and reconfigure their cybersecurity resources, skills and functional competencies and thereby develop dynamic capabilities in their incident response process by investing and using real-time analytics capability.
2) **Real-time analytics enabled dynamic capabilities.** The use of real-time analytics in cybersecurity incident response process enables three types of dynamic capabilities including real-time situational awareness, dynamic risk assessment, and cyber threat intelligence generation. These real-time analytics enabled dynamic capabilities help organizations to execute dynamic cybersecurity incident response strategies such as active reconnaissance, continuous monitoring, and active defence.
3) **Cybersecurity incident response agility.** Real-time analytics enabled dynamic capabilities together with dynamic incident response strategies infuse agile characteristics such as swiftness, flexibility and innovation in cybersecurity incident response process, which in turn, improve agility in cybersecurity incident response process.
4) **Supporting and challenging factors.** The supporting factors related to cybersecurity incident response process that facilitate the development of *real-time analytics enabled dynamic capabilities* and *dynamic cybersecurity incident response strategies* using real-time analytics include *incident response process maturity* and *collaboration* among different stakeholders. In addition, there are two essential characteristics of analytical capability including self-service analytics and key risk indicators that facilitate the development of real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies. The challenging factors in challenges in developing real-time analytics enabled dynamic capabilities and in executing dynamic incident detection and response strategies include stakeholders buy-in, misaligned analytical and security skills and understanding the role of technology.
5) **Enterprise security performance.** The use of real-time analytics to develop *real-time analytics enabled dynamic capabilities* and *dynamic incident response strategies* help organizations to improve their overall enterprise security performance by realizing economic benefits in terms of reducing the cost and time to detect and respond to cybersecurity incidents and strategic benefits in terms of building customer trust, improving security awareness and handling cybersecurity incidents in a proactive manner.

More generally, the details of the framework advance and simplify our understanding of how cybersecurity incident response teams respond to both predictable and unpredictable cybersecurity threats by developing real-time analytics dynamic capabilities and executing dynamic cybersecurity incident response strategies. In addition, the insights from this study expands our understanding of real-time analytics capability and extends the prior literature by identifying its specific dimensions in cybersecurity incident response process including defining the real-time perspective, building supporting architecture, automated decision making, and on-demand and continuous data analysis.

Furthermore, this study contributes to the literature on dynamic capabilities and cybersecurity incident response strategies by identifying real-time analytics enabled dynamic capabilities that enable agility in incident response and shape dynamic incident response strategies. Three real-time analytics enabled dynamic capabilities include real-time situation awareness, dynamic risk assessment, and cyber threat intelligence generation. Three dynamic incident response strategies include active defence, continuous monitoring, and active reconnaissance. While Baskerville et al. (2014) highlight agility as a key characteristics of dynamic incident response and calls for the development of dynamic capabilities in cybersecurity environments that face dynamic and sophisticated attacks, this research extends the prior literature by identifying three specific real-time analytics enabled dynamic capabilities in incident response and explaining how to implement dynamic incident response strategies using these dynamic capabilities and thereby improve agility in cybersecurity incident response.

From a theoretical point-of-view, the framework links real-time analytics capability and cybersecurity incident response agility with enterprise security performance and also presents cybersecurity incident response agility as a manifested type dynamic capability (Park et al. 2017; Teece et al. 2016). Real-time analytics enabled dynamic capabilities help organizations integrate, build, and reconfigure their resources to improve agility in their cybersecurity incident response process. The improved agility in cybersecurity incident response enables organizations to redeploy and redirect its cybersecurity resources, change its existing incident response processes, routines and techniques, or create new ways of responding to both predictable and unpredictable cybersecurity threats in a swift and timely manner. In this way, real-time analytics enabled dynamic capabilities instil agile characteristics of innovation, flexibility and swiftness in incident response that shape dynamic cybersecurity incident response strategies.

From a practical point-of-view, the insights from this research contribute to three groups of stakeholders in cybersecurity incident response practice. For incident response teams, this study's implications include the nuanced view of the role of real-time analytics. Rather than pursuing real-time analytics at the operational level only as a way to continuously monitor the cyber threat environment, incident response teams need to recognize the more innovative role of real-time analytics at a strategic level in implementing both protective and detective response strategies. For cybersecurity managers, the results from this study highlight that in order to build analytical capabilities in cybersecurity incident response, managers need to hire and/or train cybersecurity or analytics personnel with skills and knowledge needed to develop security analytics solutions and integrate and acquire analytical solutions provided by external vendors. For cybersecurity vendors, the findings from this study suggest that they should recognize the potentially far-reaching innovative role that their cybersecurity solutions may provide to enterprises. Creating cybersecurity solutions that can integrate threat intelligence data, automate investigations and forensic analysis, apply complex algorithms and visual analytics to discover the potential threats will help their clients create innovative incident response strategies that can deal with dynamic threat environment (Elyas et al. 2014, 2015).

1.5 Thesis Outline

The structure of the thesis, summarised in Figure 1-3, is as follows.

Chapter 2 provides a systematic review of the literature about the four main domains of this study: business analytics capabilities, cybersecurity management, dynamic capabilities and business process agility. The chapter concludes by identifying research gaps in the literature. *Chapter 3* provides a detailed description of the research design and methodology used in this study. The theoretical framework underpinning the data collection is presented and explained. The justification of the research method along with examination of the qualitative research method are provided. The criteria for case study participants and site selection are also discussed, followed by the explanation of data collection and stages of the data analysis process. Finally, an evaluation of the research design is outlined and explained.

Chapter 4 presents an illustrative story of cybersecurity incident response units of three large financial organizations and analyses their use of real-time analytics in the cybersecurity incident response process. The main narrative in this chapter explains how the use of real-time analytics in the cybersecurity incident response process helped these organizations to develop higher-order real-time analytics-enabled dynamic capabilities and dynamic incident response strategies. In addition, it also describes the impact of using real-time analytics capabilities in cybersecurity incident response process on overall enterprise performance. Finally, the key findings from the data analysis are integrated with existing literature to build an overall framework of dynamic cybersecurity incident response to improve cybersecurity incident response agility. *Chapter 5* provides the findings and key insights of the study in relation to the existing business analytics capabilities, dynamic capabilities, business process agility, and cybersecurity incident response literature. Where appropriate, the connection of this research to broader debates in the IS literature is also presented. Finally, the chapter outlines the implications of this study for IS research and practice. *Chapter 6* concludes the dissertation by summarising the research background, research method, and key contribution of this research project. The chapter also outlines directions for future research and highlights limitations of this study.

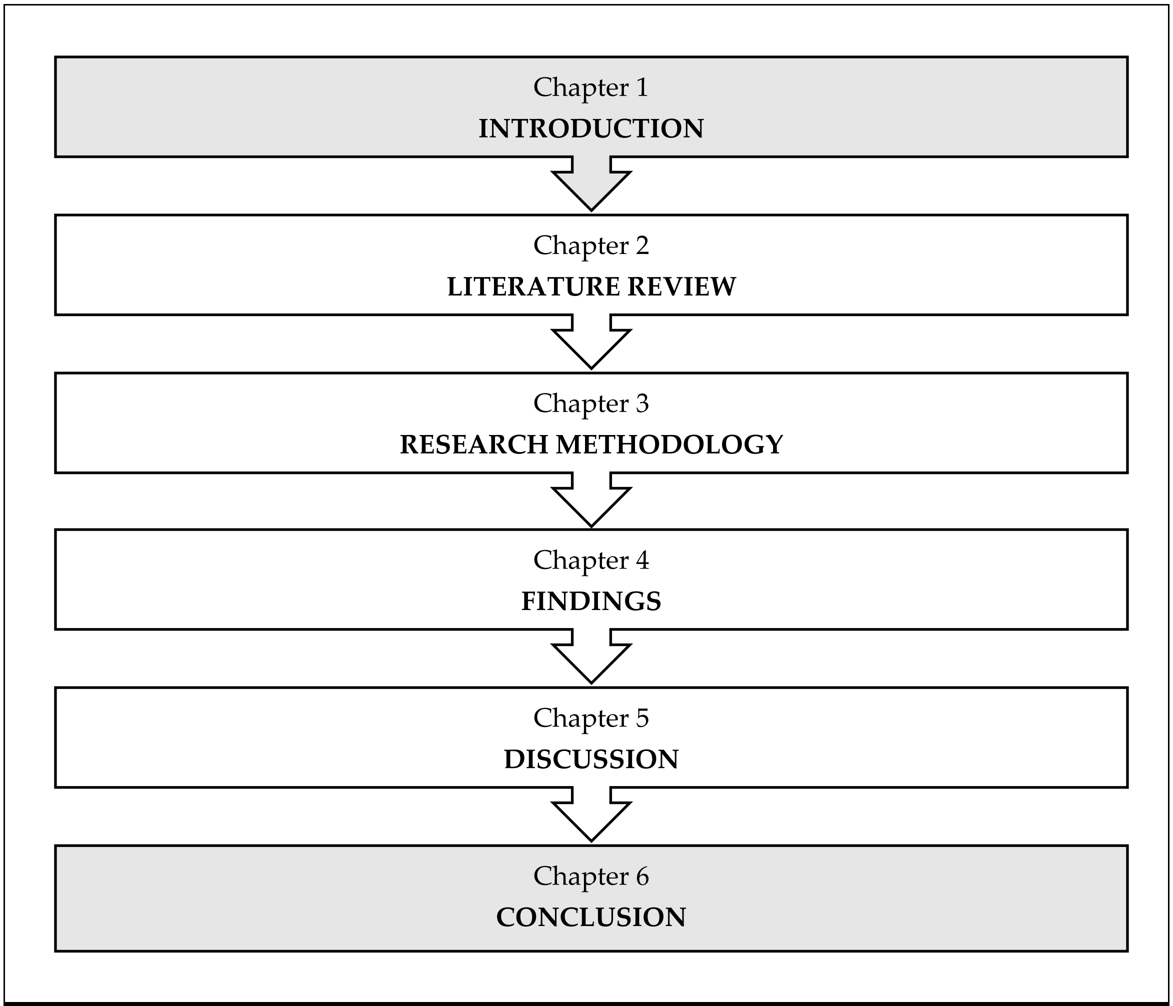


Figure 1-3. Outline of the Thesis

2

"If I have seen farther than others, it is because I was standing on the shoulders of giants."

Sir Isaac Newton (1643 - 1747)

CHAPTER 2. LITERATURE REVIEW

This chapter[1] reviews the literatures of business analytics capabilities (BA), cybersecurity management, dynamic capabilities and business process agility. Section 2.1 provides an overview of the literature review methodology. Section 2.2 examines the literature on dynamic capabilities theory and relates it to organizational agility and then business process agility. In section 2.3, the fundamentals of BA are explained along with evolution of BA concept. Section 2.4 describes the descriptive, predictive, and prescriptive categories of BA capability and introduces real-time analytics as a specialized BA capability. The section also explains the business value of BA capabilities. In section 2.5, the key concepts related to cybersecurity risk management are explained such as cybersecurity risk assessment, enterprise assets, cyber threats, and vulnerabilities. Section 2.6 presents an analysis of the deficiencies in the cybersecurity risk management process. In section 2.7, the cybersecurity incident response

[1] Elements of this chapter are published in the following articles.

Naseer, H., Ahmad, A., Maynard, S., and Shanks, G., 2018, "**Cybersecurity Risk Management Using Analytics: A Dynamic Capabilities Approach**" in *Thirty Ninth International Conference on Information Systems (ICIS)*, San Francisco, USA.

Naseer, H., Maynard, S., and Ahmad, A., 2016, "**Business Analytics in Information Security Risk Management: The Contingent Effect on Security Performance**" in *European Conference on Information Systems (ECIS)*, İstanbul, Turkey.

process is explained in detail. Finally, Section 2.8 presents an analysis of deficiencies in cybersecurity incident response process. The deficiencies identified in the process of cybersecurity risk management and incident response form the basis of this study's overarching research question: *How can organizations improve agility in their cybersecurity incident response process using real-time analytics?*

2.1. Literature Review Methodology

This research conducted a literature review by employing a methodology that has been widely used in information systems research (Watson 2015; Webster and Watson 2002). A systematic categorization and search of the relevant literature provides a reliable and consistent assessment of the contemporary status of a research field. The manner in which articles are identified, interpreted, and analysed is clearly articulated *a priori*, which makes the study (to a degree) repeatable and reduces the possibility of biases (Webster and Watson 2002). The review of literature required for this study is interdisciplinary as it intersects across multiple information systems domains such as business analytics, dynamic capabilities, business process agility and cybersecurity incident response. Therefore, following the methodology proposed by Webster and Watson (2002), a search was performed spanning the cybersecurity management, business analytics capabilities, dynamic capabilities and business process agility literatures. According to Webster and Watson (2002), there are two type of literature reviews:

"From another angle, two types of reviews exist. First, authors could deal with a mature topic where an accumulated body of research exists that needs analysis and synthesis. In this case, they would conduct a thorough literature review and then propose a conceptual model that synthesizes and extends existing research. Second, authors could tackle an emerging issue that would benefit from exposure to potential theoretical foundations. Here, the review of current literature on the emerging topic would, of necessity, be shorter. The author's contribution would arise from the fresh theoretical foundations proposed in developing a conceptual model."

This study follows the second type and reviews the extant literature on the emerging topic of improving cybersecurity incident response agility using business analytics. As a first step, this study examined peer reviewed articles from key information systems journals and conferences from popular literature databases such as Science Direct, ProQuest, JSTOR, and AIS Electronic library using the keywords: 'business analytics capabilities', 'dynamic capabilities', 'cybersecurity incident response, 'real-time analytics', 'in-memory analytics', 'cybersecurity risk management', 'business process agility' in various combinations. These searches identified over 500 articles. This initial list was refined by examining the titles and abstracts of each article to evaluate whether inclusion was warranted (i.e., article appeared to be concerned with or relevant to, the question of improving cybersecurity incident response agility using real-time analytics). This resulted in 150 articles for in-depth review and coding. In an effort to extend the search outside the original set of journals and conferences, additional papers of potential interest were also identified from reference list of reviewed articles (Webster and Watson 2002). As a result, a further set of 60 articles, from journals and conferences other than those formally searched, was collected and a subset of 50 articles was read in full and coded. In line with Webster and Watson (2002, p. 17), the categorization of the literature was concept-driven and was organized around the conceptual framework presented in Figure 2-1. The results that emerged from the analysis of literature, are presented in this research organized by the guiding frameworks and concept matrices (Watson 2015; Webster and Watson 2002). Dynamic capabilities theory was used to integrate and synthesize the literature conceptually. Out of 200 coded articles, 130 included variables of interest and are compiled in the analysis.

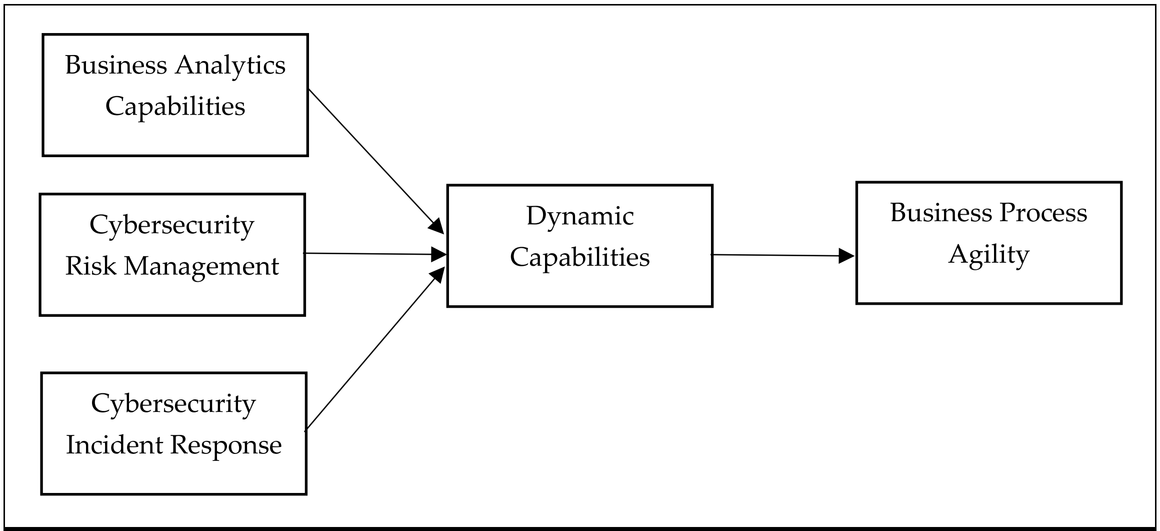

Business Analytics Capabilities
Cybersecurity Risk Management
Cybersecurity Incident Response
Dynamic Capabilities
Business Process Agility

Figure 2-1. Conceptual Framework for Literature Integration, Synthesis and Analysis

The subsequent sections present the theoretical background of this study in detail by examining the relevant areas of literature shown in Figure 2-1. First, the literature on dynamic capabilities theory is examined and used as a useful high-level theoretical lens for understanding how dynamic capabilities improve business process agility and in this case cybersecurity incident response agility. Second, the business analytics capabilities literature is explored with a particular focus on real-time analytics. Finally, the literature on the process of cybersecurity risk management and incident response is analysed to identify the deficiencies in these processes.

2.2. Dynamic Capabilities Theory

The dynamic capabilities theory, by addressing the question of how enterprises can cope with changing business environments, has gained increasing attention in the management literature in recent years, not only in the concept's original domain (strategic management) but also in many other areas including organizational learning, technology transfer, and manufacturing (Teece et al. 1997). This theory is an extension of the resource based view (RBV), which theorizes that organizations can achieve superior firm performance by developing bundles of resources (Barney 1991; Newbert 2007). These resources consist of assets and capabilities and may be tangible or intangible. Assets include applications, infrastructure, data and people, while capabilities include organizational processes, routines, skills and knowledge of the people that utilize assets to perform a task.

While many assets are readily available and some are commodities, an organization's superior performance can be mainly attributed to the unique, valuable, rare, inimitable and non-substitutable capabilities that enable the organization to perform activities more efficiently and effectively than its competitors (Wade and Hulland 2004). A capability is valuable when it enables an organisation to devise and implement strategies that will improve its efficiency and effectiveness (Barney 1991) by exploiting opportunities or neutralising threats. Organisations need to have valuable capabilities simply to survive (Barney et al. 2001; Grant 1991). Rare capabilities are scarce and not possessed by an organisation's competitors. Inimitable capabilities are expensive to imitate and provide organisations with significant cost advantage to organisations trying to develop or duplicate the capability. Capabilities that are valuable, rare and inimitable can provide competitive advantage to an organisation (Ray et al. 2004). Organisational support, including funding and strong management support, is necessary for capabilities that are valuable, rare and inimitable to provide sustained competitive advantage (Barney 1991; Ray et al. 2004).

Although the RBV is prevalent within the extant literature, it has been considered to be essentially static in nature (Ling-yee 2007) as it is inadequate in identifying and explaining the conditions in which capabilities are most valuable (Barreto 2010). The notion of changing conditions is addressed in the dynamic capabilities theory which suggests that external and internal conditions will impact the way organization is managed and subsequently may affect the capabilities required to be competitive in changing environments (Aragon-Correa and Sharma 2003; Barreto 2010). Furthermore, dynamic capabilities theory argues that organizations must adapt depending on the environmental conditions in which they exist. To extend the RBV and to overcome the static nature of RBV theory, scholars have proposed the dynamic capabilities theory (Aragon-Correa and Sharma 2003). The development of dynamic capabilities is valuable for three reasons: (1) to further improve the utility of RBV, (2) to identify conditions that affect the usefulness of different capabilities, and (3) to assess the extent to which different organizational capabilities may provide value (Aragon-Correa and Sharma 2003).

The dynamic capabilities theory emphases on two critical attributes which help organizations achieve competitive advantage in dynamic environments. First, the term 'dynamic' refers to the capacity of the firms to renew their competencies so as to achieve congruence with changing business environment in which innovative responses are required. Second, the term 'capabilities' emphasizes the key role of strategic management in appropriately 'adapting, integrating, and reconfiguring internal and external organizational skills, resources, and functional competences to match the requirements of a changing environment' (Teece et al. 1997, p. 515). Dynamic capabilities are typically built rather than bought and their creation and their evolution are embedded in organizational processes that are shaped by firms' asset positions and the evolutionary paths they have adopted in the past (Teece 2007; Teece et al. 1997). Thus, the dynamic capabilities are the unique processes to integrate, reconfigure, gain and release organizational resources that help organizations to rearrange organizational resources and renew competencies to achieve superior firm performance in changing business environments.

Following (Teece et al. 1997), several alternative conceptualizations of dynamic capabilities has been proposed. Table 2-1 below illustrates the conceptualization of dynamic capabilities by different authors (ordered by data of publication).

Table 2-1. Concept Matrix: Conceptualization of Dynamic Capabilities by different authors (Adapted from Barreto 2010)

Citation	Dynamic Capability Conceptualization
(Teece and Pisano 1994)	The subset of the competences and capabilities that allow the firm to create new products and processes and respond to changing market circumstances.
(Teece et al. 1997)	The ability of the firm to integrate, build, and reconfigure internal and external competences to address rapidly changing environments.
(Teece 2000)	The ability of the firm to sense and then seize opportunities proficiently and quickly.
(Eisenhardt and Martin 2000)	The processes within a firm that use resources—specifically the processes to integrate, reconfigure, gain, and release resources—to match and even create market change; dynamic capabilities therefore are the strategic and organizational routines by which firms achieve new resource configurations as markets emerge, collide, split, evolve, and die.

Table 2-1. Concept Matrix: Conceptualization of Dynamic Capabilities by different authors (Adapted from Barreto 2010)

Citation	Dynamic Capability Conceptualization
(Zollo, M., Winter 2002)	Dynamic capabilities are a stable and learned pattern of collective activity through which organizations systematically generates and alters its operating routines in pursuit of improved effectiveness.
(Winter 2003)	Dynamic capabilities are those capabilities that operate to create, modify, or extend ordinary capabilities.
(Zahra et al. 2006)	The abilities to reconfigure a firm's routines and resources in the manner envisioned and deemed appropriate by its principal decision maker(s).
(Helfat et al. 2009)	The firm's capacity to purposefully extend, modify or create its resource base.
(Teece 2007)	Dynamic capabilities can be disaggregated into the capacity (a) to sense and shape opportunities and threats, (b) to seize opportunities, and (c) to maintain competitiveness through enhancing, combining, protecting, and, when necessary, reconfiguring the business enterprise's intangible and tangible assets
(Teece et al. 2016)	The firm's capacity to innovate, adapt to change, and create change that is favorable to customers and unfavorable to competitors.
(Teece 2018)	Dynamic capabilities include the sensing, seizing, and transforming needed to design and implement a business model.

As illustrated in different conceptualizations of dynamic capabilities in Table 2-1, the common argument among these conceptualizations shows that the dynamic capabilities theory seeks to explain how organizations can achieve superior performance than their competitors in dynamic markets. When the changes occurring in the market are predictable and small, market dynamism can be categorized as following a moderate velocity. However, when unpredictable, unexpected and substantial changes occur in the market, then the market dynamism is of high velocity. Eisenhardt and Martin (2000) propose that moderately dynamic markets are ones in which change occurs frequently, but along a roughly predictable linear path, whereas in highly dynamic markets the change becomes less predictable or nonlinear. The nature of dynamic capabilities varies with the level of market dynamism. In moderate market dynamism, routines and processes that represent codified knowledge are detailed and specific with predictable results (Battleson et al. 2016). In contrast, in high market dynamism, the routines and process may look like unstable, simple and experiential processes that lead to adaptive but unpredictable outcomes (Eisenhardt and Martin 2000).

Dynamic capabilities, while may be distinctive in details, show numerous common features such as extensive external communication, concrete and joint experiences among team members, and the use of cross-functional teams (Eisenhardt and Martin 2000). Therefore, the dynamic capabilities theory incorporates a rich conception of routines as efficient and robust processes in moderately dynamic markets but fragile and semi structured ones in high velocity markets. There are several studies that empirically establish the link between dynamic capabilities and positive outcomes, Eriksson (2014) suggests that the outcomes of dynamic capabilities are not always positive.

(Teece et al. 1997, p. 518) notes that the 'essence of competences and capabilities is embedded in organizational processes'. Teece et al. (1997) further explain that the organizational processes play a significant role in shaping these capabilities, and thereby the competitive advantage that may be gained using these capabilities. Recent research seeks to understand how IT capabilities can be exploited to achieve competitive advantage. For example, Sambamurthy et al. (2003) argue that digital platforms such as supply chain management, enterprise resource planning, and internet computing enable an organization to rapidly recognize changes and respond quickly to changing customer requirements. In line with this, Bharadwaj (2000) recognizes the role of the strategic management of firm IT capabilities as an enabler of organizational agility. In addition, prior studies note that IT infrastructure improves the ability of organizations to detect, process, and communicate information on emerging markets, thereby facilitating organizational sensing and responsiveness (Chakravarty et al. 2013; Lu and Ramamurthy 2011). Thus, IT has been conceptualized as an enabler of organizational agility, a specific type of dynamic capability (Chen et al. 2013; Lu and Ramamurthy 2011; Overby et al. 2006). This study adopts the conceptualization of dynamic capabilities by Teece et al. (1997).

2.2.1. Organizational Agility

Recently, exploring the relationship between dynamic capabilities and organizational agility has received much attention from both academics and practitioners (Park et al. 2017). Most of the studies that have investigated the strategic management of IT capabilities to deal with changing business environments have moved the conceptualization of dynamic capabilities conceived in the strategic management literature (Eisenhardt and Martin 2000; Teece et al. 1997) in the direction of organizational agility (Chen et al. 2013; Overby et al. 2006; Park et al. 2017; Sambamurthy et al. 2003). Prior research has further noted that dynamic capabilities support very specific purposes and activities that typically depend on the context (Helfat and Winter 2011; Pavlou and El Sawy 2011; Peteraf et al. 2013; Winter 2003).

Organizational agility is the ability to sense and respond to external and internal business events of environmental changes in a timely manner in order to seize opportunities and handle threats effectively and efficiently (Van Oosterhout et al. 2006; Overby et al. 2006). Tallon (2008) describe organizational agility as the ability to detect innovation opportunities and seize these opportunities by assembling knowledge, relationships and assets with speed and surprise. Agility encompasses an organization's capabilities to interact with markets by exploring and exploiting opportunities for market arbitrage (Lee et al. 2015). Thus, agility is conceptualized as one of the dimensions of dynamic capability (Sambamurthy et al. 2003).

Teece et al. (2016) have recently highlighted organizational agility as a manifested type of dynamic capability. Organizational agility enables an organization to redeploy/redirect its resources, change its existing processes, routines and techniques, or create new ways of acting in a timely manner in order to effectively deal with changing environment regarding their competition, supply chains, customers, technologies and regulations. When there is deep uncertainty in the business environment, agility is likely to be a valuable organizational capability (Teece et al. 2016). Organizational agility is manifested by and focuses on supporting enterprise-wide strategic tasks of sensing and responding to external and internal business events of environmental changes in a timely manner to seize opportunities and handle threats efficiently and effectively (Chen et al. 2013; Lee et al. 2015; Overby et al. 2006; Park et al. 2017; Roberts and Grover 2012; Sambamurthy et al. 2003). The extant IS research literature suggests that IT enabled dynamic capabilities play a vital role in enterprises achieving organizational agility. Table 2-2 presents a summary of articles that examined the relationship between IT and organizational agility (ordered by date of publication).

Table 2-2. Concept Matrix: Studies Examining Relationship Between IT and Organizational Agility

Citation	Methodology	Specific Dimensions of Agility	IT and Agility Relationship
(Sambamurthy et al. 2003)	Conceptual Theory Development	Operational agility, customer agility, and partnering agility	IT generates entrepreneurial alertness and digital options, which in turn help firms to achieve agility.
(Overby et al. 2006)	Conceptual theory development	Sensing agility and responding agility	Knowledge-oriented IT increases sensing agility, and process-oriented IT increases responding agility.
(Tallon 2008)	Empirical theory testing and development	Business process agility	Managerial IT capabilities lead to the development of technical IT capabilities which, in turn, drives business process agility

Table 2-2. Concept Matrix: Studies Examining Relationship Between IT and Organizational Agility

Citation	Methodology	Specific Dimensions of Agility	IT and Agility Relationship
(Tallon and Pinsonneault 2011)	Empirical theory testing and development	Operational agility, customer agility, and partnering agility	IT-business alignment has a positive impact on agility. It does not find a negative impact of IT on agility.
(Nazir and Pinsonneault 2012)	Conceptual theory development	Sensing agility and responding agility	Both internal and external electronic integrations are necessary to enhance organizational agility.
(Roberts and Grover 2012)	Empirical theory testing and development	Sensing customer agility and responding customer agility	IT enables both customer sensing and responding capabilities through processing enhancing synergy and knowledge creating synergy. Alignment between sensing and responding agility types matters for competitive activities.
(Chakravarty et al. 2013)	Empirical theory testing and development	Adaptive agility and entrepreneurial agility	IT has an enabling and facilitating impact on agility.
(Lee et al. 2015)	Empirical theory testing and development	responsiveness, Proactiveness, adaptiveness and radicalness,	IT ambidexterity enables operational ambidexterity, which, in turn, increases organizational agility.
(Park et al. 2017)	Empirical theory testing and development	Sensing agility, decision making agility, and acting agility	Business intelligence and communication technologies help organizational to achieve organizational agility.

As Table 2-2 illustrates, prior research has shown that the effective and efficient management and use of IT capabilities facilitate and enable organizational agility (Chakravarty et al. 2013; Roberts and Grover 2012). Organizational operational capability mediates and analytical capabilities, environmental dynamism and IS integration moderate IT's impact on agility (Chakravarty et al. 2013; Lee et al. 2015; Roberts and Grover 2012). In addition, the strategic alignment between IT and business (Nazir and Pinsonneault 2012; Tallon and Pinsonneault 2011), IT infrastructure flexibility (Lu and Ramamurthy 2011), IT ambidexterity—the ability to simultaneously explore and exploit IT capabilities (Lee et al. 2015), and business intelligence and communication technologies (Park et al. 2017) all appear to play an enabling role in achieving organizational agility.

Sambamurthy et al. (2003) highlight three dimensions of dynamic capability: agility, digital options, and entrepreneurial alertness. Organizational agility refers to the ability to detect and seize opportunities for innovation by assembling essential resources in a timely manner. Digital options refer to the ability to develop digitized enterprise work processes and knowledge systems to integrate, inform and automate business activities using dynamic capabilities. And entrepreneurial alertness refers to the ability to explore business market, detect any potential opportunities in the market and determine actionable opportunities. Sambamurthy et al. (2003) argue that IT enables firms to develop agility and digital options through entrepreneurial alertness and these dimensions play a mediating role between IT investments and organizational performance.

Similarly, Pavlou and El Sawy (2006) explain how the effective use of IT capabilities by business units can help to reconfigure business processes and thereby build competitive advantage. Organizations can use IT to improve organizational agility and increase their alertness to deal with the challenges they face in increasingly changing business environments. Specifically, Wang et al. (2013) note that IT infrastructure flexibility increases the alertness of an organization by developing capabilities for detecting and seizing marketing opportunities. Furthermore, IT capabilities can help increase various types of organizational agility such as market capitalization agility, strategic agility and operational agility (Fink and Neumann 2007; Lu and Ramamurthy 2011; Park et al. 2017).

2.2.2. Business Process Agility

A particular type of organizational agility that is of specific interest to IS research is business process agility, or the degree to which organizations can swiftly and easily reshape their business processes to deal with dynamic market environment (Tallon 2008). Business process agility emphasizes on the need for an enterprise to detect environmental changes, threats and opportunities and then provide focused and swift responses to stakeholders and customers by reconfiguring business processes and resources (Mathiassen and Pries-Heje 2006). Agile business processes are likely to help enterprises achieve cost economies by prioritising the ease and speed with which they react to changes in the market environment. Therefore, business process agility is a vital mechanism through which enterprises deal with dynamic market environment and can explain the variance of inter-organizational performance over time (Van Oosterhout et al. 2006; Raschke 2010). In addition, it also helps enterprises to take competitive actions and exploit opportunities for innovation (Chen et al. 2013; Sambamurthy et al. 2003).

However, while organizations are paying increasing attention to enable business process agility, not enough is known regarding how to actually become more agile in specific business processes (Chen et al. 2013; Park et al. 2017; Sambamurthy et al. 2003; Teece et al. 2016). In this sense, business process agility is a rare capability. In addition, business process agility not only allows organizations to redesign and reconfigure their existing processes, techniques and routines but also to create new processes rapidly in order to be able to take advantage of uncertain market conditions (Raschke 2010). By doing so, this procedure is rooted in organizational routines and processes, thus making it harder for organization's competitors to discern which parts or processes are valuable. Thus, business process agility is difficult to imitate and non-substitutable (Barney 1991). To summarize, business process agility has the characteristics of a strategic organizational capability that can help enterprises to better acquire and deploy resources to deal with dynamic and uncertain business environments (Teece et al. 2016).

The aforementioned conceptualization of business process agility implies the capabilities of speed, flexibility, and innovation. Business process agility provides organizations with the ability to respond quickly to market dynamics, customer demands, and emerging technology options (Mathiassen and Pries-Heje 2006). This kind of agility can be demonstrated by swiftness in sensing relevant events, interpreting what is happening and assessing the consequences for the organization, exploring options and making decisions, and implementing appropriate responses (Teece et al. 2016). With business process agility, organizations can flexibly and rapidly redesign or reconfigure existing processes or create new ones to cope with dynamic market conditions (Teece et al. 2016).

Extending the aforementioned observations on IT enablement of dynamic capabilities and business process agility to a specific IT capability real-time analytics and business process cybersecurity incident response agility, this study seeks to investigate how organizations improve cybersecurity incident response agility by developing dynamic capabilities in incident response using real-time analytics.

2.3. An Overview of Business Analytics

Business Analytics (BA) deals with the development of systems, practices, applications and technologies that analyse critical business data to generate new insights about business and markets (Chen et al. 2012; Wixom et al. 2013). The new insights can be used to take actions and thus make practice of 'evidence-based decision making' possible in business (Davenport et al. 2010; Davenport and Harris 2007; Seddon et al. 2017). Understanding of the concept of BA can be developed from an examination of its heritage (Lim et al. 2013). In general, the traditional views of BA in current era are concerned with analysis of data in some way, with an aim of supporting and improving business processes and activities, for example decision making. The data analysis lies at the heart of decision making related to all business process and activities. The data analysis activities may involve calculation, inference or examination. BA systems are the latest in lengthy list of technologies that have been developed to improve and support decision making related to business processes and activities (Shollo and Galliers 2016). The use of data to support managerial decision making can be conceptualized as moving through three generations.

When mainframe computers were introduced in the 1950s, they were used to develop the first generation of data processing systems that supported managerial decision making called management information systems (MIS). In mid 1960s, these systems were followed by decision support systems (DSS) and executive information systems (EIS) (Davenport and Harris 2007; Inmon 2002). DSS applications required a storage area where data could be stored for longer duration of time than the transactional systems. The data for DSS application was then sourced not only from operational systems, but also other data, such as external data. The data was customized for the specific DSS that was developed. This was a very application-centric approach, with the data supporting a single or a few related applications. It did, however, show the critical role of data in decision support.

In late 1970s, the relational database systems were developed with the ability to capture large quantities of data and improved data modelling capability. This led to the arrival of the second generation of data processing systems such as data warehousing and online analytical processing systems (Inmon 2002) and the concept of knowledge management and knowledge management systems. Organizations in the financial services, retailing, and telecommunication industries developed data warehouses to store vast amounts of sales and customer-related data. Firms in these industries still remain the leaders in terms of the size of their data warehouses and how the data warehouses are used making informed decisions. Unlike the first generation DSS, data warehouses tend to be data-centric. While a single or a few applications may be used to help make the business case for building the data warehouse, the data is modelled to support a variety of applications. The concept of "single source of the truth" was coined by Bill Inmon, the "father of data warehousing" and now it is commonly used to describe the official repository of data that applications are supposed to use to generate insights that can help business executives to make informed decisions. In late 1980s, business intelligence (BI) systems were developed. BI systems are integrated systems that are linked to an enterprise data warehouse and other applications and are designed to facilitate the analysis of stored (real-time and historical) data in support of ad hoc managerial decision-making (Davenport and Harris 2007).

In 2000, the third generation of information systems designed to support managerial decision making began with the movement to real-time data warehousing (Watson et al. 2006). The major reason this development is significant, different and worthy of being a new generation is the changes in the way that data in the data warehouse is used. Traditionally, data are loaded “into a data store that is subject-oriented (modelled after business concepts), integrated (standardized), time-variant (permits new versions), and non-volatile (unmodified and retained)” (Inmon 2002). The loading requires an established data dictionary and a data warehouse that serves as the storage location for verified data that the organization will use for analysis. In addition, the data was primarily employed to gain an understanding of what had already happened in the past to learn from it and to predict what would happen in the future. The architectures used to build the data warehouse is based on a save-and-process paradigm in which data are first saved to a device and then queried (Watson et al. 2006). The use of data warehouse to influence current operations and real-time decisions was limited. With real-time data and analytics, current decisions and critical business processes, such as supply chain applications and customer-facing, can be significantly enhanced. In this way, real-time analytics is a proactive process that enables the monitoring of business events in real-time based on data coming from operational systems and enables organizations to make decisions and respond quickly to events as they occur such as potential opportunities or threats (Phillips-Wren et al. 2015). Figure 2-2 below shows the evolution of information systems that were designed to support managerial decision making, starting from static reports and leading to interactive reports, dashboards and analytical applications.

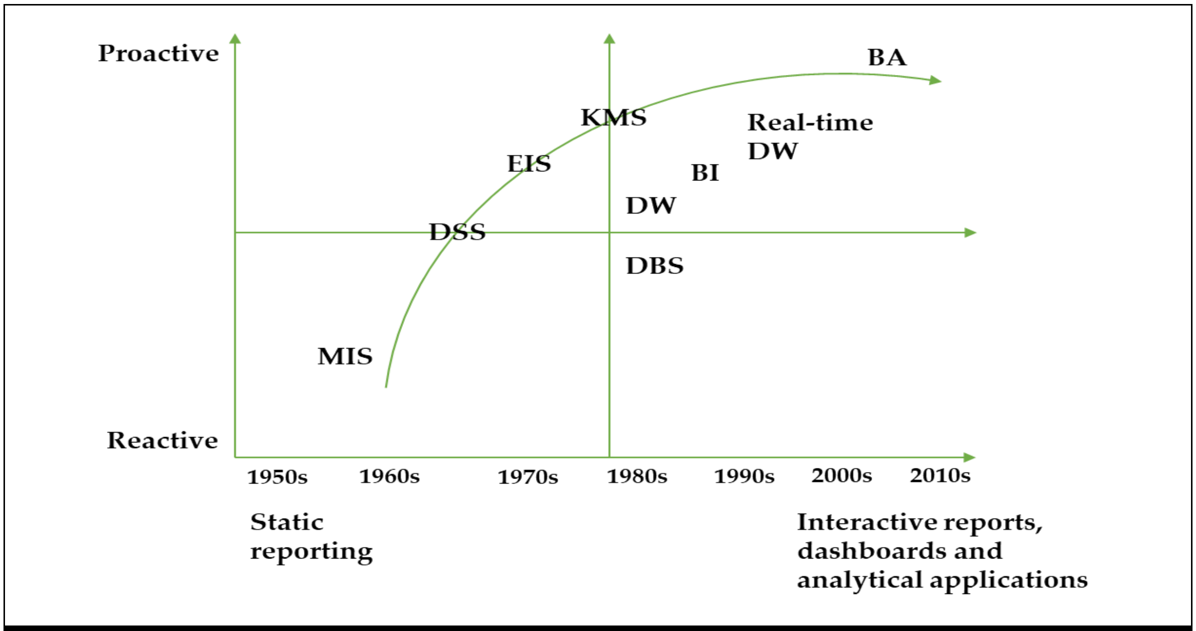


Figure 2-2. The Evolution of Information Systems Designed to Support Managerial Decision-Making

As Figure 2-2 shows, the latest in the line of data processing systems are business analytics (BA) systems that are used to build and utilize various analytical capabilities for organizational business processes and decision support (Chen et al. 2012; Eckerson 2012; Wixom et al. 2013). BA systems consist of broad range of methodologies, analytical techniques and technologies that are combined to support decision making related to business activities (Holsapple et al. 2014). In particular, BA systems consist of three components: data warehouse, analytical knowledge discovery techniques, and business performance management (BPM). This view of BA systems is explained by Davenport et al. (2007) as "the use of data, analytical techniques, and fact-based management methodologies". Data management, analytical knowledge discovery techniques, and BPM are crucial components of BA as they all enable each other.

2.3.1. Data Management

First, data management is a key component and building block of BA. The aim of BA applications is to harness data from disparate source systems and generate intelligence or insights regarding services, products, purchasing, sales, manufacturing, and customers. Therefore, the input for BA systems are the data stored in various enterprise data platforms. With the evolution of BA systems, their capability to process various types of data such as structured, semi-structured and unstructured data has also advanced.

According to (Russom et al. 2014), most of the data used for analytics in organizations is structured data that reside in tables, spreadsheets, and relational databases. Structured data corresponds to a data model that addresses the properties and relationships between them and have known data types, lengths, and restrictions. Structured data coming from a single source system can be easily captured, organized and queried due to its known structured and standards.

In recent times, semi-structured data are also increasingly used for analytics (Russom et al. 2014). Semi-structured data lack a rigid and strict structure but still have identifiable features. For example, images and photos can be tagged with date, time, creator, and other keywords to assist business users to find and organize them. Email is another example of semi-structured data that have fixed tags including time, data, sender, and recipient attached to the contents. Web pages also have identifiable elements that enables organizations to exchange information with their business partners. Lastly, industry standard such as Extensible Mark-up Language (XML) enable computing devices to identify semi-structured data by defining a set of rules for processing.

Unstructured data is also growing in importance for analytics (Davenport et al. 2010). These data are primarily in the form of human language text and are ill-defined such as video, audio, wikis, blogs, presentations, emails, text documents and web pages (Chen et al. 2012). Unstructured data mostly comes from external sources such as social media, the Web, and sensors. Text mining and natural language processing tools are usually used to analyse unstructured data.

Most of the structured, semi-structured and unstructured data coming from different source systems (e.g., customer relationship management, enterprise resource planning, supply chain management, social media and content management systems) are not suitable for data reporting and analysis without processing. Therefore, data integration or transformation through ETL (extract, transform, and load) becomes an important process for an organization's data management and enterprises usually build a data warehouse to store variety of data at a centralized location for querying, reporting, and analysis. Once data are identified as pertinent, a data warehouse team extracts data from primary sources and transforms them to support the decision objective (Watson and Wixom 2007). The capability to manage data coming from disparate source systems efficiently and effectively influences organizational performance (Seddon et al. 2017; Shanks et al. 2010; Shanks and Bekmamedova 2013).

2.3.2. *Analytical Knowledge Discovery Techniques*

Second, the data harnessed from different source systems and stored in a centralized repository such as data warehouse and the insights generated from data analysis must be utilized to make informed decisions and create business value (Sharma et al. 2014). Various data mining or knowledge discovery techniques are used to analyse the data and generate insights that provide useful information such as what customers are going to do, what events are going to happen in the market place, objective function, performance optimization, and business constraints. Data mining techniques can be categorized in three broad approaches: association, clustering and classification. Especially in recent times, the data mining technique that is receiving increasing attention is statistical modelling. For example, building artificial intelligence-based or regression models that can predict future business cases or events based on learning from the historical data.

In addition to statistical modelling, optimization and simulation applications are also modern business analytics techniques that are actively used in supply chain management. The use of aforementioned BA techniques improve efficiency within the supply chain network and provide valuable decision-making knowledge to accurately forecast market trends and minimize operating costs (Trkman et al.

2010). Organizations with more mature business analytics practices in supply chain management are reducing their costs faster and achieving higher profit margins than their less mature peers (Oliveira et al. 2012). Furthermore, BA systems also enables higher level and quality of information sharing within the supply chain network and thereby can lead to an enhanced competitive advantage and improved performance (Oliveira et al. 2012; Trkman et al. 2010).

2.3.3. Business Performance Management

Lastly, BPM is another key building block and vital component of BA. BPM enables three broad sets of activities in any business that include reporting, monitoring and analysis (Eckerson 2012). Organizations use various tools, processes and techniques to perform aforementioned three BPM activities. For example, organizations use key performance indicators (KPIs) and other metrics to monitor, report and analyse their performance in various business areas such as supply chain, marketing, finance, and procurement using dashboards and scorecards technologies (Eckerson 2010). The analysis process in BPM also requires systematic approaches to query data and identify root causes in order to develop ideas for business improvement.

2.4. Business Analytics Capability

Organizations are increasingly achieving competitive advantage by using BA capability, which includes people, process and technology that help in turning data into insights which in turn drive informed business decisions and actions (Chen et al. 2012; Wixom et al. 2013). The most important aspect of BA capability is the development of reporting and analysis applications (Eckerson 2012). These applications enable organizations to collect, store and analyse important business data to generate new insights about business and markets. The analytical solutions that organizations develop using BA capability include data marts, enterprise data warehouses, scorecards, dashboards, online analytical processing (OLAP) and data mining (Holsapple et al. 2014; Popovič et al. 2012).

Analytics in particular refers to a systematic computational analysis of data or statistics (Davenport et al. 2010). Building on the analytical perspective, BA capability can be broken down into three categories: (1) descriptive analytics; (2) predictive analytics; and (3) prescriptive analytics (Chen et al. 2012; Watson 2014). It is useful to differentiate between these categories because the differences have the implications for the people, process, technology and architecture required to develop BA capabilities.

2.4.1. *Descriptive Analytics*

Descriptive analytics uses historical data to provide trending information on past or current business events (Wixom and Goul 2014) and answers the questions such as "What has happened?". Descriptive analytics is the most common type of analytics used by the business managers that gives them insights on the past and the context they need for future actions. By combining data from different, and disparate sources and then comparing and contrasting data, descriptive analytics provides a comprehensive view and context for historical business events.

The process of analysis, and reporting using descriptive analytics spans a wide range of activities that needs to occur at various stages in using and managing data (Eckerson 2012). Querying data from relevant source systems is often the first step in reporting and analysis process and requires a predefined and often routine call to data storage for a particular piece of information. In contrast, ad hoc querying is unplanned and is mostly used for what-if analysis. Characterized by the use of KPIs, descriptive analytics drills down into data to uncover details such as the cost of operations, the frequency of business events, and the root cause analysis. Business intelligence systems usually provide descriptive insights though reports, OLAP, dashboards and scorecards (Eckerson 2012).

2.4.2. *Predictive Analytics*

Predictive analytics provides insights that exceed beyond using historical data as the principal basis for business decisions and answers the questions such as "What could happen?". Some scholars also refer to predictive analytics as exploratory or discovery analytics, although these are just other names for predictive analytics. Predictive insights help business executives anticipate likely scenarios so that they can plan ahead, rather than reacting to what has already happened (Lim et al. 2013). Using descriptive data accumulated over time, predictive analytics involves building statistical models for predicting business events. It does not, however, recommend actions. Predictive capabilities enabled by predictive analytics such as simulation and forecasting provide enhanced insight that business managers can use to make more informed decisions.

Statistical analysis and data mining applications commonly provide predictive insights (Eckerson 2012). Characterized by the use of correlations to identify patterns and time-series data analysis to analyse trends, predictive analytics uses data mining and advanced statistical analysis and sophisticated mathematics functions to validate assumptions and test hypotheses. This, in turn, provides a solid, data-based foundation that can raise managers' confidence in making future business decisions. According to (Wixom et al. 2013), organizations that use BA to determine why and what actions they should take are twice as likely to outperform their competitors. Such organizations use predictive analytics to make their daily operations to major business decisions.

2.4.3. *Prescriptive Analytics*

Prescriptive analytics explores a set of possible actions and suggests a reliable path to optimal solution based on descriptive and predictive analyses of complex data and answers the questions such as "What should we do?" (Wixom and Goul 2014). Though the final decision is up to the business managers, prescriptive analytics solutions provide the most reliable path to an optimal solution for business needs or resolution of operational problems.

Optimization applications generally provide prescriptive insights (Eckerson 2012). (Watson 2014) notes that Harrah's Entertainment, a leader in the use of analytics, actively uses prescriptive analytics in revenue management for hotel room pricing for many years. Characterized by constraints, rules and thresholds, prescriptive analytics makes use of mathematical models and advanced capabilities such as optimization to reveal not only recommended actions but also why they are recommended, along with any implications the actions might have.

Prescriptive analytics also takes uncertainty into account and recommends ways to mitigate the risks that can result from it. Its ability to not only examine potential outcomes but also make recommendations helps business managers make decisions when the data environment is too large or complex to be understood without the help of technology.

According to Watson (2014):

"*Organizations typically move from descriptive to predictive to prescriptive analytics. Another way of describing this progression is: What happened? Why did it happen? What will happen? How can we make it happen? This progression is normally seen in various BI and analytics maturity models (Eckerson 2004).*"

2.4.4. *Real-time Analytics – A Specialized Business Analytics Capability*

The descriptive, predictive and prescriptive analytical applications are valuable to business because they provide insights for both historical analysis and future planning. However, these applications have latencies such as data latency, analysis latency and decision latency (see Figure 2-3) as data are first saved to an analytical platform and then processed for insights generation (Hackathorn 2004; Phillips-Wren et al. 2015).

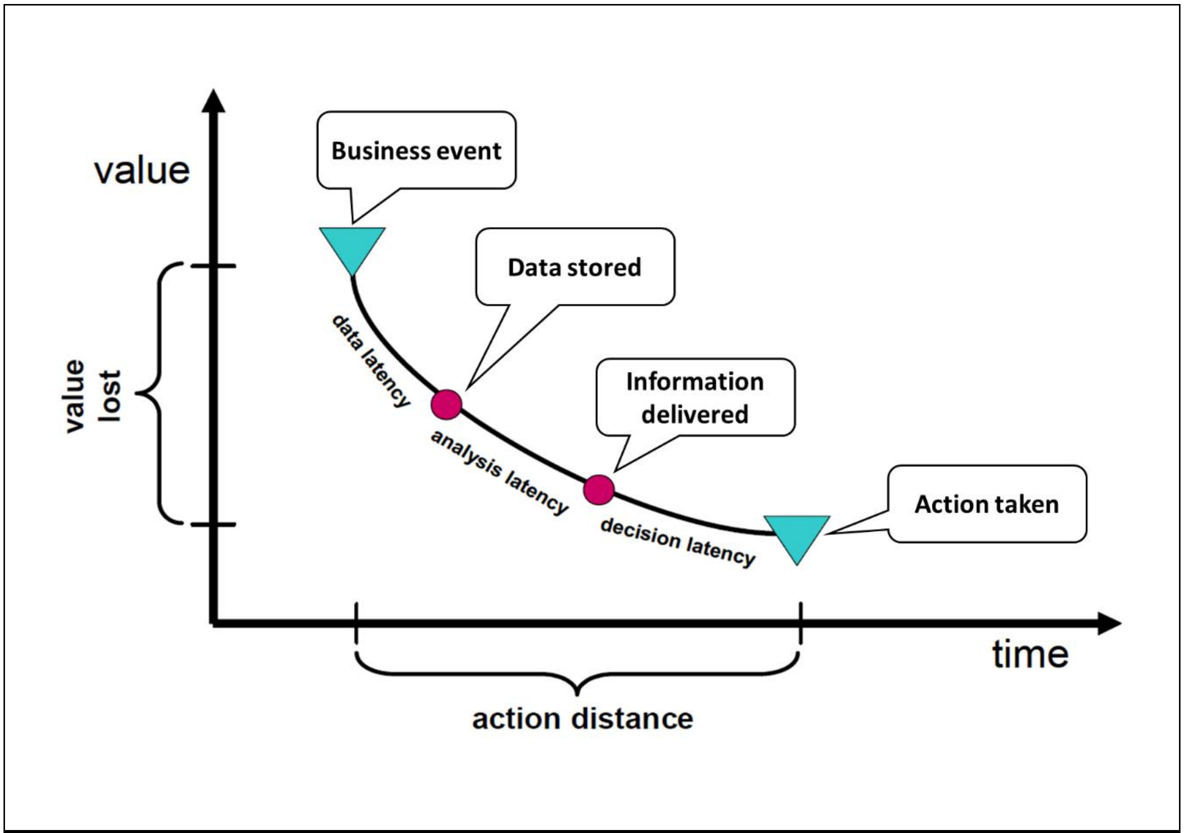


Figure 2-3. Business value vs latency (Adapted from Hackathorn 2004)

Data latency is the duration of time between when an event occurs and when the associated data is stored in the data warehouse. Analysis latency is the length of time between when the data is stored and when it is analysed and made available to users and applications. Decision latency is the duration of time from when the information is available to the decision maker until some action is taken on it. These three sources of latency are additive and result in total latency.

These applications are therefore not ideal for business events that need to be analysed as they occur (for example, fraud and cyber-attacks detection, event-based campaigns, and situational intelligence). The reduction of data and analysis latency depends primarily on the technologies and analytical architecture. Recent developments in analytical platforms provide help in this regard. However, reducing decision latency requires changes in how people use information in performing their jobs and business processes. Providing fresher data does not create business value unless it is used in a timely manner (Townsend et al. 2018). Dealing with decision latency is usually more challenging than data and analysis latency. To address this problem, BA scholars have proposed the concept of real-time analytics which is a specialized BA capability that enables monitoring and analysis of business events as they occur (Phillips-Wren et al. 2015; Watson et al. 2006). Reducing the decision-making time in order to increase business value is the main objective for real-time analytics (Townsend et al. 2018). When analytical processes are linked in real time to business operations and processes, it is possible to take corrective action before problems materialize (Watson et al. 2006).

Real time analytics is the latest development in business intelligence and analytics and it is significant because it has the potential to affect business processes, operations and tactical decision making (Watson and Wixom 2007). Initially storage and processing constraints meant that data for BA was typically kept at a summary level (daily, weekly, monthly etc), and there was a significant time delay in creating and using these summaries. Data mining and analytics on transactional systems was generally not done on real-time data, other than for areas like fraud detection. BA was typically used at a strategic or tactical level and not so much at operational level. However, with cost-effective advances in processing and storage of data have now facilitated BA at business process and operational levels, with increased use of real-time analytics. Real-time analytics has the potential to deliver significant benefits and value to organizations by improving business processes such as supply chain management, customer relationship management and marketing (Bärenfänger et al. 2014; Hahn and Packowski 2015; Xu et al. 2016).

Even though the concept of real-time analytics exists in BA literature and BA practice for more than a decade, the understanding of this concept is still limited in terms of what is the meaning of term "real-time" and what additional capabilities are required in typical BA architecture to enable real-time analytics (Dobrev and Hart 2015; Phillips-Wren et al. 2015). In addition, real-time analytics is still an emerging field that is receiving a lot of attention with the advent of big data since the data is generated at a high velocity, in high volumes and with a wider variety of data types and needs to be analysed more efficiently and in a timely manner (Phillips-Wren et al. 2015).

Since the concept of real-time analytics is still developing and needs more investigation, this study therefore seeks to expand and build upon our understanding of real-time analytics by exploring its role in developing real-time analytics enabled dynamic capabilities that are necessary to achieve agility in cybersecurity incident response.

2.4.5. *Business Value of Business Analytics Capability*

The overall value of BA practice in any organization can be explained as a simple workflow, turning data into insights, analysing the insights in a specific context to make informed decision (preferably profitable decisions) that can lead to value (Eckerson 2012, Sharma et al 2014). According to Wixom et al. (2013), once BA capabilities are developed and established, the organizations continuously execute the workflow of turning data into insights and actions and thereby make BA usage pervasive across the enterprise that, in turn, maximize their business value. Similarly, Gupta and George (2016) propose a theoretical framework which provides the evidence that big data analytics capability leads to superior firm performance. Shanks and Bekmamedova (2012) suggest that operational and dynamic BA capabilities lead to competitive advantage and improved business value. However, the process for value creation is different for various IT enabled capabilities. Thus, it is vital to understand the unique value creation processes and mechanisms for BA capabilities (Fink et al. 2017). Apart from specific BA capabilities, (Kevin et al. 2014) study in the manufacturing domain shows that accurate manufacturing data and the application of advanced analytics on it could be valuable resources for creating business value.

The key performance indicators that business executives analyse using BA capabilities range from decision-making effectiveness (Cao et al. 2015) to more complex metrics comprising process capabilities perspective, customer perspective, market perspective, financial perspective, and learning and growth perspective (Bronzo et al. 2013). Performance implications for the firm practicing marketing analytics were obtained from the metrics such as return on investment, profit and unit's total sales growth (Germann et al. 2013), whereas Kevin et al. (2014) highlight five KPIs to measure performance in manufacturing data analytics: delivery flexibility, order fulfillment, flexibility to change product mix, delivery as promised, and flexibility to change output volume.

Similarly, Kohli (2007) notes a number of metrics that managers at United Parcel Service (UPS) analysed through analysis of data in their highly integrated data warehouse to gain meaningful insights. Those include estimates of the amount of fuel that could be saved by minimising the number of left turns on their delivery routes, profitability and cost estimates of individual delivery routes, and plausible explanations for a growing backlog of package. In addition, (Watson 2001) note a number of insights that Harrah's gain into the gambling behaviour of its casino customers and (Watson et al. 2006) describe insights into customer loyalty scheduling, and pricing that Continental Airlines gained through use of its data warehouse.

According to Krishnamoorthi and Mathew (2018), there are still very limited studies on business value of BA. Similarly, regarding the research on BA, Watson (2014) notes that: "Analytics is not fully understood, there are many incorrect, imprecise, and incomplete understandings". Available case studies and success stories in both scholarly and practitioner literatures have given a head start on BA capabilities and provide the evidence that BA practices and systems deliver significant benefits to organizations and contribute to firm performance (Anderson-Lehman et al. 2004; Cosic et al. 2012, 2015; Davenport et al. 2010; Davenport and Harris 2007; Elbashir et al. 2008; Kohavi et al. 2002; Kohli 2007; Oliveira et al. 2012; Piccoli and Watson 2008; Shanks and Bekmamedova 2013; Watson et al. 2006; Wixom et al. 2013). A summary of few published BA applications and the mechanisms through which firms achieved enhanced performance in various industries is illustrated in Table 2-3.

Table 2-3. Concept Matrix: Application of BA in Various Industries

Industry	Application	Mechanisms contributing to superior firm performance and competitive advantage	Citation
Airlines	Real-time business intelligence to analyse data about customers, flights, and reservations.	Understanding the profiles of most profitable customers Personalized interactions with customers	(Anderson-Lehman et al. 2004, p. 167)
Insurance	Insurance underwriting process	Optimal pricing of insurance policies to better reflect risks	(Davenport and Harris 2007, p. 62)
Hospitality	Analysis of customer data to create customer value models	Personalized interactions with customers to give a unique and tailored experience	(Piccoli and Watson 2008, p. 117)
Transportation and Logistics	Analysis of parcel delivery data to overcome backlog of packages	Correct customer mistakes and charge them for the service	(Kohli 2007, p.204)
Retail	Analysis of clickstream data generated by a website	Reduce customer shopping cart abandonment	(Kohavi et al. 2002, p. 46)
Supply Chain	Analysis of supply chain data in plan, source and deliver	Analyse performance of supply chain by applying analytics in different areas of supply chain such as plan, source, make and delivery	(Trkman et al. 2010, p. 321)
Manufacturing	Business analytics and advanced analytical techniques to analyse manufacturing data	Analyse performance related metrics such as order fulfillment, flexibility to change product mix, flexibility to change product volume, delivery as promised and delivery flexibility to improve operational performance.	(Kevin et al. 2014, p.122)

These aforementioned case studies and success stories are further encouraging organizations to explore new business analytics domains and to collect and analyse new sources of data since they provide new insights. Holsapple et al. (2014) notes cybersecurity risk analytics as a potential domain in which features of BA capability can be applied. In addition, cybersecurity data is one of the new data sources that are recently catching a lot of attention (Chen et al. 2012; Talabis et al. 2014). Cybersecurity data encompasses any type of information that could contribute to a holistic view of an organization's cybersecurity threats and its possible business risks (Pierazzi et al. 2016). Sources of security data include traditional structured data such as logs, instrumentation data, network data, as well as new unstructured sources such as video surveillance feeds, geospatial information, and social data (Talabis et al. 2014). Therefore, BA presents organizations with a unique opportunity to quickly harness this cybersecurity data by employing real-time analytics and thereby improve their cybersecurity by detecting ongoing cybersecurity incidents as they happen and respond to them in a rapid and proactive manner. Since the application of business analytics and in particular real-time analytics in cybersecurity is still limited and needs further investigation, understanding the relationship between real-time analytics and cybersecurity incident response agility and real-time analytics role in developing dynamic capabilities would be a contribution to the literature.

2.5. Cybersecurity Risk Management

In recent years, organizations are opening and extending their data networks to allow partners, suppliers, and customers access to their corporate information in new, dynamic ways for increased collaboration and innovation. As a result, they are at the same time, becoming more and more vulnerable to information misuse and theft (Ahmad et al. 2015; Anderson and Choobineh 2008; Peltier 2010; Webb et al. 2014). Cybersecurity is a broad term that refers to the practice of protecting enterprise assets and digital information from unauthorized access, disclosure, misuse, disruption, modification or destruction (von Solms and van Niekerk 2013). Organizations use a combination of technologies, strategies, and user education to protect their enterprise assets against cybersecurity attacks that can steal data and other valuable company information, compromise systems, and damage an enterprise's reputation. (Lemay et al. 2018) notes that as the severity and volume of cyber-attacks increase, the need for cybersecurity also increases with it. The critical role of cybersecurity in protecting the enterprise assets and functioning of the organisation has been widely acknowledged (Khansa and Liginlal 2009; Shedden, Scheepers, et al. 2011).

In particular, cybersecurity risk management is a continuous process that enables organizations to not only identify risks specific to enterprise assets but also assess the impact and likelihood of a threat occurrence (Shedden et al. 2016; Spears and Barki 2010). Cybersecurity risk management strategy is built on the threat analysis of an enterprise's assets and involves executions of a range of actions taken in defence against cyber-attacks and their consequences and includes implementation of the required countermeasures. Cyber security countermeasures are associated with managing risks, improving system resilience and patching vulnerabilities. The elements and structure of an organisation's cybersecurity risk management strategy and its implementation are based on the estimated threats and risk analyses. In many cases it becomes necessary to prepare several targeted cybersecurity guidelines and strategies for an organisation.

Organizations use the cybersecurity risk assessment process, a subset of the cybersecurity risk management process to (1) identify the enterprise assets that need protection, (2) identify threats that might impact the assets, (3) identify cybersecurity vulnerabilities in the assets that might be exploited, and (4) identify specific risks (scenarios) and estimate their likelihood and potential impact (Shedden, Smith, et al. 2010; Shedden, Scheepers, et al. 2011). Based on the risk assessment, appropriate controls are implemented and then monitored to measure the effectiveness of ISRM process (Shameli-sendi et al. 2016; Shedden et al. 2016). Cybersecurity Risk assessment results are a key input to identify and prioritise specific protective measures, inform long-term investments, allocate resources, and develop strategies and policies to manage cyber security risks to an acceptable level. Humphreys (2008) argues that risk assessment is a complex process and a risk cannot be properly managed unless it is thoroughly understood. Therefore, consolidation of data from disparate cybersecurity source systems is vital for comprehensive cybersecurity risk assessment.

2.5.1. Consolidation of the Data for Cybersecurity Risk Assessment

The key goal of cybersecurity risk assessment is to identify and measure the risks in order to inform the decision-making process. For that, risk assessment process requires data about all the enterprise assets that need protection, threats to which these assets are exposed, system vulnerabilities that threats may exploit and implemented security controls.

2.5.2. Identification of the Enterprise Assets and their Value

The first step in cybersecurity risk assessment process is to identify the enterprise assets that needs protection. Assets are resources and information that have value to an enterprise. The types of organizational value that may be affected if an asset is compromised include monetary, reputation, and opportunity value. Once the asset that needs protection is identified, it must be evaluated (Bojanc and Jerman-Blažič 2013). The valuation of tangible assets is considerably easy as these are measured in money, with depreciation taken into account. Tangible assets include software elements of the information system and physical infrastructure (such as network infrastructure, workstations, and servers) and. Usually, the valuation of intangible assets such as company reputation, organization knowledge, the intellectual property, and business data stored within the enterprise systems is more difficult and complex. Risk assessment complexity increases when organizations need to protect a large number of enterprise assets (Baskerville et al. 2014). Different types of enterprise assets (tangible and intangible) and the different media where these assets reside (digital, physical, and cognitive) also results in an increased risk assessment complexity (Ahmad et al. 2005). Furthermore, distribution of enterprise assets among different targets, such as networks, software, data and physical components increases the threats and thereby complexity (Bojanc and Jerman-Blažič 2008). Finally, complexity also increases when there are different types of data that provide information about enterprise assets (Stoll 2015; Talabis et al. 2014).

When the enterprise assets are evaluated, these are usually classified into discrete classes or categories (Bojanc and Jerman-Blažič 2008; Chew et al. 2008). The categories facilitate the definition of the overall cybersecurity risks and helps organizations to focus on the most critical assets first. Different risk assessment models define a variety of asset categories. While a larger number of categories (for example, 10) is more precise, a smaller number (for example, 3 or 4) of categories reduces the time to debate and select the appropriate category designation (NIST 2011). An example of a three-category risk assessment model is critical, moderate and low-asset category. Examples of critical assets are intellectual property, bank account numbers, and financial data. Typical moderate category assets are purchase order data, internal business information, network designs and information on internal web sites. Example of low-asset category include information on published press releases, publicly accessible web pages, white papers, and product brochures.

2.5.3. Identification of Threats

Threat is another component that adds to risk. The enterprise assets are exposed to threats. Threats are essentially events or entities that can cause an organization harm given the opportunity. To execute cybersecurity strategies and strengthen the level of protection, organizations must clearly identify the threats facing their enterprise assets.

The common threats to enterprise assets are distributed among different targets, such as physical components, software, network, and data. Most current cybersecurity threats can be categorized into the following broad categories:

- Advanced persistent threats
- Insider data theft
- Phishing, spear phishing, and other forms of email-based spoofing and fraud
- Distributed denial of service (DDoS)
- Social engineering and other forms of physiological manipulation
- Zero-day attacks
- Trojan attacks
- SQL injection and other code injection techniques
- Social engineering and other forms of physiological manipulation
- URL redirection or parameter tampering

In particular, the threats caused by humans can be malicious or non-malicious. Some examples of malicious human threats are theft, loss or destruction of an enterprise asset, unauthorized access to the network services, fraud, disclosure of someone's personal data, identity theft, and infection with malicious code. The recent reports on cybersecurity suggest that the number of cybersecurity and privacy incidents is growing. According to the Creasy and Glover (2013), DDoS, ransomware and phishing attacks are the top three types of cybersecurity attacks.

There are different types of threat actors that can do the malicious acts. These may come from a broad set of backgrounds with varying degrees of motivators financial support and can be categorized into one of six categories (Eastman and Versace 2015):

Insider: Often inexperienced but can have higher-level skills; uses opportunities to target known vulnerabilities in systems and policies for self-gain.

Accidental: Generally, an insider such as an employee or a contractor; causes harm accidently because of inexperience.

Hacktivist: External party with higher-level skills that target known vulnerabilities using DDoS attacks or malware as a path to introducing more sophisticated tools into a target system; often has a political or similar motive for action.

Opportunist: An external party who lacks significant experience but uses opportunities to target known vulnerabilities employing worms, viruses, bits, and other tools; often done for bragging rights.

State-level actor: Generally, state-level actors or those who work on behalf of a national government — including industrial espionage — using high-level and sophisticated skills to target strategic or economic information.

Professional criminal: Organized crime efforts including terrorist groups that use high-level and sophisticated skills to target financially relevant information.

The vectors and targets for attacks also continue to evolve with the introduction of new technologies. Though databases and Web sites remain traditional targets, threats and vulnerabilities are seen in several new areas, including attacks on (Eastman and Versace 2015):

- Private, hybrid, or public clouds
- Social media and mobile devices
- Employee-owned devices (bring your own device [BYOD])
- The Internet of Things (IoT) where a wide variety of devices are connected to the Internet

If a cyber-attack on an organization is successful, then economic consequences of its cybersecurity breach are considerable. At present, most financial losses are caused by financial fraud, ransomware, virus (also worms and spyware), phishing attacks and system penetration by an outsider (Creasy and Glover 2013). The impact of a cybersecurity breach is counted as immediate losses and indirect losses. Typical immediate losses may include loss of productivity, loss of revenue, and increased costs (insurance premium, overtime costs etc.). In many situations, actual immediate loss remains a small part of the overall loss of cybersecurity incidents. Usually, the indirect losses appear to be more serious as they have much longer negative impact on the customer base, supplier partners, financial market, banks and business alliance relationships and those costs are almost as high, and sometimes even higher, than the immediate costs caused by the security breach (Bojanc and Jerman-Blažič 2008; Elahi 2013; Garg et al. 2003; Weishäupl et al. 2015b). Indirect losses present damage to the reputation of the organization, interruption of business processes, legal liabilities, loss of intellectual property and damage to customer confidence.

The loss due to a security breach is typically related to the confidentiality, integrity of the data or availability of information assets. Among them, the impact of confidentiality related security breaches is associated with most significant losses in the organization assets value (Bojanc and Jerman-Blažič 2013).

However, according to (Bojanc and Jerman-Blažič 2008) the data about the true cost of a cybersecurity incident are very difficult to find. One of the reasons is that most of the organizations do not systematically track and document cybersecurity incidents. The other reason is that the enterprises deal with the problems internally, fearing a disaster in public relations, a devastating loss of consumer confidence, or worse, revealing vulnerability to other hackers.

Therefore, the propagation of attack vectors and threat actors against an increasing set of target areas has resulted in an exponentially growing level of cybersecurity complexity for the organizations to deal with. The result is that proactive mitigation of these threats with current technologies is almost impossible unless a new approach is applied.

2.5.4. Identification of the Vulnerabilities

Vulnerabilities are essentially the weaknesses that allows threats to exploit an organization. Specifically, vulnerability is a weakness in cybersecurity procedures, technical controls, physical controls or other controls of an asset that a threat may exploit. Most security incidents are caused by vulnerabilities as these enable risk. Threats will always exist, and enterprise assets will innately have value, but vulnerabilities are those that create the inevitable compromise of value. Statistics reveal that the number of vulnerabilities reported has increased dramatically over the years (Creasy and Glover 2013).

Vulnerabilities are typically known as a technical issue however, there are also vulnerabilities caused by human factors. Employees are not necessarily considered a vulnerability, but poor cybersecurity awareness on their part and their resultant behaviour is the vulnerability. If an employee chooses a weak password, the password is the vulnerability. An employee can choose to click on a phishing message or not. The action of the employee can be either a countermeasure or a vulnerability. Poor awareness, a vulnerability, will cause the employee to create a potential loss. Strong awareness, a countermeasure, will cause the employee to report the message, or at least not take a harmful action. Vulnerabilities can be divided into four different categories:

- Operational vulnerabilities: These relate to how organizations do business. For example, excessive information posted on a website is an operational vulnerability. A weak process that allows for someone to change the password on an account is an operational vulnerability.

- Personnel vulnerabilities: These relate to the recruitment, hiring, and termination process. Although these are clearly operational issues in some ways, as organizations rely heavily on the trust they place in their employees, it is something to consider separately. There are also frequently legal and ethical questions that distinguish this category of vulnerabilities.
- Technical vulnerabilities: These relate to a weakness that allows for an attack against computers, networks, and related technologies. These are generally related to how the technology is designed, configured, or maintained. For example, a computer set up to be accessible publicly. There are bugs in commercially available software and in custom-developed software that provide holes to attackers.

2.6. Analysis of Deficiencies in Cybersecurity Risk Management

Once the potential cybersecurity risks have been identified, these must be assessed as to their probability of occurrence and to the potential loss. Cybersecurity assessment is the determination of the potential impact of an individual risk by assessing the likelihood that it will occur and the impact if it should occur. It helps organizations taking decision regarding the necessary investment in security controls and systems in areas that maximizes the business benefit.

There are many different methodologies for assessing cybersecurity risks. These methodologies can be categorized into two broad categories:

- Quantitative risk assessment: This method attempts to assign numeric values to the likelihood and impact of the risk and to the costs and benefits related to the introduction of security controls and systems. The purpose of security control is to mitigate the risk up to a point where the marginal cost of implementing controls is equal to the value of additional savings from security incidents.
- Qualitative risk assessment: This approach attempts to calculate relative values, instead of assigning exact financial values to assets, expected losses, and cost of controls and systems. Qualitative risk analysis is usually conducted through a combination of questionnaires and collaborative workshops.

Both qualitative and quantitative approaches have their advantages and drawbacks. The problem with the quantitative risk analysis is in non-existence of a standard method that will effectively calculate the values of the assets and the cost of the controls and systems required to be applied. The advantage of a qualitative approach is in that the process itself demands less staff and the accurate calculation of the asset value and the cost of control is not required. The drawback of the qualitative approach is in the resulting figures that are usually vague as they are derived as relative values of the assets. Typically, organizations that do not have mature cybersecurity capabilities and have limited resources find the qualitative approach more convenient.

There is considerable evidence in the literature that suggests three trends in the practice of cybersecurity risk assessment (1) organizations conduct cybersecurity risk assessments on occasional (as opposed to continuous) basis (Baskerville et al. 2014; Parker 2007; Webb et al. 2014) and (2) it is considered to be a cost of doing business rather than an integral part of key business processes (Gordon and Loeb 2006; Khansa and Liginlal 2009; Peltier 2010; Rees and Allen 2008) and (3) cybersecurity risk assessments are done on the basis of speculation rather than evidence (Parker 2007; Rees and Allen 2008; Shameli-sendi et al. 2016; Shedden et al. 2016; Webb et al. 2014). This implies that security executives at present do not have holistic security awareness since they are not incorporating important security data into their decision-making process and are therefore unable to make informed security related decisions.

Table 2-4. Concept Matrix: Deficiencies in Cybersecurity Risk Management Process

Citation	Methodology	Deficiencies in Cybersecurity Risk Management		
		Lack of evidence-based decision	Not an integral part of key business processes	Risk assessments not done on
(Gordon and Loeb 2006)	Survey		X	
(Khansa and Liginlal 2009)	Single Case Study		X	
(Peltier 2010)	Multiple Case Studies		X	
(Rees and Allen 2008)	Survey	X	X	
(Shedden, Scheepers, et al. 2011)	Single Case Study	X		
(Webb et al. 2014)	Single Case Study	X	X	X
(Baskerville et al. 2014)	Multiple Case Studies		X	X

Cybersecurity risk management is not a separate entity isolated from other business processes; rather it is an integral part of managing a modern business and helps an organization in achieving and sustaining a competitive advantage over its business rivals (Ahmad, Bosua, et al. 2014; Shedden et al. 2009; Stoll 2015). The traditional cybersecurity strategies to address cybersecurity risks and threats by building bigger walls (antivirus software and firewalls) while still crucial is no longer sufficient. A holistic approach to cybersecurity risk management across the whole organisation including its supply chains, networks and the larger ecosystem is required. Therefore, organisations need to move the cybersecurity risk management process from a mid-level technical function up to the board room and top management where strategic decisions are made.

Furthermore, (Baskerville et al. 2014) note that the objective of the cybersecurity risk management strategy in many organizations is to invest in sophisticated preventive controls aimed at combating known threats, rather than in a sophisticated response process to address unknown complex and evolving threats. The result of using a prevention-centric strategy is that organizations are better equipped to deal with cybersecurity threats that are static and predictable. However, they are more vulnerable to dynamic and unpredictable cybersecurity threats, such as Advanced Persistent Threats (Baskerville et al. 2014).

Baskerville et al. (2014) argue that risk-driven and control-centered security management systems have proven to be quite effective in the static prevention of predictable threats but not very well suited to dynamic response against unpredictable threats such as APTs. Baskerville further argues that in addition to developing a sophisticated response capability, a fundamental strategic shift is required where organizations use both prevention and response modes to their best advantage as part of their cybersecurity risk management strategy. For that, Baskerville et al. (2014) have called for the development of dynamic capabilities in cybersecurity environments that face dynamic and sophisticated attacks.

Even though organizations are paying considerable attention in developing such capabilities, not enough is known about the role that analytics plays in achieving dynamic capabilities. Therefore, this study applies the lens of dynamic capabilities theory to examine how a specialized business analytics capability (in this case real-time analytics capability) may help organizations to develop dynamic capabilities in cybersecurity and thereby improve agility in the process of cybersecurity incident response.

2.7. Cybersecurity Incident Response Process

Cybersecurity IR is a continuous process in which cybersecurity IR teams use a defined process to identify, investigate, respond and learn from potential cybersecurity incidents in a timely and cost-effective manner (Cichonski et al. 2012). This process is crucial for enterprises because they cannot always prevent a breach and therefore a swift incident response to a cybersecurity attack can help them to avoid any financial damage and most importantly, protect their business, reputation and competitive advantage.

In an effort to deal with cybersecurity attacks and data breaches, organisations engage their cybersecurity incident response teams (ad-hoc or dedicated) to detect and eradicate the cyber-attacks (Ahmad et al. 2012; Grispos et al. 2014; Johnson 2013). The primary goal of a cybersecurity incident response team is to minimize the effects of an incident along with managing the organization's return to an acceptable security posture (Ruefle et al. 2014). Cybersecurity incident response teams are the 'firefighters' within enterprises who detect, analyse, respond and recover from cybersecurity incidents (Ruefle et al. 2014). In order to ensure continuity of business operations, incident response is the immediate action that incident response teams execute to deal with cyber-attacks. Therefore, a swift execution of cybersecurity incident response process is crucial and requires variety of qualities in incident response teams such as technical, analytical and communication skills.

Several organizations, such as International Organization for Standardization (Institution 2013) and the National Institute of Standards and Technology (Cichonski et al. 2012), have published guidance on cybersecurity incident investigation and recovery methods. In addition to best practices, academic scholars have also proposed cybersecurity incident processes (Mitropoulos et al. 2006; Ruefle et al. 2014). These cybersecurity incident response approaches centre around a common method, starting from preparatory actions before an incident occurs, the identification and analysis of the incident, followed by its containment which, in turn, allows incident response teams to eradicate, recover and then, potentially, provide feedback information into the preparation stage. Incident response is therefore an organized process to address and manage the results of a cybersecurity incident (Ahmad et al. 2015). The primary goals of incident response process are to rapidly minimize the damage of the attack, the time of recovery from the attack, and to create countermeasures and instructions that would help in preventing such attacks in the future.

A synthesis of the phases of cybersecurity incident response process (Cichonski et al. 2012) is shown in Figure 2-4 and details of each phase within the incident response process are explained below.

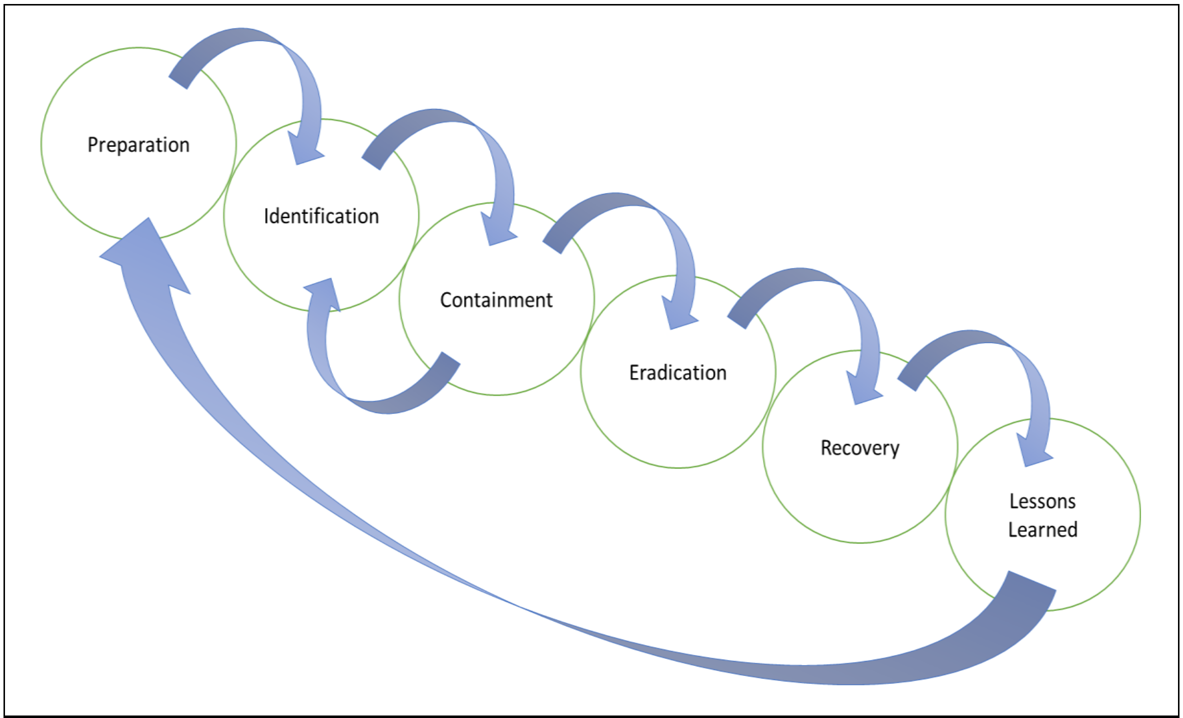


Figure 2-4. Phases of the Cybersecurity Incident Response Process

2.7.1. *Phase 1: Preparation*

Whenever an organization is under a cyber-attack, its cybersecurity incident response team must take rapid and precise actions to respond to it. This requires preparation. In this phase, the cybersecurity team establishes policies and processes and tools that can help prevent, detect and respond to different types of cyber-attacks. Another important task in preparation phase is to train the organization's employees. All employees of the organizations must be familiar with cybersecurity processes and policies so that they know what to do whenever there is a cyber-attack. Lastly, the incident response team that executes the process of incident response builds expertise by continuously gaining knowledge in the incident response field and through constant practice.

2.7.2. *Phase 2: Identification*

In the identification phase, the incident response team determines if the cybersecurity event is actually an incident. For that, incident response team compares the available information regarding the cybersecurity event to the known indicators of compromise (IOC) (Johnson 2013). These indicators help in identification of potentially malicious activities on networks and systems. Some examples of IOC include multiple failed login attempts, unusual network traffic, suspicious system or registry file changes, and the presence of files used by malicious software.

To collect IOC, the incident response team can get information from threat feeds and public reports and perform static and dynamic analysis of malicious software (Johnson 2013). Static analysis is comparatively easy and can be done without launching the software. For example, static analysis can be useful in obtaining web and email addresses used by the software, and hashes of its files. Dynamic analysis is difficult to perform as it requires execution of the software in the protected environment (standalone computer or sandbox). Dynamic analysis helps in understanding the software behaviour and IOC gathering related to it.

The collection of IOC is a cyclic process. After getting the initial information about the cyber-attack, the incident response team creates the detection scenarios. Application of these scenarios enables detection of new IOC that helps to further identify the attack and gather more information about it by doing data analysis, thus creating a cycle. Figure 2-5 below illustrates the cyclic process for collection of indicators of compromise.

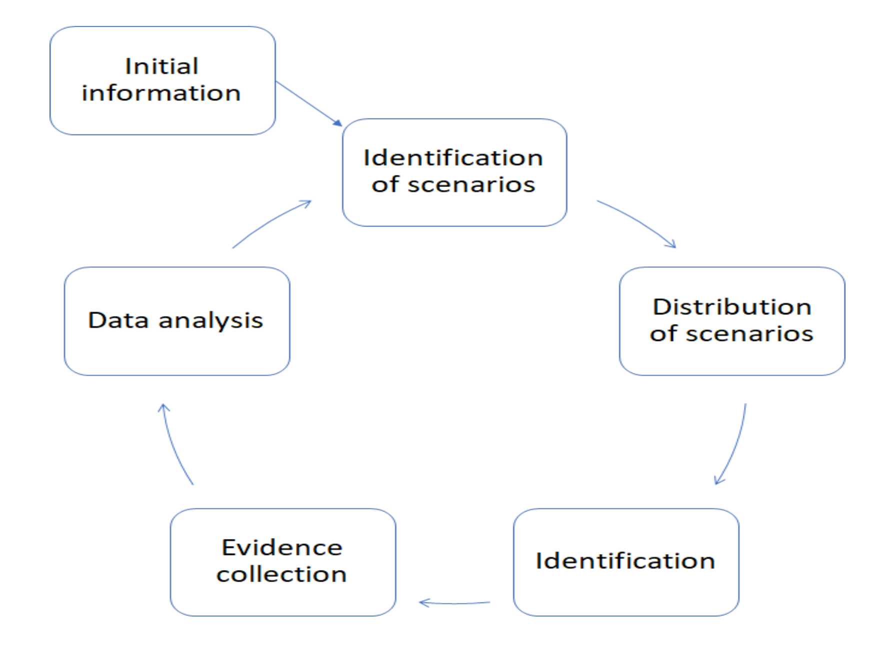


Figure 2-5. Indicators of Compromise Collection Cycle

2.7.3. *Phase 3: Containment*

In containment phase, the cybersecurity incident response team identifies the compromised assets and adjust the cybersecurity policies to prevent further damage. The incident response team also reconfigures the organization's networks to make sure that existing business processes continue to run smoothly while they restore the compromised assets. For example, if one of the servers in the organization's network is compromised by the cyber-attack, the incident response team isolates this server from the network and adjusts the cybersecurity routing policies to distribute the compromised server's load to other servers.

2.7.4. *Phase 4: Eradication*

In the eradication phase, the incident response team restores the compromised assets to their original state. This involves removing the malicious software, restoring the configuration, and removing any artefacts that were left by the malicious software. For example, if a computer is compromised with backdoor software, the incident response team must delete the backdoor software, restore the compromised files and the system registry to the original state, and delete the backdoor software installation files.

2.7.5. *Phase 5: Recovery*

In the recovery phase, the assets and services that were compromised due to the cyber-attack are put back into normal operation. The incident response team needs to monitor the condition of the assets for certain duration of time to make sure that the threat was completely eradicated. For example, if one of the servers in the organization's network is restored, the security team puts it back into the organization's network, adjusts the routing policies to use this server, and monitors the server's behaviour for some time to make sure that there is no further suspicious activity.

2.7.6. *Phase 6: Lessons learned*

In this final phase, the incident response team analyses the cybersecurity incident in detail and develops measures that will help to prevent such incidents in the future and updates the cybersecurity incident response plan for incidents of such kind. The measures may include changing the configuration of the organization's assets, adjusting security policies, and conducting the information security training for organization's employees.

2.8. Analysis of Deficiencies in Cybersecurity Incident Response

As cybersecurity incidents are increasingly rising and impacting organizations, it is imperative that organizations have the ability to investigate, detect, report and, respond to cybersecurity incidents in a rapid and cost-effective manner. The review of cybersecurity incident response literature suggest that the objective of the cybersecurity incident response approaches in many organizations is to invest in sophisticated preventive measures aimed at controlling known risks rather than in an adaptive response process to investigate and combat unknown complex and evolving risks (Baskerville et al. 2014). Recent commercial deliberations also suggest that fundamental problems exist with the application of current approaches in real-world security incident handling context (Creasy and Glover 2013; Eastman and Versace 2015). This is because most of the cybersecurity incident response approaches are structured using a linear plan-driven approach starting from preparation phase that leads to detection of cybersecurity incident. This is followed by containment that permits eradication of the malicious act and finally lessons learned are incorporated into the next preparation stage (Grispos et al. 2014).

Although majority of the literature on cybersecurity incident response has focused on the technical practices for implementing cybersecurity incident response capabilities within organizations, researchers have also discussed and identified several deficiencies in the current organizational practice of cybersecurity incident response approaches. Some of these deficiencies include (1) being too linear, not providing enough insight into the causes of the incident, not maximizing the benefits of digital forensic capabilities and not reflecting the concurrent lifecycle of real-world incident handling (Ahmad et al. 2012; Baskerville et al. 2014; Casey 2005, 2006; Shedden, Scheepers, et al. 2011; Shedden et al. 2016; Tan et al. 2003; Werlinger and Botta 2007).

Table 2-5 summarizes the deficiencies identified in the cybersecurity incident response approaches.

Table 2-5. Concept Matrix: Deficiencies in Cybersecurity Incident Response Process

Citation(s)	Deficiencies in Cybersecurity Incident Response
(Gonzalez 2005; Werlinger and Botta 2007)	The traditional linear-plan driven approaches for incident response have become outdated and do not support in the development of highly efficient capability that is required to manage and handle modern cybersecurity attacks.
(Werlinger et al. 2010; Werlinger and Botta 2007)	There is a progression flaw in linear processes, if one phase in the linear process is not completed, the entire process cycle may stop midstream.
(Ahmad et al. 2012; Tan et al. 2003)	Important steps are often skipped because the incident response process is too focused on containment, eradication, and recovery.

Table 2-5. Concept Matrix: Deficiencies in Cybersecurity Incident Response Process

Citation(s)	Deficiencies in Cybersecurity Incident Response
(Ahmad et al. 2012; Jaatun et al. 2009; Shedden, Scheepers, et al. 2011; Shedden et al. 2016)	Current approaches do not provide enough insight into the underlying causes of the cybersecurity incident.
(Tan et al. 2003)	Poor provisions for incident planning.
(Casey 2005, 2006)	Do not maximize the benefits of digital forensic capabilities.
(Casey 2006; Tan et al. 2003)	Undermine the value of forensic evidence possibly required for subsequent legal action.
Baskerville et al. (2014)	The objective of the incident response strategy, in many organizations, is to invest in sophisticated preventive controls aimed at combating known threats, rather than in a sophisticated response process to address unknown complex and evolving threats.

(Werlinger et al. 2010) explored the cybersecurity incident response activities of practitioners across various organizations and industries and particularly focused on the socio-technical aspects of incident response. (Werlinger and Botta 2007) examined what tools were used in the cybersecurity incident response process and how these tools could be improved. (Werlinger et al. 2010) reported that the current incident response tools and guidelines do not sufficiently support the highly collaborative nature of incident response investigations. Furthermore, the incident response teams often need to develop their own solutions to perform specific exploratory tasks.

Werlinger and Botta (2007) noted that the traditional linear-plan driven approaches for incident response have become outdated and do not support in the development of highly efficient capability that is required to manage and handle modern cybersecurity attacks. (Gonzalez 2005) argued that although organizations do implement the traditional linear-plan driven approaches, they do not follow it efficiently and effectively. Furthermore, there is a progression flaw in linear-plan driven processes. If one phase in the linear-plan driven model is not completed, the entire process cycle may stop midstream (Gonzalez 2005).

Gonzalez (2005) notes that due to advancement in the technologies, there has been a shift in the way cybersecurity incidents are impacting organizations and, as a result, the rapid and precise detection and resolution of cybersecurity incidents is a critical capability for many organizations. The key reason for this shift is that attackers are now using sophisticated and automated tools and methods to extend cyber-attacks. Accordingly, the unavailability of vital enterprise systems can result in severe damages such as financial and reputational loss and loss of sensitive information (Gonzalez 2005).

A number of articles focused on the problems with the current cybersecurity incident response methods in reference to learning from incidents (Ahmad et al. 2012; Shedden, Ahmad, et al. 2010, 2011). Ahmad et al. (2012) used the case study method to examine the shortcomings in the practice of incident response in an organization. (Ahmad et al. 2012) argued that the incident response process is too focused on containment, eradication, and recovery and therefore that key steps such as lessons learned, are often skipped. They further noted that, even though the organization in their study closely followed industry best practices, the organization's inclination was to focus on maintaining business continuity along with improving the technical aspects of security incidents. Ahmad et al. (2012) highlighted the fact that the organization neglected to engage any post-incident learning activities.

Similarly, Shedden et al. (2011) argued that the practice of incident response in many organizations is highly informal and therefore, the learning from cybersecurity incidents should also be informal. For that, they proposed the "Informal and Incidental Learning Model" to encourage security incident learning within organizations. Likewise, Jaatun et al. (2009) proposed the Incident Response Management (IRMA) method that particularly focused on proactive preparation and reactive learning. Jaatun et al. (2009) proposed learning phase of IRMA focuses on learning from an incident by identifying sequences of events using the Sequential Timed Events Plotting (STEP) method. However, the model developed by Jaatun et al. (2009) was specifically designed to investigate and handle cybersecurity incidents in the petroleum industry.

Tan et al. (2003) examined the factors which influenced cybersecurity managers to not conduct security incident investigations. These factors included a highly regulated industry which penalizes organizations for security incidents, a lack of prior planning and industrial emphasis on system recovery as opposed to performing an incident investigation (Tan et al. 2003). In addition, Tan et al. (2003) noted that the organization, in their case study, was not able to identify how the cyber-attack took place, unaware of the benefits associated with prosecuting offenders related to security incidents. They also did not have a clear definition for a cybersecurity incident.

Casey (2005) argued that closer collaboration is required between security forensic examiners, system administrators, and cybersecurity incident handlers, so that all relevant stakeholders understand the need to report even seemingly minor security incidents. Casey (2005) noted that even with a moderate amount of forensic preparation, an organization can mitigate the impact of an incident. Casey (2006) stated that in corporate environments forensic investigation can be challenging. The reason is very few logging systems are designed with evidentiary value in mind and that requires forensic specialists to apply the principles of evidence preservation creatively to each source of log data that an organization maintains (Casey 2006).

Casey (2006) noted that implementation of digital forensic practices is evolving from merely a customary role in law enforcement to a more comprehensive resolution for organizations to investigate prohibited acts. However, researchers have indicated that organizations may not be maximizing corporate forensic capabilities along with undermining the value of forensic evidence, potentially, required for subsequent legal action (Casey 2005; Tan et al. 2003). Nnoli et al. (2012) argued that a lack of forensic readiness could result in organizations wasting financial resources, effort and time when conducting forensic investigations. The proper collection of forensic evidence can potentially benefit organizations through faster incident resolution, legal defence support, demonstration of due diligence and verification of commercial transactions (Nnoli et al. 2012).

Baskerville et al. (2014) argued that the objective of the cybersecurity strategy in many organizations is to invest in sophisticated preventive measures aimed at controlling known risks rather than in an adaptive response process to investigate and combat unknown complex and evolving risks (Baskerville et al. 2014). The result of organizations basing themselves in the prevention paradigm is that they tend to be better equipped to deal with cybersecurity threats that are static and predictable, and are more vulnerable to dynamic and unpredictable cybersecurity threats such as APTs (Baskerville et al. 2014; Jalali et al. 2018). To address the full range of threats, a fundamental shift is required where organizations use both the prevention and response paradigms to their best advantage.

Baskerville et al. (2014) highlighted agility as a key characteristic of the incident response capability in the response paradigm. In addition, agility or business process agility in general is also receiving a lot of attention from both academics and practitioners in recent times (Chen et al. 2013; Park et al. 2017). Even though organizations are paying increasing attention in improving agility in their cybersecurity incident response, not enough is known about how agility can be improved in incident response process (Grispos et al. 2014). Therefore, this study applies the lens of dynamic capabilities theory to examine how a specialized business analytics capability (in this case real-time analytics) may help organizations to develop dynamic capabilities in cybersecurity and thereby improve agility in the process of cybersecurity incident response.

2.9. Summary

This chapter presented the results of literature review of multiple information systems domains including business analytics, dynamic capabilities, business process agility and cybersecurity incident response following the methodology proposed by Webster and Watson (2002). The results that emerged from the analysis of literature, were presented in this chapter organized by the guiding frameworks and concept matrices (Webster and Watson 2002). Dynamic capabilities theory was used to integrate and synthesize the literature conceptually. Dynamic capabilities theory was also used as a useful high-level theoretical lens for understanding how it can help organization to improve business process agility and in this study cybersecurity incident response agility. The literature on the process of cybersecurity risk management and incident response was analysed to identify the deficiencies in these processes. Finally, the real-time analytics capability was introduced as a specialized business analytics capability that can help organization to develop dynamic capabilities in their incident response and thereby improve agility in their cybersecurity incident response process. The next chapter provides a detailed description of the research design and methodology used in this study.

3

"Research is to see what everybody else has seen and to think what nobody else has thought."

Albert Szent-Gyorgyi (1893 - 1986)

CHAPTER 3. RESEARCH METHODOLOGY

The purpose of this chapter is to describe and explain the research methodology of this study. The first section of this chapter explains and justifies the research method used to answer this study's overarching research question (*How can organizations improve agility in their cybersecurity incident response process using real-time analytics?).* This study aims to investigate how enterprises improve their cybersecurity incident response process agility using real-time analytics. Based on the aims of this study and dynamic nature of the cybersecurity environment, an exploratory field study using multiple case study design is conducted to answer the aforementioned research question. In section 3.2, the research context is explained in detail and the logic behind selection of three large financial organizations as multiple-case study sites is discussed. In section 3.3, background information on the studied organizations is given. In sections 3.4 and 3.5, an overview of data collection and analysis process is described. In section 3.6, the four stages of the data analysis process undertaken to systematically move from raw data to theoretical interpretations following the methodology in Gioia et al. (2013) are explained. The evaluation of the methodological rigor of this study's research method is provided in section 3.7.

3.1. Research Method

The aim of this study is to explore how organizations improve agility in their cybersecurity incident response process by developing dynamic capabilities using real-time analytics. To answer this research question, a field study using a multiple case study design is conducted (Eisenhardt and Graebner 2007; Yin 2017). The units of analysis are individual organizations that use real-time analytics in their cybersecurity incident response process to detect and respond to different types of cybersecurity threats. Given the highly dynamic cyber threat environment context, it is necessary to be open to unexpected and new findings in the fieldwork, therefore this research followed an inductive and exploratory multiple-case study research method.

Despite the growing literature on BA, there is a lack of systematic framework to understand how real-time analytics may help organizations to improve incident response agility through the development of dynamic capabilities, and this motivates the choice of this study's research methodology to inductively develop a framework (Eisenhardt 1989; Gioia et al. 2013). Qualitative methods can help in gaining insights into the complexity involved in using real-time analytics to achieve dynamic capabilities in cybersecurity incident response, and also facilitate the development of richer and more informative conclusions (Alavi and Carlson 1992; Trauth 2001).

Yin (2017) defines a case study as "an empirical enquiry that investigates a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are clearly evident … and it relies on multiple sources of evidence" (p. 13). Empirical investigation of real-time analytics-enabled dynamic capabilities aligns well with this view. Case study research is useful when a phenomenon is broad and complex, cannot be studied outside the context in which it occurs and requires a holistic, in-depth investigation without explicit control or manipulation of variables (Darke et al. 1998; Paré 2004). Another critical reason for selecting case study as a research method is the nature of the question that is being investigated. Case studies are best suited for investigating 'how' questions (George, Alexander and Bennet 2005; Yin 2017) and thus, in this instance, the investigation of how real-time analytics-enabled dynamic capabilities improve cybersecurity incident response agility is consistent with these definitions of the case study method.

This qualitative study follows the interpretivist tradition that is similar to the method used by (Smith 2014). Yin (2017) categorizes case studies into three types: descriptive, exploratory and explanatory case studies. The reason to use a descriptive case study is to present a complete description of a phenomenon within its context; an exploratory case study is used to define the hypotheses and questions of a subsequent study or to determine the feasibility of the desired research procedures (theory building); and the purpose of an explanatory case study is to test the causal relationships in the hypotheses (theory testing). Given the nascent nature of the research goal, this study is exploratory in that it focuses on inductive theory building and uses a multi-case study methodology based on the case study protocols and guidelines specified in Yin (2017) and Gioia et al. (2013). This study considers each case as a distinct analytical unit and builds theory from the case studies by recursive cycling among the case data, emerging theory, and extant literature following the replication logic (Eisenhardt and Graebner 2007). This research follows the steps that Gioia et al. (2013) outlines for building a theory which is grounded in the data collected.

Eisenhardt (1989)) and (Dube and Paré (2003, p. 605) note that exploratory case studies may be aimed at 'defining questions, proposing new constructs, and/or building new theories'. As no existing theory could sufficiently answer this study's research question, therefore this research did not start with any specific hypotheses that could be tested. In fact, according to Eisenhardt and Graebner(2007), such a method is very appropriate for an exploratory research such as mine.

According to Gioia et al. (2013), during an inductive theory building process 'existing ideas or theories' may be used to explain some of the findings. This study subscribes to Gioia et al. (2013) view that using elements of existing theory might be of significant help in examining 'not only all the major emergent concepts, themes, and dimensions, but also in explaining their dynamic interrelationships'. Therefore, this study uses seed concepts from the literature on dynamic capabilities theory and business process agility, which provide the theoretical framing that is necessary for developing an understanding of how organizations improve cybersecurity incident response agility by developing dynamic capabilities using real-time analytics. Although, dynamic capabilities theory is used as the sensitizing tool, this study infers its claims and findings from, and grounded them in, the empirical data.

3.2. Research Context and Case Selection

In this research, the theoretical sampling (Patton 2015) is used to select the organizations where latest and most sophisticated cybersecurity and BA solutions (such as security information and event management (SIEM), complex event processing systems, and reporting and analysis tools), are employed to support and improve cybersecurity incident response decision making process. A field study with a multiple-case study design (de Corbiere and Rowe 2013) is conducted because it can enhance the generalizability of the findings (Yin 2017). Multiple cases, adequately sampled and carefully analysed, can enhance the relevance or applicability of this study's findings. In addition, a multiple case study can enhance our understanding and explanation of a focal issue (Yin 2017).

Specifically, this research sought participants who possess a wide repertoire of in-depth knowledge and experiences in using real-time analytics in cybersecurity incident response process. Twenty-six different participants drawn from three large financial organizations participated in the study. All the case organizations are recognized as successful financial companies with a high-market share, each employing more than 15,000 employees.

The selection of multiple-case study sites was driven by purposeful, theoretical sampling (Gioia et al. 2013; Yin 2017), that is, the potential to investigate the use of real-time analytics in achieving dynamic capabilities and their role in improving cybersecurity incident response agility. The sites offered a theoretically relevant organizational context because many of them were pioneering the use of real-time analytics in innovative ways. Specifically, financial sector organizations were selected that were facing a dynamic environment in which the cyber threat landscape changes rapidly and had reported and developed a business intelligence and analytics capability in their cybersecurity incident response process. In addition, all the organizations were at high levels of maturity in their cybersecurity incident response process and also in their practice of business intelligence and analytics. The unit of analysis for the case study was chosen to be 'cybersecurity incident response teams' as they are the first line of defence against cyber-attacks and their primary responsibility is to identify, investigate, respond and learn from potential cybersecurity incidents in a timely and cost-effective manner.

In all the three sites, an access to the incident response teams was provided, which included strategic top-level managers, middle level senior managers, cybersecurity analysts and data analysts. Participants who had rich learning experiences pertaining to the use of real-time analytics in cybersecurity incident response were identified as subjects for this study. The selection of this study's multiple-case study sites is consistent with the notion of 'information-oriented selection' to maximize the utility of information from a small sample (Battleson et al. 2016).

Selecting participants at various levels within each organization helped to triangulate the insights from different sources, replicate findings, and thereby strengthening the potential for generalizability (Darke et al. 1998; Eisenhardt 1989; Eisenhardt and Graebner 2007; Gioia et al. 2013; Yin 2017). However, the primary rationale underlying selection of the study sites was their potential to provide a rich context to understand and develop insights into the use of real-time analytics to improve cybersecurity incident response agility by developing dynamic capabilities rather than them serving as representative organizations from which to generalize the findings.

Table 3-1 below provides the profiles of the participating organizations. To ensure the confidentiality of the case participants, this research uses FinBank, FinInsuranceA, and FinInsuranceB to label the three organizations.

Table 3-1. The Profiles of Case Firms

ID	Organization type	Number of employees	Annual revenue (billion AUD)	Cybersecurity strategy includes
FinBank	Bank	50,000+	> 20	SOC, SIEM, Custom built Security Analytics Solution
FinInsuranceA	Insurance	15,000+	>10	SOC, SIEM, Managed Security Services Provider
FinInsuranceB	Insurance	35,000+	>15	SOC, SIEM

- Security operations centre (SOC)
- Security information and event management (SIEM)

3.3. Case Study Backgrounds

As outlined in the methodology, for the case study, three organizations from financial sector i.e. FinBank, FinInsuranceA and FinInsuranceB, were selected to explore their use of real-time analytics in the cybersecurity incident response process. While FinBank is far ahead in terms of practicing business intelligence and analytics and becoming a completely data-driven decision-making organization, FinInsuranceA and FinInsuranceB are relatively late entrants into the implementation of integrated enterprise systems and are still in the process of fully becoming data-driven decision-making organizations. Furthermore, since FinBank was already using analytical systems for several years to practice evidence-based decision making when the study was conducted, it was able to provide insights on the capabilities that they developed in their cybersecurity incident response process by using real-time analytics over time and their impact on enterprise security performance. In case of FinInsuranceA and FinInsuranceB, which had deployed BA for fewer years and were in the ongoing process of deploying real-time analytics systems when the study was conducted, they were able to provide insights on developing new capabilities using real-time analytics capability in cybersecurity incident response process and how they are impacting their enterprise security performance.

3.3.1. Case Study Site 1 - FinBank

FinBank is one of the largest financial companies in Australia and a major international banking and financial services group that is among the top 50 banks in the world. FinBank recognises the importance of effective decision-making to its business success and established a dedicated analytics team ten years ago working collaboratively with the business functions. The top-level management is committed to achieving strong control, and a distinctive analytical and cybersecurity incident response capability that enables FinBank divisions and business units to perform their daily operations securely and meet their performance objectives efficiently.

At FinBank, the reason for integrating analytical practices into the cybersecurity function was to nurture a data-driven decision-making culture in cybersecurity management. FinBank's cybersecurity strategy includes SOC, SIEM systems and a custom-built security analytics solution that helps to generate insights based on security data and take informed actions. FinBank uses analytics in all the phases of their cybersecurity incident response process including preparation, response and follow-up. Some examples where FinBank's cybersecurity incident response team uses real-time analytics includes (a) access management (e.g. in blocking and logging of unauthorised access); (b) forensic analysis (e.g. analysing network data to monitor network activity in real-time.); and (c) analysis of logs (e.g. service and application logs, operating system logs, network device logs and network flows).

3.3.2. Case Study Site 2 – FinInsuranceA

FinInsuranceA is a multinational insurance company headquartered in Sydney, Australia. FinInsuranceA is recognized as a successful financial company with a high-market share, employing more than 15,000 employees. FinInsuranceA implemented its corporate data warehouse eight years ago that integrates and correlates data from multiple data sources such as customer relationship management systems, sales systems and claim management systems. The data from these sources are used to produce reports and dashboards to analyse the effectiveness and the performance of supporting business processes. However, since 2014, FinInsuranceA has been investing in building a data-driven decision-making capability within cybersecurity functions using the latest data analytics platforms.

FinInsuranceA has a dedicated SOC and analytics team that is building their security analytics capability. FinInsuranceA's cybersecurity strategy includes SOC, SIEM and managed security service provider. FinInsuranceA uses analytics in all phases of the cybersecurity incident response process including preparation, response and follow-up. Some examples where FinInsuranceA's cybersecurity incident response team uses real-time analytics include (a) Security logs analysis to correlate security events; (b) access management (e.g. managing access across all of its systems and assets in real-time); and (c) malware analysis.

3.3.3. Case Study Site 3 – FinInsuranceB

FinInsuranceB is a multinational financial services company headquartered in the USA and has many financial services branches in Australia. FinInsuranceB is also recognized as a successful financial company with high-market share, employing more than 35,000 employees. In Australia, FinInsuranceB has a cybersecurity division that supports multiple business domains with a dedicated SOC and analytics team and collaboratively works with the business functions. The cybersecurity division was established six years ago primarily to address the insider threat and data leakage issues of the organization.

FinInsuranceB's cybersecurity strategy includes a combination of SOC and SIEM systems. FinInsuranceB analytics team is building their security analytics capability and delivers insights to security executives so that they can make data-driven informed actions related to cybersecurity. FinInsuranceB also uses analytics in all phases of cybersecurity incident response process including preparation, response and follow-up. Some examples where FinInsuranceB's cybersecurity incident response team uses real-time analytics include (a) insider threat detection; (b) employee activity monitoring; and (c) analysis and monitoring emerging cyber threats.

3.4. Data Collection

Since this research involved human participants, ethics approval was required prior to data collection. For studies conducted in the School of Computing and Information Systems at the University of Melbourne, researchers must seek ethics approval from the Human Ethics Advisory Group (HEAG) before the research is undertaken. An ethics application was submitted (ID 1646735.1) and approved for this study. The research reported in this thesis was then conducted within the ethics guidelines of the HEAG.

The data were collected from the aforementioned cases over the course of a year starting in July 2016 and ending in June 2017. Data were collected by conducting interviews. Relevant background information documents (including strategic progress reports, organizational charts, PowerPoint presentations and meeting agendas) were also made available depending on request and served as a complementary material to the interview data.

In addition, information from the organizations websites and industry analyses reports was also extracted which allowed the researcher to triangulate the understanding of each organization's cybersecurity incident response unit context, strategy, practices and outcomes. In total, 26 interviews were conducted across the three case organizations. To triangulate insights from different sources, participants at various levels in the cybersecurity unit were interviewed (see Table 3-2), including (1) the strategic top-level managers, (2) the middle-level senior managers, (3) cybersecurity analysts, and (4) data analysts working with cybersecurity incident response unit (Eisenhardt 1989).

Data collection and analysis were conducted progressively in an iterative fashion. This study also used snowball sampling in that it initially identified key contact persons (strategic top-level managers) in the organizations. These top-level managers were first interviewed, and the research objectives were discussed with them. They identified the additional participants for this study. The participants were selected according to the criteria that they all had experience in both cybersecurity and analytics domains and had sufficient knowledge to provide insights on behalf of the organization they represented. Most of the interviews for this study lasted about an hour, however some of them lasted up to two hours.

An interview guide (see Appendix A) was developed based on the concepts of real-time analytics, cybersecurity incident response, cybersecurity risk management, and corresponding literature on dynamic capabilities, together with several open-ended questions about business analytics and security performance in general. Five pilot interviews were also conducted to refine the interview guide. The form of the interviews was semi-structured, a guided conversation to elicit reflective thoughts from the interviewee.

The interviews started with demographic and open-ended questions to understand the organizational context and was followed by questions focusing on the use of real-time analytics in cybersecurity incident response process. All the interviews were recorded and transcribed with the consent of the participants. The interviews followed case study protocol. All the interviews were aimed at understanding the key features of real-time analytics capability in cybersecurity incident response process, the role that real-time analytics enabled capabilities play in improving cybersecurity incident response agility and their impact on enterprise security performance.

The participants were asked to give specific examples in order to gain a better understanding of what was being said. At the end of the interviews, the participants were also asked for further reflections on the examples given. In addition, extensive notes were made during all these interviews for reference during data analyses. Data collection and analysis were undertaken until 'theoretical saturation' (Eisenhardt 1989) was reached, wherein further data provided no new insights. The details about the participants of this research is summarized in Table 3-2.

Table 3-2. Summary of Details About the Informants

Firm	Description of interviewees	Number of Interviewees
FinBank	• Top-level managers: General manager of cybersecurity risk management, General manager of data and analytics • Middle-level managers: Cybersecurity senior managers (2), Head of cybersecurity incident response team (CSIRT), • Cybersecurity analysts: Senior cybersecurity analysts (3) • Data analysts (2)	11
FinInsuranceA	• Top-level managers: General manager of cybersecurity strategy and governance, • Middle-level managers: Manager of IT and information security, Manager of cybersecurity strategy and governance, Manager of cyber defence centre, Head of cyber threat detection and response team • Cybersecurity analysts: Senior IT risk partners (2) • Data analysts (2)	9
FinInsuranceB	• Top-level managers: Director of global cyber forensics, Chief security architect • Middle-level managers: Head of global insider threat detection, Senior managers of cybersecurity incident response team (3)	6
Total number of interviews		26
Average experience of respondents in cybersecurity		21 years
Average experience of respondents in business analytics		15 years

Follow-up discussions were done with the participants to seek clarifications and obtain additional insights. This research presents evidence through quotes in Chapter 4 to explain the findings derived from the qualitative data analysis collected in accordance with recommended practices in qualitative research studies (Gioia et al. 2013). Each quote presented in this study also identifies the organization and the role of the respondent (see Table 3-2).

3.5. Overview of Data Analysis Procedure

In this study, the guidelines proposed in Gioia et al. (2013) are followed to seek qualitative rigor and systematically transfer raw data into theoretical interpretations. Although this study is necessarily presented in a linear structure, the process of data analysis was iterative to improve insights and generalizability (Langley 1999; Locke et al. 2008; Yin 2017).

The data analysis process started by reviewing the background materials and interview transcripts, together with the field notes that were taken to record the impressions at the time of each interview. In particular, the goal was to look specifically for indicators of how cybersecurity incident response teams were using real-time analytics in their everyday practices. It is use of real-time analytics in cybersecurity incident response process that constitutes this study's primary unit of analysis. This study employed constant comparative techniques and the combination of open, axial and selective coding (Strauss and Corbin 2014) for analysing interview data. Analysis of the data was an iterative process starting from coding the raw data (See Figure 3-1 for an overview of the different steps followed during data analysis).

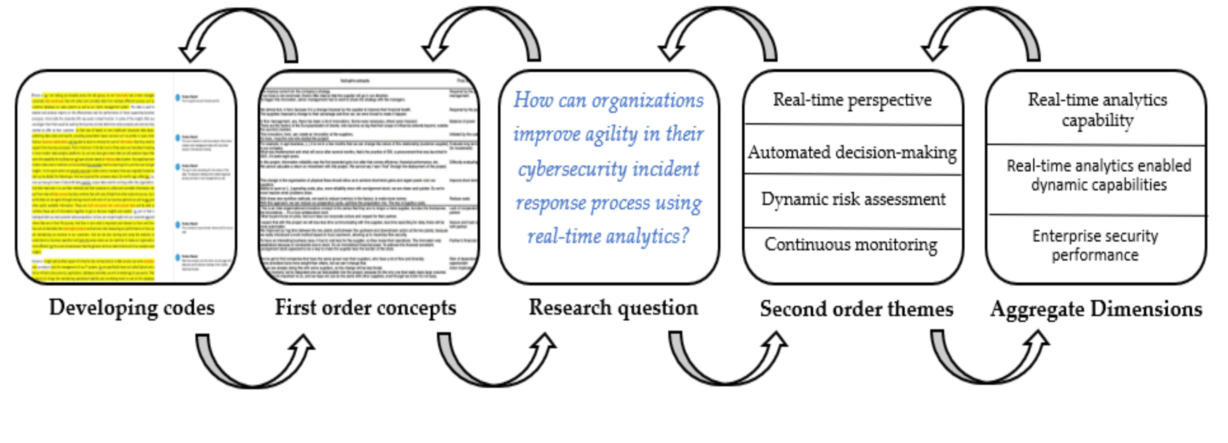

How can organizations improve agility in their cybersecurity incident response process using real-time analytics?
Real-time perspective
Automated decision-making
Dynamic risk assessment
Continuous monitoring
Real-time analytics capability
Real-time analytics enabled dynamic capabilities
Enterprise security performance
Developing codes
First order concepts
Research question
Second order themes
Aggregate Dimensions

Figure 3-1. Overview of Steps Followed During Data Analysis

The codes captured concepts such as 'analysis on demand', 'self-service analytics' and 'cyber kill chain'. These codes were assigned to words, sentences or even paragraphs in the margins of the interview transcripts. Overall, this study captured 350 codes relevant to describe the role of real-time analytics in improving cybersecurity incident response agility. These codes were organized into data tables in Excel spreadsheets that supported a topic or a single theme across data sources (Smith 2014). Every new relevant statement was listed under its appropriate code. The process of coding the interview data continued until it was not possible to discover any more distinct, shared patterns among the data. In this way, theoretical saturation was accomplished (Suddaby 2006). During the next phase of the analysis, codes that were recognised as similar were collated into the same first order concepts, using informant terms whenever possible (Gioia et al. 2013; Strauss and Corbin 2014). In parallel with the development of the first order concepts, linkages among the categories started to surface and become evident. These linkages were the seeds that initiated the development of second-order themes.

The data was further sorted and analysed by developing second order themes, using this study's main research question to go through the first order concepts. During this phase, the first order concepts were examined using existing theories and looked for all possible explanations for the observed data. The data and first order concepts were analysed by looking for linkages or overlap among first order concepts to assemble these into higher order themes. The process of developing the higher second order themes involved many iterative cycles. During these cycles, the first order concepts were merged, revised and sometimes abandoned in order to reach a higher level of abstraction and to arrive at fifteen second-order themes (Gioia et al. 2013). During the final phase, the data was further analysed by investigating whether it is possible to aggregate the concepts identified in second order themes to form higher-level more abstract concepts (dimensions). By doing so, the fifteen second-order themes were combined into five aggregate dimensions that captured the overarching concepts relevant for understanding the role of real-time analytics in improving cybersecurity incident response agility.

3.6. Data Analysis

In this section, the four stages of data analysis that the researcher went through to systematically move from raw data to theoretical interpretations are explained in detail (Gioia et al. 2013). Analytical methods proposed in (Eisenhardt 1989; Yin 2017) were adopted to generate insights within each case and then compared these insights across all the cases. Even as each stage is described, the whole process was iterative to improve insights and generalizability. The stages of the analytics process are summarized in Table 3-3.

Stage 1: Develop thick descriptions.

A rich case study for each cybersecurity incident response unit within the three case organizations was developed that incorporated various types of data to describe the organizational context, real-time analytics capabilities, incident response strategies and the impact of using real-time analytics in the

Table 3-3. Data Analysis: Stages of Analytical Process

Stage	Analytical Activities	Output
1. Develop thick descriptions to generate initial insights	1. Generate thick descriptions of each case 2. Share descriptions with informants to increase comprehensiveness and reliability	• Three thick case studies, one for each cybersecurity incident response unit of case organizations
2. Identify higher-order real-time analytics enabled dynamic capabilities	1. Generate a list of capabilities that exhibit the characteristic of being dynamic and agile 2. Code dynamic capabilities using short phrases or in vivo codes 3. Cluster and incorporate literature to identify real-time analytics enabled dynamic capabilities 4. Return to raw data to confirm all instances of identified capabilities 5. Identify language and terms that informants use to describe their understanding of real-time analytics enabled dynamic capabilities	• 5 higher-order capabilities that exhibit the characteristics of being dynamic and agile • Three themes describing emergent real-time analytics enabled dynamic capabilities
3. (a) Identify incident response strategies to different types of cybersecurity threats	1. Code data to identify incident response strategies to different types of threats 2. Cluster codes into meaningful groups (three dynamic incident response strategies) 3. Check coding reliability with external researchers 4. Integrate existing literature to aggregate into dimensions	• Three incident response strategies aggregated into dimension of dynamic incident response strategies
(b) Identify factors that foster and hinder the development of dynamic capabilities	1. Code data to identify factors that facilitate and hinder the development of dynamic capabilities. 2. Cluster facilitating factors into two groups (a) incident response and (b) analytical capability	• Two themes of facilitating factors and one theme of challenging factors aggregated into dimension of supporting and challenging factors
(c) Examine the impact of dynamic capabilities on enterprise security performance	1. Code data to identify how real-time analytics capabilities impact enterprise security performance 2. Classify improvement in terms of strategic and economic benefits.	• Two types of benefits (1) strategic, and (2) economic aggregated into dimension of enterprise security performance
4. Integrate literature with data to build a theoretical model	1. Combine data on real-time analytics capability, real-time analytics enabled dynamic capabilities, dynamic cybersecurity incident response strategies to describe their impact on enterprise security performance 2. Incorporate existing literature to inform an overall model of dynamic cybersecurity incident response to improve incident response agility	• A model of dynamic cybersecurity incident response to improve incident response agility

cybersecurity incident response process on overall enterprise performance (Langley 1999). The case writing was combined with data collection, allowing questions and insights from the case studies to guide future data collection. The insights gleaned from the cases were shared with key participants to assess comprehensiveness and reliability.

Three crucial insights emerged from the case studies that guided subsequent analyses. First, senior managers explained what they mean by real-time analytics and then identified the key features of their real-time analytics capability in the context of cybersecurity incident response. They described real-time analytics concept using various perspectives and mentioned automated decision making, continuous and on-demand data analysis as key features of real-time analytics. This insight led me to focus on specific higher-order capabilities that are enabled by real-time analytics in cybersecurity incident response process as primary unit of analysis.

Second, higher-order capabilities enabled by real-time analytics in the cybersecurity incident response process are developed over time. Analysis of in-depth data over the duration of a year enabled me to generate novel insights into the patterns of real-time analytics usage in cybersecurity incident response in each case. Furthermore, comparison of three distinct case studies surfaced differential patterns of real-time analytics usage in cybersecurity incident response. As cybersecurity incident response teams utilize real-time analytics capabilities in incident response process, new capabilities emerge. Informants described enhanced security awareness and real-time access to cyber threat intelligence feeds as the emergent capabilities. This insight guided the researcher to focus on the role these emergent capabilities played in shaping cybersecurity incident response strategies.

Finally, early insights suggested four different cybersecurity incident response strategies including defence-in-depth, deception, monitoring, and reconnaissance that organizations used to respond to different types of cybersecurity threats. In addition, the participants also explained the factors that foster and hinder the development of higher-order real-time analytics enabled capabilities and execution of cybersecurity incident response strategies.

The aforementioned insights guided the future analyses, in which the raw data was coded systematically to develop theoretical constructs (Gioia et al. 2013) and ultimately to analyse the role of real-time analytics enabled dynamic capabilities in improving incident response agility and their impact on overall enterprise security performance.

Stage 2: Identify higher-order real-time analytics enabled dynamic capabilities.

In this stage, specific higher-order real-time analytics enabled dynamic capabilities in the process of cybersecurity incident response were identified. To do so, a list of capabilities that emerged as a result of using real-time analytics capabilities in cybersecurity incident response over time was generated. The capabilities that exhibited the characteristic of being dynamic (capacity to renew incident response competences so as to achieve congruence with a changing cyber threat environment in which innovative responses are needed) and enabled agile features in cybersecurity incident response process such as innovation, swiftness and flexibility were included.

Real-time analytics enabled dynamic capabilities were coded using short descriptions or in vivo codes. The researcher returned to each case to ensure that all the emergent capabilities were captured. Thematic grouping and incorporation of existing literature resulted in five higher-order capabilities which were clustered into three emergent dynamic capabilities including real-time situational awareness, cyber threat intelligence generation and dynamic risk assessment.

Stage 3: Identify dynamic incident response strategies, factors that foster and hinder the development of dynamic capabilities and their impact on enterprise security performance.

To further investigate this study's research question, how enterprises improve agility in their cybersecurity incident response process using real-time analytics, the researcher read through the raw data, asking: How does the use of real-time analytics capabilities in cybersecurity incident response process impact enterprise security performance?

Three types of codes emerged:

(1) dynamic cybersecurity incident response strategies to address different types of cybersecurity threats;

(2) factors that foster and hinder the development dynamic capabilities; and

(3) the impact of these capabilities on enterprise security performance.

To code for dynamic incident response strategies to respond to different types of cybersecurity threats, the researcher read through the raw data and created short phrases for related key passages, which were then clustered to meaningful groups. This process resulted in three themes describing dynamic cybersecurity incident response strategies that studied organizations used to respond to both predictable and unpredictable cybersecurity threats. Three types of dynamic incident response strategies that emerged from data include active defence, continuous monitoring, and active reconnaissance. These themes were shared with two researchers not involved with this study and used their feedback to distinguish and clarify emergent themes.

In the next step, the factors that facilitate and hinder the development of dynamic capabilities in the process of cybersecurity incident response were identified. Cybersecurity incident response process maturity and collaboration with trusted partners to exchange threat intelligence were identified as the key supporting factors related to incident response process. In addition, self-service analytics and measuring the relevant key risk indicators were the main supporting factors related to analytical capability. The potential challenging factors that hinder the development of dynamic capabilities in the incident response process were also noted such as stakeholder buy-in, misaligned BA and cybersecurity skills, and understanding the role of technology.

In the final step, the impact of using real-time analytics in the cybersecurity incident response process on overall enterprise security performance was examined. The analysis of this study’s data suggests that studied organizations reaped both strategic and economic benefits and thereby improved their overall enterprise security processes as a result of developing real-time analytics enabled dynamic capabilities and dynamic incident response strategies. For example, in FinInsuranceB, the general manager of cybersecurity strategy and governance noted that the capabilities enabled by real-time analytics have helped them to develop more efficient and robust access models and thereby improve their access management across all enterprise systems.

Stage 4: Integrate findings to build a theoretical model

The data about real-time analytics capabilities, real-time analytics enabled dynamic capabilities, dynamic incident response strategies, factors that facilitate and hinder the development of dynamic capabilities and enterprise security performance were integrated to describe their overall features. Finally, existing theory was embedded to assist in explaining the relationships between constructs. The integration of data and extant literature resulted in a model of dynamic cybersecurity incident response to improve incident response agility. I shared the emergent model with two peer researchers to clarify theoretical insights. The output of these analyses describes a model of dynamic cybersecurity incident response to improve incident response agility.

3.7. Evaluation of the Research Method

The extant literature proposes different approaches to assess the rigor in case study research both for the positivist (Dube and Paré 2003; Paré 2004; Yin 2017) and interpretivist (Gioia et al. 2013) paradigms. In order to evaluate the methodological rigor for exploratory case study research, this study adopts the framework proposed by (Carson 2001). This list of recommended techniques integrates several recommendations from the literature and is centred on the trustworthiness of the findings. Table 3-4 shows (Carson 2001) thirteen techniques for improving trustworthiness and these are mapped to the approaches used in this study.

Table 3-4. Trustworthiness of the Findings (Adapted from Carson 2001)

Technique	Application in this study	Status
Researching in the field	All the interviews took place at the informant's office.	✓
Purposive sampling	As explained in Section 3.2, the selection of multiple-case study sites was driven by purposeful, theoretical sampling.	✓
Cross-context comparison of results	As explained in Section 3.6, cross-context comparison was done in the analysis phase to generate insights within each case and then compared these insights across all the cases.	✓
Depth/intimacy of interviewing	All interviews were semi-structured in order to encourage discussion and reflection, rather than direct the interviewee in a specific direction.	✓
Negative case analysis	Evidence to disconfirm the proposition was sought both actively (by asking interviewees to elaborate on any contrasting views) as well as passively (by avoiding pointing the interviewees to any particular concepts included in the research model).	✓
Debriefing by peers	Debriefing by peers was used throughout data collection of the study. The first debriefing session normally occurred right after the interview (see also "Multiple interviewers" below). Several additional debriefing sessions were held with fellow academics, particularly in the course of the case study analysis.	✓
Maintaining a journal	The researcher maintained an extensive collection of memos and notes in relation to the research project and the preliminary thoughts on the findings at different stages of the project.	✓

Table 3-4. Trustworthiness of the Findings (Adapted from Carson 2001)

Technique	Application in this study	Status
Multiple interviewers	Most interviews were conducted by two interviewers (me and one of my supervisors) to balance the benefits of debriefing and the intimacy of interviewing (see above). In a limited number of occasions only a single or three interviewers were used.	✓
Present the findings to respondents	Some of the insights from cases were shared with key participants to assess comprehensiveness and reliability.	✓
Data triangulation	As explained in Section 3.2, data triangulation was achieved during the data collection by selecting participant at various levels within each organization. In addition, triangulation was also achieved by complementing the interviews with the review of relevant documentation.	✓
Draft review by respondents	This was not possible due to time constraints.	✗
Independent audits	This was not feasible due to confidentiality arrangements and the difficulties involved in sourcing an external auditor.	✗
Prolonged and persistent observation	This technique is not applicable, as observation was not a part of the research design.	**N/A**

As the Table 3-4 shows, this study matches all relevant criteria except for those related to draft review by informants, which was not possible due to time constraints within this study.

In addition, this study also adopted prescribed methods for data collection and analysis that sought to further increase the trustworthiness of the findings, including:

- using multiple levels of informants and multiple sources of data to triangulate perspectives (Darke et al. 1998; Eisenhardt 1989);
- a prolonged engagement with the research site to become enmeshed in the context and data (Smith 2014);
- developing thick descriptions and incorporating informant feedback to capture the rich context, and to ensure the quality and validity of interpretations (Langley 2007);

- using real-time cases to expedite data collection, while minimizing bias (Eisenhardt and Graebner 2007; Yin 2017); and
- researchers not taking part in the study reviewing the emergent models and constructs to vet ideas, and to enhance the validity and reliability of interpretations (Lincoln & Guba, 1985).

3.8. Summary

This chapter has outlined a detailed description of the research design and methodology used in this study. Firstly, justification of the interpretivist paradigm along with examination of the qualitative research method were provided. After that, the justification for using the exploratory multiple case study research method for this study was explained in detail. The criteria for case study participants and site selection were discussed, followed by the explanation of data collection and stages of the data analysis process. This chapter closed with an evaluation of the research method. The next chapter describes the analysis and findings of this study.

4

"Using analytics, we are improving our cybersecurity awareness and that is changing the perception that risk management is a valuable capability in the organisation and not what we call a handbrake on the happiness."

(General Manager of Cybersecurity Strategy and Governance, FinInsuranceA)

CHAPTER 4. FINDINGS

In last chapter, the research design and methodology were outlined, discussed and justified as appropriate to address this study's overarching research question, how organizations improve agility in their cybersecurity incident response process using real-time analytics. This chapter presents the results and key findings of the four stages of data analysis as outlined in the previous chapter. The first section of this chapter provides an illustrative story of each case in detail. All three studied organizations experience the dynamic cyber threat environment characterized by the dynamic, sophisticated and evolving nature of cybersecurity threats. Section 4.2 of this chapter presents the framework that this study develops based on the analysis of qualitative data. The subsequent sections explain each component of the framework in detail with supporting data.

In section 4.3, the key features of real-time analytics capability (real-time perspective, supporting architecture, automated decision making, and on-demand and continuous data analysis) in the process of cybersecurity incident response are explained. Section 4.4 describes three types of dynamic capabilities (real-time situational awareness, dynamic risk assessment, and cyber threat intelligence generation) that are enabled by the use of real-time analytics in the cybersecurity incident response process. In section 4.5, dynamic cybersecurity incident response strategies (active reconnaissance, continuous monitoring, and active defence) are explained. Section 4.6 identifies and explains the factors that facilitate and hinder the development of dynamic capabilities and execution of dynamic incident response strategies. In section 4.7, the strategic and economic benefits that studied organization reaped by using real-time analytics in their incident response process are explained. Section 4.8 explains the framework from improvement in incident response agility perspective. Finally, section 4.9 provides the summary of the key argument presented in this chapter.

4.1. The Case Studies Analysis

In this study, cybersecurity incident response units of three large organizations from the financial sector i.e. FinBank, FinInsuranceA and FinInsuranceB, were selected to explore their use of real-time analytics in the cybersecurity incident response process. Each of the incident response units of these organizations launched a data-driven incident response strategy no less than nine months and no more than 2 years before beginning this study. As a result, many of the insights that emerged in this study represent the output of that strategy. The cybersecurity incident response unit of FinBank is far ahead in terms of implementing their data-driven incident response strategy. In contrast, FinInsuranceA and FinInsuranceB were still in the process of integrating their cybersecurity systems and fully implementing their data-driven incident response strategy. All the organizations were at high levels of maturity in their cybersecurity incident response process and in their practice of business intelligence and analytics.

Since FinBank was already using analytical systems for several years to practice evidence-based decision making in their cybersecurity incident response process when the study was conducted, it was able to provide insights on the capabilities that they developed in their cybersecurity incident response process by using real-time analytics over time and their impact on overall enterprise security performance. In case of FinInsuranceA and FinInsuranceB, which had deployed business analytics for fewer years and were in the ongoing process of deploying real-time analytics systems when the study was conducted, they were able to provide insights on developing new capabilities using real-time analytics in cybersecurity incident response process and how they are impacting their enterprise security performance. The detailed description of each case is given below.

4.1.1. The FinBank Story

FinBank is one of the largest financial companies in Australia and a major international banking and financial services group that is among the top 50 banks in the world. FinBank is globally recognized as a successful financial company with very high market share, employing more than 50,000 employees and with revenue of over AUD$20 billion annually. FinBank recognises the importance of effective decision-making to its business success and established a dedicated analytics team ten year ago working collaboratively with the business functions. The top-level management is committed to achieve strong control, and a distinctive analytical and cybersecurity incident response capability that enables FinBank divisions and business units to perform their daily operations securely and meet their performance objectives efficiently.

> "So, we are a bank. Our whole business model is based on taking risk. Across all the disciplines or majority of disciplines of risk, credit lending, market positioning, market risk, liquidity risk, technology operational risk and compliance; there needs to be an ability to be able to consume the history of the organization, digest that and be able to try and use that information to be able to predict the future. This is where we use analytics. That is taking information we know, being able to take the data, apply various models and statistical means to consume that information, presenting that information against scenarios, presenting that information simply against history to be able to get trends, to be able to understand what the organization is doing strategically (perhaps that is a scenario), model against it with a view of being able to determine where do we believe there is an increased or enhanced risk exposure to the organization." (General manager of cybersecurity risk management, FinBank)

At FinBank, the reason for integrating analytical practices in cybersecurity function was to nurture data-driven decision-making culture in cybersecurity management.

> "From the security perspective, certainly we are forever consuming the information regarding the increasing and changing threat factors. Analysing the data related to that help us understand what our weaknesses are and what are therefore the mitigants which might well be investments in new appliances to help manage and protect the bank. All that needs to be formed up into a business case, and that business case needs to be backed up by facts often from security or technology perspective, it is much like doing a piece of work which is mandated to you by law. The business case has no benefit per se that is of financial nature, it is much more around protection. So, it is about how we take in the analytics of what we see in our cyber threat landscape, knowing about our existing capability, the gap is therefore the door that we need to close. How we articulate that back to the CFO for example in representation that enables us to get money needs to be repositioned into a language which is more of a compliance nature. So,

> you are looking at two types of investments that a bank does. In capability, it invests in products which ultimately ends up in the market and generate revenue. And there is another large stream of work which is effectively managing the ability of the bank to adhere to legislation, compliance, industry standards and its own weaknesses. And sometime, its own weaknesses are generated by its own activities. Now all the investment that is generated into new products or new capability, my team uses analytics in this process and plays a part by presenting themselves as the security architects into that capability ensuring that the most current information around threat is factored into the business case. And these are factored in as requirements from security perspective so that when we build the product or the capability, the capability is not only revenue generating but it also safe to do business with it." (General manager of cybersecurity risk management, FinBank)

FinBank has a dedicated security operations centre (SOC) team whose primary job is to establish and maintain a security information and event management (SIEM) system that receives data related to cybersecurity events, such as user access and activity logs. The SOC team analyses the SIEM logs to identify malicious activities, including indicators of compromise, event correlation rules and evaluating details from potential adversaries. The key roles and responsibilities of FinBank SOC team include:

- Tier 1 security analysts (reviews vulnerability assessment reports and runs vulnerability scans, reviews the latest cybersecurity alerts to determine urgency and relevancy and generates alerts that require tier 2 incident response review),
- Tier 2 security analysts (leverages threat intelligence feeds to identify scope of attack and affected systems, reviews alerts generated by tier 1 analysts and determines and directs recovery and remediation efforts),
- Tier 3 expert security analysts (uses the latest threat intelligence feeds to identify analyse stealthy threats, reviews vulnerability assessment and asset discovery data, and recommends how to optimize cybersecurity monitoring tools based on threat hunting discoveries),
- SOC manager (reviews the incident reports and manages the escalation process, supervises the activities of the whole SOC team, supports the audit process and runs compliance reports, communicates the value of cybersecurity operations to C level executives and measures SOC performance metrics), and

- Chief information security officer (responsible for defining the overall cybersecurity operations at FinBank, communicates with management regarding cybersecurity issues and manages compliance related tasks).

FinBank's cybersecurity strategy includes SOC, SIEM systems and a custom-built security analytics solution that helps to generate insights based on security data and take informed actions. FinBank uses analytics in all phases of the cybersecurity incident response process including preparation, response and follow-up. Some examples where FinBank's cybersecurity incident response team uses real-time analytics include (a) access management (e.g. in blocking (and logging) of unauthorised access); (b) forensic analysis (e.g. analysing phishing attacks and network data to monitor network activity in real-time.); and (c) analysis of logs (e.g. service and application logs, operating system logs, network device logs and network flows).

> "I think phishing is probably our biggest concern, because phishing leverages the flesh and blood that are our staff and that is the main control point that we cannot regulate technically. Technology helps to do whole lots of things in a routine way, but humans don't behave routinely. Therefore, phishing is a very serious issue. Broadly in terms of how we control it, we educate our staff on regular basis and use real-time analytics to monitor and analyse communications across our email servers. We also do phishing fire drills. We sort of roll up scenarios to staff and watch their behaviour. Then we take the data back from this activity and analyse why the staff are doing what they did. What did they see? Why did they respond the way they did and so on? So, we manage the data collection from human force and the technical force and we are consuming and digesting that in different ways for different reasons." (Manager of IT and information security, FinInsuranceA)

4.1.2. The FinInsuranceA Story

FinInsuranceA is recognized as a successful financial company with high-market share, employing more than 15,000 employees and with revenue of above AUD$10 billion annually. FinInsuranceA implemented its corporate data warehouse eight years ago that integrates and correlates data from multiple data sources such as customer relationship management systems, sales systems and claim management systems. The data from these sources are used to produce reports and dashboards to analyse the effectiveness and the performance of supporting business processes.

> "Our analytics team manages a corporate data warehouse that collects and correlates data from multiple different sources such as customer database, our sales systems as well as our claims management system. This data is used to analyse and produce reports on the effectiveness and the performance of those supporting business processes. Historically the corporate data warehouse was quite a siloed function. Some of the insights that we would gain from that would be used by the business to help determine what products and services they wanted to offer our customers. So that was all based on very traditional structured databases, publishing data cubes and reports, providing presentation layers services such as portals or query tools that our business stakeholders are be able to tailor to retrieve the sort of information that they need to support their business processes. That is historical." (General manager of cybersecurity strategy and governance, FinInsuranceA)

However, since 2014, FinInsuranceA has been investing in building a data-driven decision-making capability that can help them harness both structured and unstructured data to generate comprehensive business insights using latest data analytics platforms.

> "We now have got a team that we call customer labs that owns the capability for building non-SQL type solutions based on Hadoop data clusters. Also, applying more modern data science methods such as assisted or non-assisted machine learning to try and discover and get insights. To the point where we actually acquired a data science company that was originally funded as a start-up by the federal government. We acquired the company about eighteen months ago. So, now we have got a team of about sixty data scientists, proper data scientist working within the organisation and with our cybersecurity incident response team. And their main aim is to use their methods and their practices to collect and correlate information not just from internal data sources but also combine that with sets of data from other external sources. Such as the data we can share around with some of our business partners as well as government and other publicly available information. These are both structured and unstructured data and be able to combine these sets of information together to get or discover insights and wisdom. So, part of that is looking at both our customer value proposition. So, how can we get insight regarding who our key customers are and where they are in their life journey? And then in turn what is important and relevant to them and then how can we translate into meaningful products and services? Also measuring our performance in how we are maintaining our promise to our customers. And we are also turning and using the analytics to also understand our business operation and look into

> areas where we can optimize those to make our organisation more efficient. So, it is a very broad answer that is the general remit of our team that does all of our analytics and insights." (General manager of cybersecurity strategy and governance, FinInsuranceA)

FinInsuranceA also has a dedicated SOC team whose primary job is to leverage cybersecurity monitoring tools to discover malicious or suspicious activities by investigating indicators of compromise and analysing alerts. The key roles and responsibilities of FinInsuranceA SOC team include:

- Chief information security officer (communicates with management regarding cybersecurity issues and has the responsibility of defining the overall security operations at FinInsuranceA),
- SOC manager (manages all SOC activities, including management of other team members and creating new procedures and policies),
- Security analysts (Investigates, detects and responds to cybersecurity threats and implements additional cybersecurity measures where required) and
- Security architects (builds cybersecurity architecture and liaises with developers to ensure systems are up-to-date and has the responsibility of maintaining and recommending new cybersecurity analysis and monitoring tools).

FinInsuranceA's SOC team is also liaising with the analytics team to build their cybersecurity analytics capability.

> "Our analytics platform people are extremely hungry and interested in the information that we are collecting into SPLUNK so that they can then ingest that in to their HADOOP data clusters. So that they can use that information to do analysis on operational performance in the organisation. So, they can see other insights that they can get from the data that we are collecting, and they are not currently getting. We are also looking at leveraging some of their capabilities to help us analyse and improve our access management. We have practices and processes around managing accounts and setting up permissions for our colleagues i.e. role-based access. And we have been talking to our analytics team around using some of their capabilities to optimise how we manage our access control for assistance to help us reduce our risk exposure and achieve outcomes like principle of least privilege and timely provisioning and de-provisioning of access." (Manager of cybersecurity strategy and governance, FinInsuranceA)

FinInsuranceA cybersecurity strategy include SOC, SIEM and managed security service provider.

> "From a security point of view, Splunk is our tool of choice that our SOC team uses for collecting information from multiple sources to correlate and determine what we call actionable events such as indicators of compromise, or emerging threats. I still think we have certainly got a way to go to fully implement our cybersecurity analytics capability. We also have a relationship with an external service provider who also offers some analytics capability for security events and incidents using their own proprietary platforms. The next thing in our roadmap is to move to a capability such as behavioural analytics and apply machine learning and so on." (Manager of cybersecurity strategy and governance, FinInsuranceA)

FinInsuranceA uses analytics in all phases of the cybersecurity incident response process including preparation, response and follow-up. Some examples where FinInsuranceA's cybersecurity incident response team uses real-time analytics include (a) Security logs analysis to correlate security events; (b) access management (e.g. managing access across all its systems and assets in real-time); and (c) malware analysis.

> "I think the real benefits that we are seeing from using real-time analytics right now like in immediate term future is helping us in our access management. In the past, we were very in-efficient with how we managed our access across all our systems and assets as we are very complex environment. So, it's the way we set up and manage our permissions and access of our people was very in-efficient and was resulting in the loss of productivity and increased risk exposure. Because people have got excessive access to the systems that has increased the likelihood of internal fraud or accidents happening. So, the immediate opportunity that we see in applying more advanced analytics techniques is to try and develop more efficient and robust access models. That will then help us progressively reduce our risk of thing like fraud or accidental of disclosure or destruction of information. Beyond that we also want to continue and build our relationship with the analytics team to look at what we can do to develop the predictive analytics capability as well." (Manager of cybersecurity strategy and governance, FinInsuranceA)

4.1.3. The FinInsuranceB Story

FinInsuranceB is a multinational financial services company headquartered in USA and has many financial services branches in Australia. FinInsuranceB is also recognized as a successful financial company with high-market share, employing more than 35,000 employees and with revenue of over AUD$15 billion annually. In Australia, FinInsuranceB has a cybersecurity division that supports multiple business domains with a dedicated SOC and analytics team and collaboratively works with other business functions. The cybersecurity division was established six years ago primarily to address the insider threat and data leakage issues of the organization.

> "So, around six years ago we reviewed our cybersecurity strategy particularly from insider threat and data leakage perspective. The one thing that we found that we were very weak in our capability around detection and response regarding insider threat and data leakage. In addition, our incident management practice was also immature. So, we established a cybersecurity division here to address these issues and improve our detection and response capability by using analytics. By improving our detection capability adequately will address our exposure around reducing the likelihood and the impact of data breach by being able to quickly discover and respond. That is common to many other organisations where the time of discovery can be 100s of days after the actual breach event has taken place. So that was the realization, then translating that into a roadmap to decide an outcome is the journey we are still on. So, we went through a process of determine what our best options are with regards to our SIEM tools and processes. So, we created a new team with appropriate skills and invested in technology called Splunk and enterprise security manager." (Director of global cyber forensics, FinInsuranceB)

They cybersecurity incident response unit at FinInsuranceB also contains a dedicated SOC team whose primary job is to leverage cybersecurity monitoring tools to discover, analyse and respond to cybersecurity incidents by investigating indicators of compromise and security alerts. In addition, SOC team at FinInsuranceB continuously monitors and analyses user access events to protect its data and infrastructure. The key roles and responsibilities of FinInsuranceB SOC team include:

- Chief information security officer (manages compliance tasks, communicates with management regarding cybersecurity issues and has the responsibility of defining the overall security operations at FinInsuranceB),
- SOC manager (develops and executes crisis management plan to chief information security officer and other stakeholders, manages all SOC activities, including management of other team members and creating new procedures and policies),

- Security architects (reviews and update cybersecurity events correlation rule, builds cybersecurity architecture and liaises with developers to ensure systems are up-to-date and has the responsibility of maintaining and recommending new cybersecurity analysis and monitoring tools), and
- Security analysts (performs triage on the security alerts by determining their criticality and scope of impact, investigates, detects and responds to cybersecurity threats and implements additional cybersecurity measures where required).

FinInsuranceB cybersecurity strategy include combination of SOC and SIEM systems. FinInsuranceB analytics team is building their security analytics capability and delivers insights to security executives so that they can make data-driven informed actions related to cybersecurity.

> "Where we are aspiring to be, and we are in the process of creating this capability which is going to be finished early next year. That capability is effectively a data lake into which we will throw everything and therefore create a single source of consumption for cybersecurity analytics. For us, that is probably the best in class that you can get today with all your information in a single spot. So, behind that, we will have an analytics engine which we have purchased. That will position us reasonably well in the market place for quite a sometime to be able to start becoming deeply conscious and responsive to the cybersecurity events. That new capability will I think hopefully allow us to be far more predictive rather than reactive." (Chief security architect, FinInsuranceB)

FinInsuranceB also uses analytics in all phases of the cybersecurity incident response process including preparation, response and follow-up. Some examples where FinInsuranceB's cybersecurity incident response team uses real-time analytics include (a) insider threat detection; (b) employee activity monitoring; and (c) analysis and monitoring emerging cyber threats.

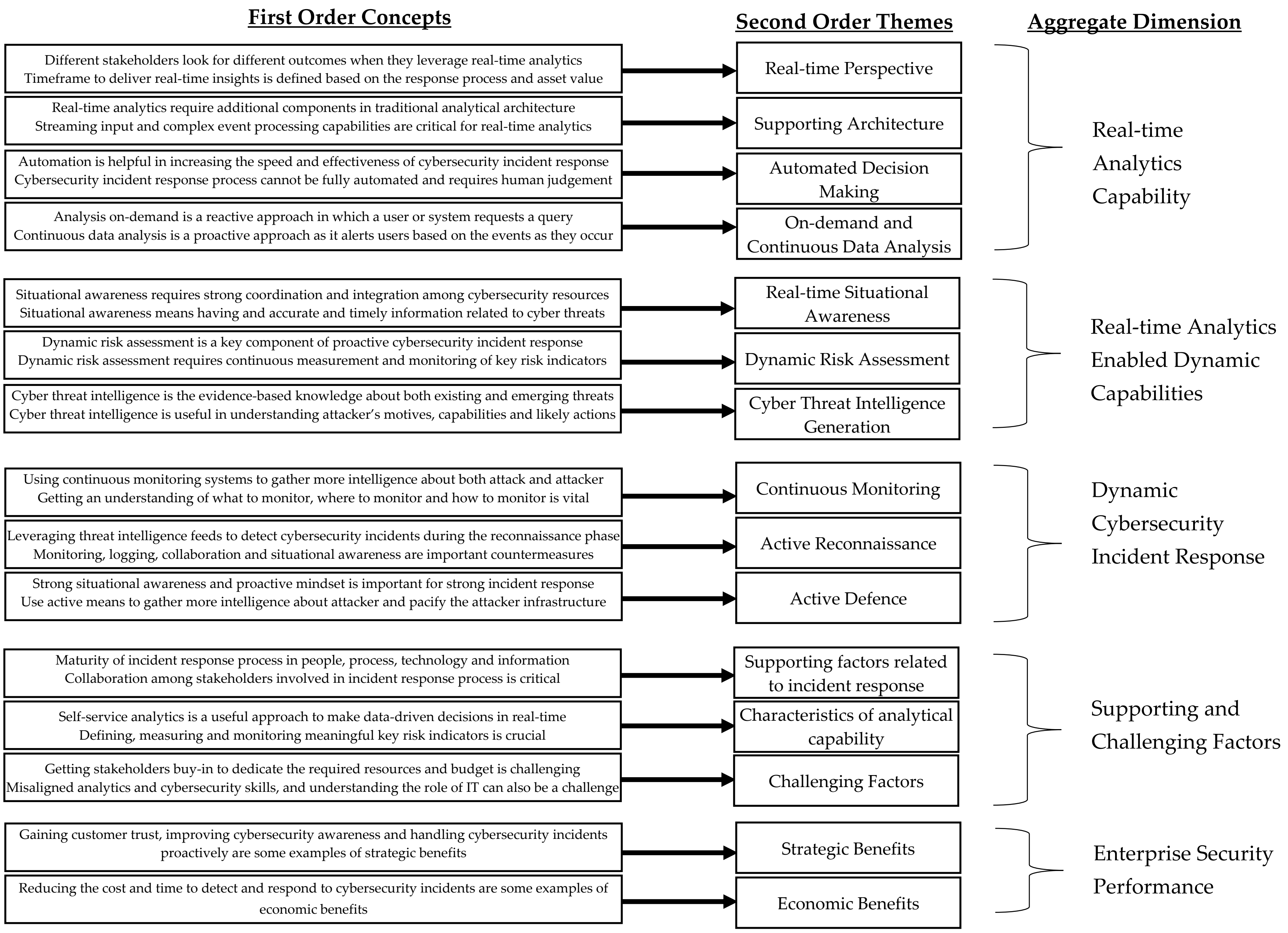
> "Actually, the recreational hacker given what he knows and sees, because the public community in the internet allows him to understand, he is actually no longer a recreational hacker. At fifteen, you can have a reasonably sophisticated individual who because we now have the land of the cloud, so very cheap access to significant computing power enables a kid to become a rogue hacker very simply. It could still be recreational, but it is far more advanced and sophisticated and nimble to be able to be more damaging to the organizations than ever before. So never ever before has it been more important for us to use analytics to be able to understand what people

> are doing internally in the organization from malicious insider, and just ensuring our staff more broadly do what they are supposed to do and nothing more all the way through to what is happening at outside world." (Chief security architect, FinInsuranceB)

4.2. The Framework

This study explores the use of real-time analytics in the cybersecurity incident response process of three large organizations from financial sector i.e. FinBank, FinInsuranceA and FinInsuranceB. The narrative that follows describes how the use of real-time analytics in the cybersecurity incident response process helped these organizations to develop higher-order real-time analytics-enabled dynamic capabilities and dynamic incident response strategies. In addition, it also describes the impact of using real-time analytics capabilities in cybersecurity incident response process on overall enterprise performance. To further support this narrative, a data structure display (Figure 4-1), and a data table (Table 4-1) that supports emergent constructs are also included. Finally, the findings from the data analysis are integrated with existing literature to build an overall framework of dynamic cybersecurity incident response to improve cybersecurity incident response agility.

Figure 4-2 shows the framework that this study develops based on the analysis of qualitative data. All the studied organizations experience dynamic cyber threat environment characterized by the dynamic, sophisticated and evolving nature of cybersecurity threats (predictable and unpredictable) such as advanced persistent threats, insider data theft, zero-day attacks, phishing and spear phasing attacks. These organizations respond to this dynamic threat environment by using real-time analytics in their cybersecurity incident response process. Specifically, they use real-time analytics capability to develop higher order analytics-enabled dynamic capabilities such as real-time situational awareness, dynamic risk assessment and cyber threat intelligence generation. These three dynamic capabilities, enabled by real-time analytics, help shape three dynamic incident response strategies (namely, active reconnaissance, continuous monitoring, and active defence). These dynamic capabilities together with dynamic incident response strategies infuse agile characteristics such as swiftness, flexibility and innovation in cybersecurity incident response process, which in turn, lead to positive outcomes in enterprise security performance by delivering strategic and economic benefits. In addition, the framework also identifies two groups of factors (cybersecurity incident response factors and characteristics of analytical capability) that foster the development of dynamic capabilities and execution of dynamic cybersecurity incident response strategies. The framework is described in detail below.



First Order Concepts	Second Order Themes	Aggregate Dimension
Different stakeholders look for different outcomes when they leverage real-time analytics Timeframe to deliver real-time insights is defined based on the response process and asset value	Real-time Perspective	Real-time Analytics Capability
Real-time analytics require additional components in traditional analytical architecture Streaming input and complex event processing capabilities are critical for real-time analytics	Supporting Architecture	
Automation is helpful in increasing the speed and effectiveness of cybersecurity incident response Cybersecurity incident response process cannot be fully automated and requires human judgement	Automated Decision Making	
Analysis on-demand is a reactive approach in which a user or system requests a query Continuous data analysis is a proactive approach as it alerts users based on the events as they occur	On-demand and Continuous Data Analysis	
Situational awareness requires strong coordination and integration among cybersecurity resources Situational awareness means having and accurate and timely information related to cyber threats	Real-time Situational Awareness	Real-time Analytics Enabled Dynamic Capabilities
Dynamic risk assessment is a key component of proactive cybersecurity incident response Dynamic risk assessment requires continuous measurement and monitoring of key risk indicators	Dynamic Risk Assessment	
Cyber threat intelligence is the evidence-based knowledge about both existing and emerging threats Cyber threat intelligence is useful in understanding attacker's motives, capabilities and likely actions	Cyber Threat Intelligence Generation	
Using continuous monitoring systems to gather more intelligence about both attack and attacker Getting an understanding of what to monitor, where to monitor and how to monitor is vital	Continuous Monitoring	Dynamic Cybersecurity Incident Response
Leveraging threat intelligence feeds to detect cybersecurity incidents during the reconnaissance phase Monitoring, logging, collaboration and situational awareness are important countermeasures	Active Reconnaissance	
Strong situational awareness and proactive mindset is important for strong incident response Use active means to gather more intelligence about attacker and pacify the attacker infrastructure	Active Defence	
Maturity of incident response process in people, process, technology and information Collaboration among stakeholders involved in incident response process is critical	Supporting factors related to incident response	Supporting and Challenging Factors
Self-service analytics is a useful approach to make data-driven decisions in real-time Defining, measuring and monitoring meaningful key risk indicators is crucial	Characteristics of analytical capability	
Getting stakeholders buy-in to dedicate the required resources and budget is challenging Misaligned analytics and cybersecurity skills, and understanding the role of IT can also be a challenge	Challenging Factors	
Gaining customer trust, improving cybersecurity awareness and handling cybersecurity incidents proactively are some examples of strategic benefits	Strategic Benefits	Enterprise Security Performance
Reducing the cost and time to detect and respond to cybersecurity incidents are some examples of economic benefits	Economic Benefits	

Figure 4-1. Data Structure

Table 4-1. Data Supporting Interpretations of Second Order Themes

Dimension	Themes	Representative Quotes
Real-time analytics capability	Real-time perspective	"Real-time analytics is about taking streaming data in and analysing it in some way within the timeframe that we have agreed on and meets our requirements." (Head of global insider threat detection, FinInsuranceB) "We define real-time analytics timeframe depending on the asset value and how important it is to execute an appropriate response once a threat is detected. So, when we are trying to stop a cybersecurity attack or compliance threat before it causes any damage to us, it is critical that we execute the lowest latency response." (General manager of cybersecurity risk management, FinBank) "Real-time analytics has different meaning to different people. It depends on your role and the process you are using it in to enable instant decision making." (General Manager of cybersecurity strategy and governance, FinInsuranceA)
	Supporting architecture	"The tool that we are using to enable real time analysis in our cybersecurity incident response process is SPLUNK. What it enables us to do is real-time analysis, search and monitoring of cybersecurity events…So, we are able to drill down\monitor in real time using different views across our dashboards." (General manager of cybersecurity strategy and governance, FinInsuranceA) "I think the first thing was setting the base infrastructure and prioritizing the feeds that needed to be consumed into the services based on their value. Some of it was all part of the more detailed roadmap and planning around the SIEM project. So, that was one of the early milestones agreeing on the scope, approach and the desired target architecture for our real-time analytics capability." (Chief security architect, FinInsuranceB) "We have added several additional components in our analytics architecture to implement real-time analytics such as in-memory analytics, data virtualizations and service-oriented architecture." (Chief security architect, FinInsuranceB)
	Automated decision making	"We use complex event processing tools to analyse streaming data in real time. Based on the rules, the system can then either generate alerts that our threat hunting team monitors to see patterns and trends or can also trigger automated response." (Head of cyber threat detection and response team, FinInsuranceA) "Recently, we have added the automated response capability in our security event processing solution. It can execute automated response or actions like flagging, filtering, transforming, and alerting of cybersecurity events as they arrive. A response might be executed based on sophisticated criteria, such as anomaly detection models. We not only use this in our cybersecurity incident detection and response, but also in fraud detection and recommendation, as these demand lowest latency response." (General manager of cybersecurity risk management, FinBank) "The progression to automated incident response in real-time is often gradual. What I mean by that is, the improvement in the speed with which we executed the response was improved gradually, such as getting from days to hours to minutes or even seconds. Then, if required further refinement can also be done based on the business need." (General manager of cybersecurity risk management, FinBank)
	On-demand and continuous data analysis	"Real-time analytics helps us to react to cybersecurity threats without any delay…In simple words, what we are doing is continuously analysing cybersecurity events to detect potential threats and prevent incidents before they happen." (Manager of cybersecurity strategy and governance, FinInsuranceA) "To combat advanced cybersecurity threats, such as sensitive data exfiltration and zero-day malware, we use both on-demand and continuous real-time analytics to analyse all network traffic, log data from applications, security systems, and network data and also fuse external threat intelligence in real-time." (Director of global cyber forensics, FinInsuranceB) "We use continuous monitoring systems (SIEM) to analyse cybersecurity events in which we do event and log collection and correlation. This helps us to separate real events (incidents) from nonimpact events. In addition, this also helps us to locate and contain cybersecurity incidents." (Manager of cybersecurity strategy and governance, FinInsuranceA)

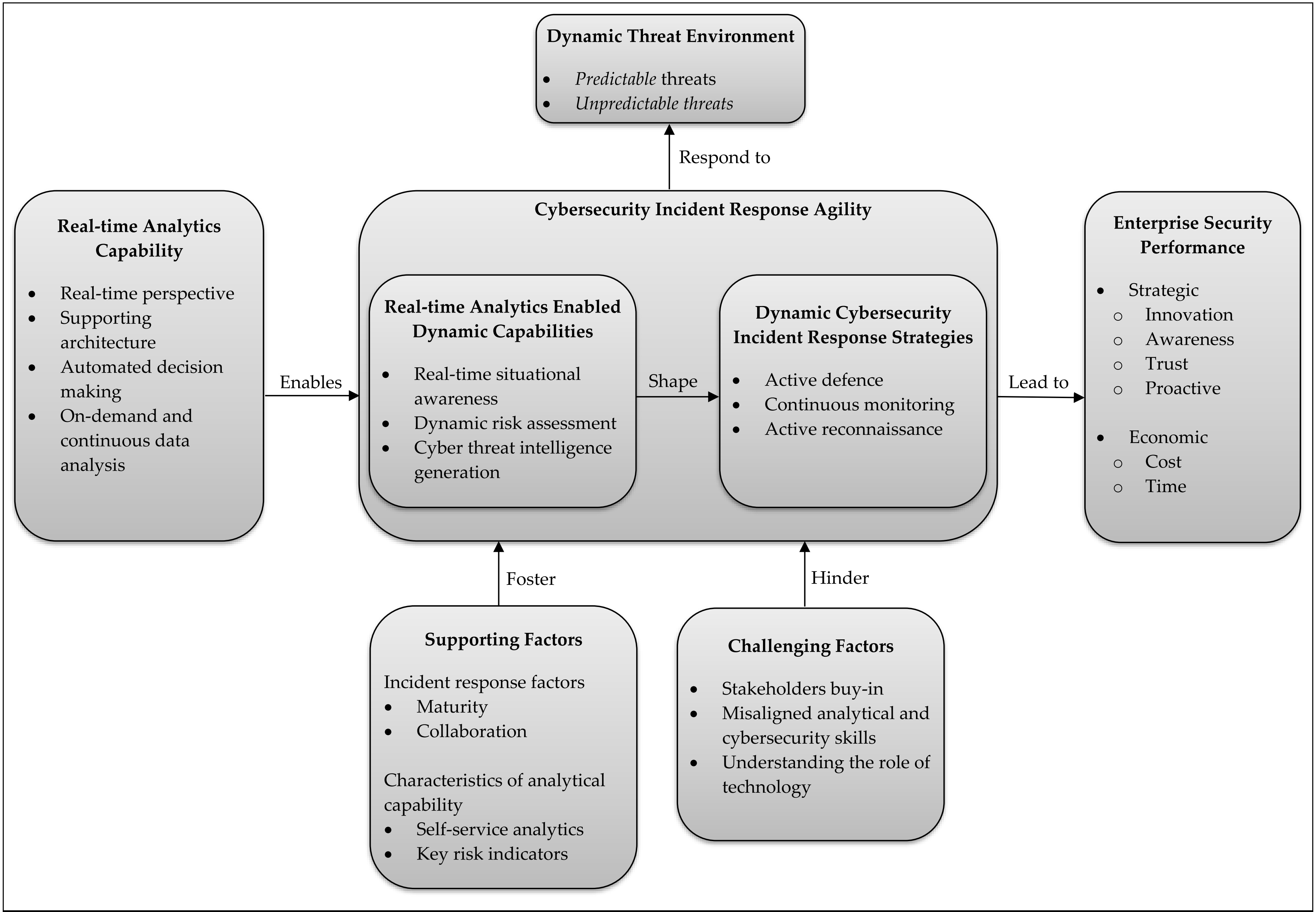
Table 4-1. Data Supporting Interpretations of Second Order Themes (Continued)		
Dimension	**Themes**	**Representative Quotes**
Real-time analytics enabled dynamic capabilities	Real-time situational awareness	"Because we are using continuous monitoring systems to analyse cybersecurity events across the network, this greatly improves the level of cybersecurity awareness of our cybersecurity managers." (Data analyst, FinBank) "To achieve successful continuous monitoring of networks and improve our cybersecurity awareness, both detective and proactive monitoring actions must work together." (Head of global insider threat detection, FinInsuranceB) "We have deployed intrusion prevention, log management and advanced SIEM systems with correlation capabilities to consolidate threat intelligence feeds into monitoring dashboards and alerting systems. The effort that we have put in consolidating this information has resulted in improved situational awareness of activities, users and systems as well as awareness of the attacks being attempted on our networks." (General manager of data and analytics, FinBank) "Even if we did go through the process of raising an item in our risk register we found that the risk consciousness, the awareness across all of the information systems or assets owners was not such that they are necessarily taking the appropriate timely action to respond with any remediation treatment activities that they may have…So, the analytics driven decision making has developed a culture in such a way that we are able to establish a much firmer tone of management intent, much clearer guidelines around what our risk tolerance or risk apatite is, and also being able to deliver meaningful insights that can empower the decision makers to take the appropriate timely actions." (General manager of cybersecurity strategy and governance, FinInsuranceA)
	Dynamic risk assessment	"If I make a comparison of using batch style analytics with real-time analytics, it may take hours or even days to yield results using batch style analytics. So, our batch analytical applications are very good in delivering "after the fact" insights (lagging indicators). In contrast, the insights that we get from analysing leading key risk indicators allow us to get ahead of the curve." (General manager of data and analytics, FinBank) "By consolidating information from continuous monitoring systems into a dashboard, our threat hunting team can identify and monitor assets that have higher levels of risk and then respond to threats against these assets appropriately." (Head of cybersecurity incident response team, FinBank) "So, by virtue of our teams periodically reviewing and measuring our capabilities against the framework and against our industry peers, we are demonstrating that we are proactively trying to continue to improve our capabilities to stay one step ahead of the threats." (Manager of IT and information security, FinInsuranceA) "We are definitely more interested in reporting and analysing the lead indicators in real-time that would demonstrate that the organisation is drifting outside of its risk appetite." (Director of global cyber forensics, FinInsuranceB)
	Cyber threat intelligence generation	"Our cyber defence and response team is proactively taking and analysing that information and then translating that into changes in our security services to try and provide a counter measure before we actually see those attacks hit our enterprise." (Head of cyber threat detection and response team, FinInsuranceA) "We have threat intelligence feeds in which we use analytics to analyse what is happening and we also participate in threat intelligence sharing communities." (General manager of cybersecurity strategy and governance, FinInsuranceA) "We use cyber threat intelligence feeds to continuously improve the effectiveness of cyber security threat analysis process. So, for example while we are investigating a cybersecurity incident, having access to cyber threat intelligence can be very useful in understanding attacker's capabilities, motives and likely actions." (General manager of cybersecurity risk management, FinBank)

Table 4-1. Data Supporting Interpretations of Second Order Themes (Continued)

Dimension	Themes	Representative Quotes
Dynamic Cybersecurity Incident Response Strategies	Continuous monitoring	“We need clear visibility into data regarding system configuration and patch levels, device behaviour, vulnerabilities, and overall cybersecurity state. The information regarding cybersecurity state and vulnerabilities for these systems needs to be continuously monitored and correlated to demonstrate security compliance when required.” (Cybersecurity senior manager, FinBank) “Getting an understanding of what to monitor, where to monitor and how to monitor is very important. Continuous monitoring does not mean that everything including all applications, systems, end points, networks, security processes and infrastructure needs to be monitored everywhere and all the time. Therefore, it is very important to determine what needs to be monitored and set monitoring policies around those needs.” (Chief security architect, FinInsuranceB)
	Active defence	“Sometimes people commonly misunderstand proactive may necessarily be equal to protective or preventative and yet if you talk to a lot of experts in the cybersecurity industry current thinking basically says that you can assume that at some point you might actually be compromised, or you have breach of some sort. So rather than just saying by putting all your investment in a preventative approach, you can still be proactive in boosting your detection and response capabilities so that when something happens you know that sooner, which means you can decrease the impact and then also recovery and all that is well planned so that you cater better in reduction of impact.” (Manager of cybersecurity strategy and governance, FinInsuranceA)
	Active reconnaissance	“Our incident response team uses cyber threat intelligence feeds to understand the procedures, tactics and techniques of the attackers and can stop some attacks by degrading or disrupting their efforts. In this way, cyber threat intelligence helps us in detecting an incident during the reconnaissance phase, that is before we have actually been attacked.” (General manager of cybersecurity risk management, FinBank) “Using [cyber] threat intelligence, our incident response team tries to understand the methodology, intent and focus of the attack and in some cases, can detect an incident during the reconnaissance phase.” (General manager of cybersecurity strategy and governance, FinInsuranceA)
Supporting and Challenging Factors	Supporting factors related to cybersecurity incident response	“Identifying what our current level of capability maturity is helps us to identify what our gaps are. We can then formulate our strategy to fill these gaps and improve our capability for cyber security services over time.” (General manager of cybersecurity strategy and governance, FinInsuranceA) “The first step we did to improve the analytical capability in incident response process was to collaborate and establish a relationship with our analytics team. We started embedding some of their practices and processes and even using some of their services. By building stronger relationships and leveraging the capabilities of analytics team, we were able to improve and drive our decisions based on the data.” (Director of global cyber forensics, FinInsuranceB)
	Characteristics of analytical capability	“Self-service analytics is definitely a useful approach to make data-driven decision in real-time, but it is something that comes with at a very high maturity level.” (General manager of data and analytics, FinBank) “Being able to measure the cybersecurity operations or processes using key risk indicators is crucial. So, until we get to a point where we have meaningful key risk indicators that are measurable, comparable, informational and predictable, we cannot get full benefit out of analytics.” (Manager of cybersecurity strategy and governance, FinInsuranceA)
	Challenging factors	“If we went to the board and said that we want to spend some money to invest on some technology or product to develop a capability and the project is not mandatory [compliance requirement], getting their support and involvement is very difficult.” (General manager of cybersecurity strategy and governance, FinInsuranceA) “We have got people from the security infrastructure background and from the threat intelligence background. That does not necessarily mean that they are strong data analysts.” (Manager of IT and information security, FinInsuranceA)

Table 4-1. Data Supporting Interpretations of Second Order Themes (Continued)

Dimension	Themes	Representative Quotes
Enterprise Security Performance	Strategic benefits	"The concept of cybersecurity risk management is so that we can operate our business processes in a manner with some assurance that we can actually be very confident in doing our daily business operations. The analogy is like where you have brakes on a car, it is actually the breaks that are there to allow you to go faster, it is not to slow you down. So, the benefit of using analytics is that we can actually manage our risks appropriately and we can have the confidence to innovate and operate our business processes in a manner that they can be very effective and efficient." (Manager of cybersecurity strategy and governance, FinInsuranceA) "I think we have started getting real benefits of using analytics in our cybersecurity incident response in last 12 months. We also had the managed service, I mentioned that we have got an external service provider that has been doing some of the analysis for us. We have been able to use that information to better inform ourselves around what our gaps are. What our weaknesses are? And I can say in last 3 years we have got an evidence that we have been able to use analytics to proof a gap. And invest in a security controls that have reduced our security exposure or reduced the number of incidents that we have seen." (General manager of cybersecurity risk management, FinBank) "I think the real benefits that we are seeing from cybersecurity analytics right now like immediate term future is helping us our access management. So, our immediate opportunity that we see in applying more advanced analytics techniques is to try and develop more efficient and robust access models. That will then help us progressively reduce our risk of thing like fraud or accidental disclosure of information." (Manager of cybersecurity strategy and governance, FinInsuranceA) "So, what we are doing is turning our cybersecurity risk management and incident response capability into it is almost like an opportunity, it is the upside instead of the downside, so if we have not managed our risks appropriately, we would not have availed ourselves the business opportunities. We do not have the confidence of saying we have millions of customers if we don't have appropriate risk management controls and how we manage our data." (General manager of cybersecurity strategy and governance, FinInsuranceA) "Using analytics, we are improving our security awareness and that is changing the perception that risk management is a valuable capability in the organisation and not what we call a handbrake on the happiness." (General manager of cybersecurity strategy and governance, FinInsuranceA)
	Economic benefits	"Organizations who invest in the analytics and do it the right way, of course they can lower their cost. So, if an organization is spending 25% of their budget in dealing with security incidents, breaches and penalties versus another organization that is only spending 10% because they are using the right tools and analytics to prevent incidents, breaches and not paying penalties. That means they already have economic benefit over their competitors." (Chief security architect, FinInsuranceB) "I don't think analytics is something we will market as a differentiator because for our customers, we are supposed to do that anyway. So, I think it is more of a case of just a necessity for us to do business… One thing that is worth calling out is insurance is a trust product. We are a trust business. So, you trust us with a lot of information. You have to tell me a lot about you and your life so that I can help protect you. It is a necessary part of our business that we maintain that trust. One of the ways that we maintain that trust is by protecting the information that you gave to us is using analytics." (General manager of cybersecurity strategy and governance, FinInsuranceA) "There are two critical components that drive overall cost in the incident response process, (1) once the attacker first gain access in the network, how long does it take to detect the intrusion; and (2) Once we have detected the intrusion or incident, how quickly can we execute a response and remediate the incident. Real-time analytics helps us in addressing both questions by reducing the time it takes to detect and responds to cybersecurity incidents and that can also lead to cost savings and better protection of data." (Head of cybersecurity incident response team, FinBank)



Dynamic Threat Environment

- *Predictable* threats
- *Unpredictable threats*

Respond to

Real-time Analytics Capability

- Real-time perspective
- Supporting architecture
- Automated decision making
- On-demand and continuous data analysis

Enables

Cybersecurity Incident Response Agility

Real-time Analytics Enabled Dynamic Capabilities

- Real-time situational awareness
- Dynamic risk assessment
- Cyber threat intelligence generation

Shape

Dynamic Cybersecurity Incident Response Strategies

- Active defence
- Continuous monitoring
- Active reconnaissance

Lead to

Enterprise Security Performance

- Strategic
  - Innovation
  - Awareness
  - Trust
  - Proactive
- Economic
  - Cost
  - Time

Foster

Hinder

Supporting Factors

Incident response factors

- Maturity
- Collaboration

Characteristics of analytical capability

- Self-service analytics
- Key risk indicators

Challenging Factors

- Stakeholders buy-in
- Misaligned analytical and cybersecurity skills
- Understanding the role of technology

Figure 4-2. A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility

4.3. Real-time Analytics Capability in Cybersecurity Incident Response

The cybersecurity environment is changing at a rapid pace. Most of the changes in cybersecurity landscape originate from the ways in which focal organizations create, collect, store and share information. The exposure of this information across multiple targets such as networks, software, data and physical components make it a tempting target for hackers and criminals. Therefore, continuous monitoring of cybersecurity events across these targets is crucial for business continuity and that is why the cybersecurity incident response units of all three studied organizations considered real-time analytics as an integral part of their cybersecurity incident response capability. As the general manager of cybersecurity strategy and governance in FinInsuranceA noted:

> "Real-time analytics helps our cyber defence and response team to analyse events as they occur and then determine if the event is really an incident. An event is just an item of interest and an incident is something that has caused a loss or an impact, or it is about to, or has the potential to cause a loss or impact. If they are an incident, then we respond to them using our cybersecurity incident response processes." (General manager of strategy and governance, FinInsuranceA)

The head of cybersecurity incident response team in FinBank echoed the same point and explained that real-time analytics helps them to identify cybersecurity incidents that require immediate attention and which assets are being impacted by the incident:

> "We use real-time analytics to determine whether an incident requires attention right now and which assets are impacted by the incident." (Head of cybersecurity incident response team, FinBank)

Real-Time Analytics touches almost every part of the cybersecurity incident response process, from the chief information security officer and cybersecurity architects, to cybersecurity analysts and cybersecurity managers, they all need to collect, use, and analyse data to shape their roles and strategies. That is why the key decision makers including cybersecurity managers and analysts in focal organizations used real-time analytics to analyse streaming data from various sources to detect malicious activities that can cause damage.

> "With real-time analytics, we are focused on incident detection. For example, using stream processing of data from network flows, sensors, and meta data, our managers and analysts look

> for suspicious or anomalous network activities that strongly indicate a security incident is in progress." (General Manager of data and analytics, FinBank)

In addition, each decision maker in the cybersecurity incident response process uses real-time analytics in different ways, depending on what their goals and needs are.

> "From managing compliance from a specific set of cybersecurity applications and detecting insider threats to calculating the assets value that are at risk, different stakeholders in the cybersecurity incident response process will be looking for different outcomes when they leverage analytics." (Director of global cyber forensics, FinInsuranceB)

Organizations also need to continuously monitor cybersecurity events to reduce exposure of information assets to new and evolving threats. This requires collection, storage and analysis of security data to generate insights that can help security executives to monitor and analyse activities across all information assets. General manager of cybersecurity risk management in FinBank explained that real-time analytics helps them to quickly integrate data from multiple data sources as follows:

> "Our security analytics solution continuously delivers insights from all network traffic logs and relevant business information to help us identify cyber threats quickly across the network". (General manager of cybersecurity risk management, FinBank)

He also identified the sources of security data as follows:

> "Analytics helps us in collection, analysis and correlation of information from multiple data sources such as IPS, IDS, SIEM, spam and antivirus software, and network and application logs so that we can gain visibility into most pertinent insights related to cybersecurity risks and can make informed actions accordingly".

When asked about who are the primary users of insights that are generated by analytical platforms, manager of cybersecurity strategy and governance in FinInsuranceA stated that:

> "The primary users of the information are our security operations centre and threat intelligence teams. So, they are our security analysts whose primary job is to analyse the incidents, or I should say events to determine if the event is really an incident". (Manager of cybersecurity strategy and governance, FinInsuranceA)

A Cybersecurity senior manager at FinBank further explained how their security executives use dashboards to inform their understanding of the cybersecurity environment:

> "Security executives analyse the consolidated information in the dashboards to understand what is happening across the network and use this information to minimize the risks to valuable assets under their management." (Cybersecurity senior manager, FinBank)

To further elaborate the critical role of real-time analytics in cybersecurity incident response, chief security architect of FinInsuranceB stated that:

> "We use real-time analytics to automate our common cybersecurity tasks." (Chief Security Architect, FinInsuranceB)

The key features of real-time analytics capability in cybersecurity incident response process observed in the studied organizations are discussed below.

4.3.1. Real-time Perspective

In today's dynamic cyber threat landscape, the incident response teams need to be nimble in order to deal with this dynamic threat environment. Cybersecurity managers need actionable insights faster than ever before to reduce risks, meet compliance requirements and detect and respond to cybersecurity threats in a timely manner. The typical workflow of any analytical application is to turn data into insights and then insights into decisions that add value. In cybersecurity incident response process with multiple levels, this workflow needs to happen very quickly to deliver a response in a timely fashion. In many focal organizations, the timeframe to execute this workflow can be different as it is dependent on the people, process and technology involved in the cybersecurity incident response process. The general manager of data and analytics in FinBank stated that:

> "The most important thing for us is to understand what our goals are for using real-time analytics, what resources we need and what any particular tool is providing us so that we can use it effectively." (General manager of data and analytics, FinBank)

The manager of cybersecurity strategy and governance in FinInsuranceA explained that the timeframe within which they execute the incident response can range from few minutes up to few hours depending on the type and nature of cybersecurity incident they are dealing with:

> "We use different types of approaches to address different types of cybersecurity incidents. As there is no single plan that fits for all purpose, our cybersecurity incident response timeframe can range from few minutes up to few hours." (Manager of cybersecurity strategy and governance, FinInsuranceA)

The term real-time analytics in focal organization was used and understood in different ways depending on the role of the stakeholder involved and requirements of the cybersecurity incident response process. The most important thing for them was to understand what data sources are relevant for real-time data analysis and what outcome they wanted to achieve using real-time analytics.

> "Real-time analytics is about taking streaming data in and analysing it in some way within the timeframe that we have agreed on and meets our requirements." (Head of global insider threat detection, FinInsuranceB)

> "Real-time analytics has different meaning to different people. It depends on your role and the process you are using it in to enable instant decision making." (General Manager of cybersecurity strategy and governance, FinInsuranceA)

Another crucial factor to consider in defining the timeframe for real-time analytics is to evaluate the asset value. When the most important organizational assets are under attack, then it is critical to execute the lowest latency response. General manager of cybersecurity risk management stated that:

> "We define the real-time analytics timeframe depending on the asset value and how important it is to execute an appropriate response once a threat is detected. So, when we are trying to stop a cybersecurity attack or compliance threat before it causes any damage to us, it is critical that we execute the lowest latency response." (General manager of cybersecurity risk management, FinBank)

Thus, the real-time analytics perspective or context can be different across different organizations as long as they leverage the right people, process, and technology to deliver analytical insights within the timeframe that meets the requirements of organizational cybersecurity incident response process.

4.3.2. Supporting Architecture

Traditionally, the architecture for majority of cybersecurity analytics solutions is designed on the logic of batch processing of data in which data from sources including intrusion detection systems, firewall logs, network flow logs, antivirus, and spam logs are extracted, transformed and then loaded into a centralized repository such as a SIEM system. Chief security architect at FinInsuranceB highlighted the importance of implementing an overarching cybersecurity analytics architecture that can help organizations generate, disseminate and take actions based on security insights:

> “cybersecurity analytics [capability] requires an architecture that can handle data from multiple sources in greater volume than at present, integrate this data into a centralized repository and then provide insights that can lead us quickly to the most pressing issues”.

To add real-time analytics capability in typical cybersecurity analytics architecture, the manager of cyber defence centre in FinInsuranceA noted that:

> “When we started building real-time analytics capability, we needed to add real-time analytics tools in our analytics architecture to analyse logs in real-time. So, for example some of the logs that we need in the SIEM also go into the real-time analytics platform as streaming data where it can be used for real-time analytics.” (Manager of cyber defence centre, FinInsuranceA)

Similarly, a senior cybersecurity analyst in FinBank explained how their cybersecurity analytics architecture supports streaming input, which handles continuous flow of data that comes from various sources in the form of logs and they use this streaming architecture to handle and process complex events.

> “Our streaming architecture provides insights related to cybersecurity incidents by running query analysis against event data and live feeds. The goal is to identify cybersecurity incidents that can cause damage and respond to them promptly.” (Senior cybersecurity analyst, FinBank)

Focal organizations identified SIEM tools as an integral part of cybersecurity analytics architecture and a key enabler of real-time analytics. SIEM tools enable real-time monitoring, search, and analysis of cybersecurity events that can be fed through dashboards to update incident response teams about what is going on across cyber threat landscape. General manager of cybersecurity strategy and governance in FinInsuranceA stated that:

> “The tool that we are using to enable real time analysis in our cybersecurity incident response process is SPLUNK. What it enables us to do is real-time analysis, search and monitoring of cybersecurity events…So, we are able to drill down and monitor in real time using different

> views across our dashboards." (General manager of cybersecurity strategy and governance, FinInsuranceA)

One of the key milestones in developing real-time analytics capability in cybersecurity incident response process is to define the baseline architecture, target architecture and then a transition plan that can guide the focal organizations to reach the desired target architecture. Chief security architect in FinInsuranceB highlighted this milestone and noted that:

> "I think the first thing was setting the base infrastructure and prioritizing the feeds that needed to be consumed into the services based on their value. Some of it was all part of the more detailed roadmap and planning around the SIEM project. So, that was one of the early milestones agreeing on the scope, approach and the desired target architecture for our real-time analytics capability." (Chief security architect, FinInsuranceB)

He further explained that they have added numerous additional components in their existing analytics architecture including data virtualization, service-oriented architecture and in-memory analytics to develop real-time analytics capability in their cybersecurity incident response.

> "We have added several additional components in our analytics architecture to implement real-time analytics such as in-memory analytics, data virtualizations and service-oriented architecture." (Chief security architect, FinInsuranceB)

Thus, the implementation of real-time analytics in typical cybersecurity analytics architecture requires several additional components to enable streaming input and data analysis and complex event processing capability.

4.3.3. Automated Decision-Making

One of the key features and benefits of using real-time analytics in cybersecurity incident response process is that it helps to generate automatic threat alerts and trigger actions based on the business rules. As cybersecurity senior manager in FinBank noted that:

> "We are facing new types of cybersecurity threats every day and the most significant way to combat against them is through intelligent and automated defence mechanism that can quickly identify existing and new threats and then can generate alerts and trigger actions to mitigate them." (Cybersecurity senior manager, FinBank)

The manager of IT and information security in FinInsuranceA explained the goal of cybersecurity solution that can make automated decisions using real-time analytics as follows:

> "The goal is to create an analytics solution that can screen and identify threats, and when a threat is detected trigger automated corrective actions. For example, our advanced threat detection systems automatically generate threat intelligence alerts that are passed to our threat prevention systems for immediate blocking. Likewise, automated alerts that indicate any kind of malicious activity help us to speed up our administrative responses, such as blocking high-risk IP addresses and quarantining at risk systems. This kind of actionable intelligence needed rethinking and even retooling of our cybersecurity infrastructure." (Manager of IT and information security, FinInsuranceA)

According to head of global insider threat detection in FinInsuranceB, cybersecurity incident response process cannot be fully automated and requires the involvement of cybersecurity managers to investigate analyse, and confirm the threats particularly when the threats are dynamic and unpredictable such as malicious insiders theat.

> "Given the sensitive nature of cybersecurity issues, the cybersecurity incident response process cannot be fully automated and security managers still need to investigate and confirm threats, particularly when the threats are internal." (Head of global insider threat detection, FinInsuranceB)

Automation in cybersecurity incident response process also delivers several benefits such as faster decision-making, reduced complexity, fewer human errors, improved knowledge sharing and less duplication to the focal organizations. The general manager of data and analytics in FinBank described the benefits of automated decision making in cybersecurity incident response process as follows:

> "Automation in our cybersecurity incident response process has delivered many benefits such as less duplication, faster decision-making, reduced complexity, improved knowledge sharing, streamlined processes, and fewer human errors." (General manager of data and analytics, FinBank)

Complex event processing feature of real-time analytics enables analysis of streaming data. Based on the business rules, complex event processing systems can trigger an automated response or can generate alerts for cybersecurity incident response teams that can help them to analyse and monitor patterns and trends.

> "We use complex event processing tools to analyse streaming data in real time. Based on the rules, the system can then either generate alerts that our threat hunting team monitors to see patterns and trends or can also trigger automated response." (Head of cybersecurity threat detection and response team, FinInsuranceB)

The focal organizations are using automated response feature of real-time analytics not only in cybersecurity incident response process, but also in other subject areas such as anomaly and fraud detection, as these demand lowest latency response. General manager of cybersecurity risk management in FinBank stated that:

> "Recently, we have added the automated response capability in our security event processing solution. It can execute automated response or actions like flagging, filtering, transforming, and alerting of cybersecurity events as they arrive. A response might be executed based on sophisticated criteria, such as anomaly detection models. We not only use this in our cybersecurity incident detection and response, but also in fraud detection and recommendation, as these demand lowest latency response." (General manager of cybersecurity risk management, FinBank)

He further explained that the implementation of automated cybersecurity incident response is a gradual process. The improvement in the speed with which incident response is implemented is based on the asset value and business need.

> "The progression to automated incident response in real-time is often gradual. What I mean by that is, the improvement in the speed with which we executed the response was improved gradually, such as getting from days to hours to minutes or even seconds. Then, if required further refinement can also be done based on the business need." (General manager of cybersecurity risk management, FinBank)

Thus, automated response is one of the key features of real-time analytics in cybersecurity incident response process. The goal of using automation in incident response is to swiftly detect and respond to cybersecurity incidents. However, the involvement of humans (cybersecurity managers) is critical as the complexity of incident response requires human input during the process of assessing the impact, scope and severity of the cyber-attacks.

4.3.4. On-demand and Continuous Data Analysis

Organizations are using two specific types of real-time analytics (on-demand and continuous) in their cybersecurity incident response process to analyse data from disparate sources. The general manager of data and analytics in FinBank differentiated these two types as follows:

> "Analysis on demand is a reactive approach in which a user or system requests a query to further investigate and understand what is happening right now…whereas continuous data analysis is a proactive approach that alerts users or triggers actions based on the events as they occur." (General manager of data and analytics, FinBank)

The head of cyber threat detection and response team in FinInsuranceA explained how they are using continuous monitoring systems to analyse data, generate alerts and thereby improve their cybersecurity awareness.

> "Our continuous monitoring systems run all day and monitor events as they occur and generate alerts as soon as a threat is detected that needs a response. The response can either come from our incident response team or from the system itself." (Head of cyber threat detection and response team, FinInsuranceA)

A senior cybersecurity analyst in FinBank discussed examples of on-demand and continuous data analysis as follows:

> "Spear-phishing and phishing attacks are the most common attacks we encounter on daily basis. Our tier 1 security analysts are using security monitoring tools to monitor our email servers to detect any phishing attacks. Once an attack is detected by tier 1, our tier 2 security analysts uses threat intelligence tools to further investigate if it is a spear-phishing or phishing attack." (Senior cybersecurity analyst, FinBank)

The director of global cyber forensics mentioned that they use continuous monitoring to learn user activities on their website and thereby enable user and entity behaviour analytics.

> "We continuously monitor our website traffic and user activities on it to detect any changing patterns that do not indicate normal user behaviour." (Director of global cyber forensics, FinInsuranceB)

Continuous data analysis helps focal organizations to monitor cybersecurity events as they occur and proactively detect and prevent incidents before they actually happen. The manager of cybersecurity strategy and governance in FinInsuranceA explains this feature as follows:

> "Real-time analytics helps us to react to cybersecurity threats without any delay…In simple words, what we are doing is continuously analysing cybersecurity events to detect potential threats and prevent incidents before they happen." (Manager of cybersecurity strategy and governance, FinInsuranceA)

He further explained that the analysis of cybersecurity events using continuous monitoring systems enable them to focus on important events that has the potential to cause damage.

> "We use continuous monitoring systems (SIEM) to analyse cybersecurity events in which we do event and log collection and correlation. This helps us to separate real events (incidents) from nonimpact events. In addition, this also helps us to locate and contain cybersecurity incidents." (Manager of cybersecurity strategy and governance, FinInsuranceA)

Finally, the director of global cyber forensics in FinInsuranceB elaborated that they use both on demand and continuous data analysis to combat advanced cybersecurity threats by analysing log data from security systems and integrating external threat intelligence feeds with it to generate comprehensive cybersecurity insights.

> "To combat advanced cybersecurity threats, such as sensitive data exfiltration and zero-day malware, we use both on-demand and continuous real-time analytics to analyse all network traffic, log data from applications, security systems, and network data and also fuse external threat intelligence in real-time." (Director of global cyber forensics, FinInsuranceB)

Therefore, both on-demand and continuous real-time analytics have their time and place within cybersecurity incident response process. Continuous data analysis is more proactive as it alerts the incident response teams with continuous updates in real-time. On-demand data analysis is reactive as it waits for cybersecurity managers to request a query and then delivers insights.

4.4. Real-time Analytics-Enabled Dynamic Capabilities

The aforementioned key features of the real-time analytics capability help organizations to integrate, build, and reconfigure their cybersecurity resources, skills and functional competencies. As a result, these features of real-time analytics capability and their use in cybersecurity incident response process enables three types of dynamic capabilities (real-time situational awareness, dynamic risk assessment, and cyber threat intelligence generation) that helps focal organization to execute dynamic cybersecurity incident response. The details of real-time analytics-enabled dynamic capabilities are given below.

4.4.1. Real-time Situational Awareness

Real-time analytics can not only help organizations to monitor and respond to cybersecurity events as they occur but also help them achieve cybersecurity resilience through real-time situational awareness. The general manager of cybersecurity risk management in FinBank stated that:

> "Having real-time cybersecurity awareness means that we have accurate and timely information related to potential incidents and about our cyber threat landscape." (General manager of cybersecurity risk management, FinBank)

> "Using analytics, we can understand the cybersecurity threats in a broader context…putting business context behind each threat indicator enables us to develop and execute most effective and efficient mitigation strategy." (General manager of cybersecurity risk management, FinBank)

He further explained that real-time situational awareness requires strong coordination and integration between cybersecurity resources.

> "We are also automating data flows and improving collaboration and integration between our security operations centre and threat intelligence teams to improve our cybersecurity awareness. The goal is to make information available as soon as possible to everyone regarding security incidents, vulnerability management, and endpoint security." (General Manager of cybersecurity risk management, FinBank)

A cybersecurity senior manager in FinBank highlighted the importance of sharing cybersecurity related information in a structured way in order to develop situational awareness as follows:

> "Being a senior manager, I need to be aware of not only any particular cybersecurity incident but also of the whole cyber threat landscape. In this aspect, my cybersecurity awareness is both

> global and local. This can only happen if we share cybersecurity related information in a structured way." (Cybersecurity senior manager, FinBank)

The chief security architect in FinInsuranceB explained that real-time situational awareness helps them to separate important signals from the noise:

> "Real-time cybersecurity awareness helps our threat detection team to focus on serious, actual threats and not bogged down in false positives." (Chief security architect, FinInsuranceB)

> The general manager of cybersecurity strategy and governance in FinInsuranceA explained how improving the situational awareness of employees in their organization had a significant impact on reducing the cost and number of security incidents.

> "Through real-time monitoring tools and security awareness programs, we were able to communicate to them [employees] about the security risks they should be cautious towards. This was very important as they [employees] need to know and understand where and how to report any security risk. The information from this improved our overall security posture and reduced the likelihood of incidents significantly." (General Manager of cybersecurity strategy and governance, FinInsuranceA)

The manager of cyber defence centre in FinInsuranceA further explained how they use dashboards to monitor the key information regarding cybersecurity events to maintain awareness of what is happening in their cybersecurity environment.

> "Detecting and understanding potential cybersecurity threats to our business is not enough. Information from monitoring tools and threat intelligence needs to be consolidated and communicated to [cybersecurity] managers…The cybersecurity awareness provided by the consolidated information in the dashboards enable us to understand what's happening and respond to incidents without wasting anytime." (Manager of cyber defence centre, FinInsuranceA)

Furthermore, continuous monitoring systems help focal organizations to improve their situational awareness as it enables monitoring and analysis of cybersecurity events across the network.

> "Because we are using continuous monitoring systems to analyse cybersecurity events across the network, this greatly improves the level of cybersecurity awareness of our cybersecurity managers." (Data analyst, FinBank)

> "To achieve successful continuous monitoring of networks and improve our cybersecurity awareness, both detective and proactive monitoring actions must work together." (Head of global insider threat detection, FinInsuranceB)

The integration and consolidation of information from different cybersecurity systems such as SIEM, log management, intrusion detection and prevention systems with threat intelligence feeds and its analysis using monitoring dashboards is crucial in improving situational awareness of cybersecurity managers. As the general manager of data and analytics in FinBank stated that:

> "We have deployed intrusion prevention, log management and advanced SIEM systems with correlation capabilities to consolidate threat intelligence feeds into monitoring dashboards and alerting systems. The effort that we have put in consolidating this information has resulted in improved situational awareness of activities, users and systems as well as awareness of the attacks being attempted on our networks." (General manager of data and analytics, FinBank)

The manager of cybersecurity strategy and governance in FinInsuranceA explained the importance of employee situational awareness as follows:

> "We monitor the percentage of employee in our organisation that has taken the security awareness programs. If we see that the percentage of completion is small, then the training has not been effective because most of the people have not done it… So that again gives us a key risk indicator which suggests that a likelihood of an event resulting from the poor employee security awareness is higher." (Manager of cybersecurity strategy and governance, FinInsuranceA)

Finally, the analytics driven decision making culture in the focal organizations has resulted in improved situational awareness and that has empowered their cybersecurity managers to make timely and productive decision.

> "Even if we did go through the process of raising an item in our risk register we found that the risk consciousness, the awareness across all of the information systems or assets owners was not such that they are necessarily taking the appropriate timely action to respond with any

> remediation treatment activities that they may have…So, the analytics driven decision making has developed a culture in such a way that we are able to establish a much firmer tone of management intent, much clearer guidelines around what our risk tolerance or risk apatite is, and also being able to deliver meaningful insights that can empower the decision makers to take the appropriate timely actions." (General manager of cybersecurity strategy and governance, FinInsuranceA)

Thus, the key features of real-time analytics capability such as continuous monitoring and timely integrated and consolidated information sharing among cybersecurity resources help organizations achieve real-time situational awareness in cybersecurity incident response.

4.4.2. Dynamic Risk Assessment

Organizations are increasingly adding proactive approaches to respond to cybersecurity incidents in a dynamic way along with reactive approaches to get more visibility into their cybersecurity environment. General Manager of cybersecurity strategy and governance in FinInsuranceA noted dynamic risk assessment as the key component of becoming proactive in cybersecurity incident response:

> "In my own team's roadmap, the priority is to improve the measurement of metrics and report the coverage and effectiveness of our security controls and do dynamic risk assessment by looking at what we call as Key Risk Indicators." (General manager of cybersecurity strategy and governance, FinInsuranceA)

> "Key risk indicators are crucial for dynamic risk assessment as they help in the mitigation and monitoring of risks and facilitate risk reporting". (General manager of cybersecurity strategy and governance, FinInsuranceA)

There are two types of key risk indicators that focal organizations were looking at (1) lag indicators and (2) lead indicators. The manager of cybersecurity strategy and governance explained each of them as follows:

> "What we are looking at is what we call as lag indicators and lead Indicators. So, historically we are very good with lag indicators. We have been able to report on the types of incidents that have happened in the organisation. Lag indicators provide statistics around (a) this is how much spam we received last month, (b) this is the number of desktops that have been affected by malware,

> (c) and this is how many malicious URLs that were accessed. But they are after the event and those are called lag indicators. They tell us something bad that happened which we detected. What lead indicators tells us is how things are working and can give us some information about the future so that we can take pre-emptive actions. So, for example, the lead indicator for us can be the number of people that requested a security exemption to formally be non-compliant with a security policy or standard. This indicates to us that may be our risk appetite is invalid. We need to change our risk appetite or that we need to do more work around awareness or education." (Manager of cybersecurity strategy and governance, FinInsuranceA)

General Manager of cybersecurity strategy and governance in FinInsuranceA further explained the use of lead and lag indicators in dynamic risk assessment through the following examples:

> "A lead indicator for us in vulnerability management is the number of servers that have not been patched in the appropriate service agreed time frames. So, if we are finding that the exposure of period of a server is not being patched is increasing, then that means that our aggregate risk exposure is increasing. We need to raise management awareness that we are becoming more and more exposed on a daily basis and we need to get the appropriate funding or the appropriate management focus to try and to reduce the lag in people patching their servers to demonstrate that they are proactively reducing the risk exposure. Another non-technology one [lead indicator] might be the percentage of people in our organisation that has taken the recent security awareness program. So, if we are having a small percentage of completion then the training has not been effective because most of the people have not done it. So that again gives us a lead indicator to suggest that a likelihood of an event resulting from the poor education is higher because not many people have done the program." (General manager of cybersecurity strategy and governance, FinInsuranceA)

The director of global cyber forensics in FinInsuranceB noted the use of real-time analytics in monitoring and analysing lead indicators as follows:

> "We are definitely more interested in reporting and analysing the lead indicators in real-time that would demonstrate that the organisation is drifting outside of its risk appetite." (Director of global cyber forensics, FinInsuranceB)

Focal organizations also measure and review their risk management capabilities against standard frameworks and industry peers to improve their risk assessment process in a proactive manner.

> "So, by virtue of our teams periodically reviewing and measuring our capabilities against the framework and against our industry peers, we are demonstrating that we are proactively trying to continue to improve our capabilities to stay one step ahead of the threats." (Manager of IT and information security, FinInsuranceA)

When asked about what dynamic cyber risk assessment is, general manager of cybersecurity risk management in FinBank stated that:

> "Dynamic risk assessment is a decision-making process that involves identification, assessment and analysis of risk, and then taking actions that can reduce or eliminate risk in the rapidly changing circumstances of a cybersecurity incident." (General manager of cybersecurity risk management, FinBank)

The general manager of data and analytics in FinBank compared batch processing of data and analytics with real-time analytics. He explained that analytical application that process data in batches deliver historical insights based on lagging indicators, on the other hand the insights generated by real-time analytical platforms deliver insights that are more current and predictive in nature as they are based on leading indicators.

> "If I make a comparison of using batch style analytics with real-time analytics, it may take hours or even days to yield results using batch style analytics. So, our batch analytical applications are very good in delivering "after the fact" insights (lagging indicators). In contrast, the insights that we get from analysing leading key risk indicators allow us to get ahead of the curve." (General manager of data and analytics, FinBank)

Finally, real-time analytics was highlighted as an integral part of dynamic risk assessment process by head of cybersecurity incident response team in FinBank. He also explained that dynamic risk assessment is about decision making which involves analysing and monitoring the risks and threats presented by the cybersecurity attack and providing the actionable information to decision makers in near real-time.

> "By consolidating information from continuous monitoring systems into a dashboard in real-time, our threat hunting team can identify and monitor assets that have higher levels of risk and then respond to threats against these assets appropriately." (Head of cybersecurity incident response team, FinBank)

Thus, real-time analytics enable organizations to do risk assessment in a dynamic way by helping them analyse and monitor the cybersecurity risks and threats using key risk indicators that provide them the timely information regarding risk exposure, emerging risk trends and changes in risk profile of the organization.

4.4.3. Cyber Threat Intelligence Generation

Organizations cannot successfully respond to cybersecurity attacks until they know what threats are coming their way and develop a comprehensive understanding of their cybersecurity threat landscape. That is why cyber threat intelligence generation was identified as another crucial real-time analytics-enabled dynamic capability in focal organizations. General manager of cybersecurity strategy and governance in FinInsuranceA noted that:

> "What we know today about our cyber threat environment is not good enough for tomorrow and that is why traditional cybersecurity approaches and solutions are not sufficient to deal with changing [cybersecurity] environment." (General manager of cybersecurity strategy and governance, FinInsuranceA)

Real-time analytics capability helps focal organizations in cyber threat intelligence generation to better understand what threats are coming their way and how should they respond to them. The director of global cyber forensics in FinInsuranceB explained that as follows:

> "Cyber threat intelligence is the analysed information that helps us understand the capability, opportunity and intent of malicious actors…Intent reflects the desire of a malicious actor in targeting our assets, capability is the means used in the malicious activity, and opportunity is the vulnerabilities that a malicious actor can exploit…analysing this information is extremely important and cyber threat intelligence gives us this information". (Director of global cyber forensics, FinInsuranceB)

The head of cyber threat detection and response team in FinInsuranceA explained that in comparison with traditional cybersecurity solutions and methods, real-time analytics helps them to continuously monitor different types of cybersecurity threats and get specific information regarding current or potential attacks that can cause any damage.

> “Our cyber defence and response team is proactively taking and analysing that information and then translating that into changes in our security services to try and provide a counter measure before we actually see those attacks hit our enterprise.” (Head of cyber threat detection and response team, FinInsuranceA)

The general manager of cybersecurity strategy and governance in FinInsuranceA explained that the ability to analyse data and extract anomalies that may indicate an active threat in the network is another example of identifying cyber threats using real-time threat intelligence:

> “On an operational point of view, we also have processes where we are proactive in addressing the [cyber] threat landscape. We have continuous threat intelligence feeds from networks in which we use analytics to analyse what is happening and detect anomalies.” (General manager of cybersecurity strategy and governance, FinInsuranceA)

He further elaborated that they use threat intelligence feeds to understand what is happening across their cyber threat landscape and participate in threat intelligence sharing communities to learn from their peers.

> “We have threat intelligence feeds in which we use analytics to analyse what is happening and we also participate in threat intelligence sharing communities to learn from our peers.” (General manager of cybersecurity strategy and governance, FinInsuranceA)

The general manager of data and analytics in FinBank echoed how real-time analytics has enabled them to continuously monitor and analyse key risk indicators and detect anomalous behaviours and patterns to identify different types of cyber-attacks such as phishing, malware, password attacks and ransomware. Manager of cybersecurity strategy and governance in FinInsuranceA discussed an example of how their managed services analytics team uses real-time threat intelligence to detect and respond to email malware as follows:

> “We had multiple incidents where because we have got access to analytics, that we were able to contain the malware infection through emails. Our managed services provider has analytics visibility across multiple clients. As we are one client and they can analyse to see if it is a zero-

> day attack. It is an email malware, but we have actually seen this trend across multiple clients. So, we get an early warning for that. We have got may be 20 such emails and we can pull those from the inbox. So, it helps our response process. Our response is to the point where we can contain it so that there is no impact. This is because we now know that email is a bad email and we can now actually withdraw that from the user mailboxes before they even open the email and click the attachment."

Finally, focal organizations also use cyber threat intelligence feeds to continuously improve the efficiency and effectiveness of their cybersecurity incident response process. Cyber threat intelligence also helps them to understand the capabilities, motives and likely action of the attackers. General manager of cybersecurity risk management in FinBank stated that:

> "We use cyber threat intelligence feeds to continuously improve the effectiveness of cyber security threat analysis process. So, for example while we are investigating a cybersecurity incident, having access to cyber threat intelligence can be very useful in understanding attacker's capabilities, motives and likely actions." (General manager of cybersecurity risk management, FinBank)

Thus, focal organizations have been able to create real-time cyber threat intelligence on both external and internal cyber threats using real-time analytics capabilities that helps them to detect cyber-attacks as they happen and respond to them in a timely manner.

4.5. Dynamic Cybersecurity Incident Response Strategies

The most challenging part of cybersecurity incident response process in many organizations is the timely and accurate detection and assessment of possible cybersecurity incidents, and then selection and execution of the most appropriate response strategy. As the number of cyber-attacks and threat actors continues to increase and the attack vectors have grown and migrated to more targeted and sophisticated advanced persistent threats, fraud, insider attacks and cybercrime, the traditional cybersecurity strategies and solutions are not sufficient to deal with this new cyber threat landscape.

The focal organizations are responding to this dynamic threat environment that encompasses both predictable and unpredictable threats by executing three different dynamic cybersecurity incident response strategies including active reconnaissance, continuous monitoring and active defence that are useful to detect and respond to dynamic cybersecurity attacks:

(1) Active reconnaissance (leveraging threat intelligence feeds to detect cybersecurity incidents during the reconnaissance phase, before the organization is actually been attacked);

> "Our incident response team uses cyber threat intelligence feeds to understand the procedures, tactics and techniques of the attackers and can stop some attacks by degrading or disrupting their efforts. In this way, cyber threat intelligence helps us in detecting an incident during the reconnaissance phase, that is before we have actually been attacked." (General manager of cybersecurity risk management, FinBank)

> "Using [cyber] threat intelligence, our incident response team tries to understand the methodology, intent and focus of the attack and in some cases, can detect an incident during the reconnaissance phase." (General manager of cybersecurity strategy and governance, FinInsuranceA)

(2) Continuous monitoring (continuously monitor the attack by gathering more intelligence about both attacker and attack through passive means); and

> "We need clear visibility into data regarding system configuration and patch levels, device behaviour, vulnerabilities, and overall cybersecurity state. The information regarding the cybersecurity state and vulnerabilities for these systems needs to be continuously monitored and correlated to demonstrate security compliance when required." (Cybersecurity senior manager, FinBank)

> "Getting an understanding of what to monitor, where to monitor and how to monitor is very important. Continuous monitoring does not mean that everything including all applications, systems, end points, networks, security processes and infrastructure needs to be monitored everywhere and all the time. Therefore, it is very important to determine what needs to be monitored and set monitoring policies around those needs." (Chief security architect, FinInsuranceB)

(3) Active defence (to defend the attacked enterprise assets through active means by harnessing more intelligence about the attack and pacify the attacker infrastructure).

> "Sometimes people commonly misunderstand proactive may necessarily be equal to protective or preventative and yet if you talk to a lot of experts in the cybersecurity industry current

> thinking basically says that you can assume that at some point you might actually be compromised, or you have breach of some sort. So rather than just saying by putting all your investment in a preventative approach, you can still be proactive in boosting your detection and response capabilities so that when something happens you know that sooner, which means you can decrease the impact and then also recovery and all that is well planned so that you cater better in reduction of impact." (Manager of cybersecurity strategy and governance, FinInsuranceA)

The head of cybersecurity incident response team in FinBank explained how they have designed their cybersecurity incident response strategy around the cyber kill chain model that helps them to focus on the different stages of an attack and thereby execute appropriate response strategy:

> "We have designed our cybersecurity incident monitoring and response plan based on cyber kill chain model that identifies sequence of stages which an attacker must pass through to reach the desired goal. The incident response type and execution of recommended actions from the playbook are dependent on the stage where attack was detected". (Head of cybersecurity incident response team, FinBank)

He further elaborated with examples of different response types and the importance of cyber threat intelligence in cyber-attack investigation as follows:

> "Sometimes denial of service attacks can be a diversion from another serious attack and they are hard to detect. Our SOC team actively monitors and investigates all the relevant activity and applies threat intelligence before taking any counter attacking actions…similarly multi stage attacks like APT's are the most difficult to defend against. Therefore, it is crucial for them [SOC team] to analyse the events in a larger context by incorporating the latest threat intelligence updates." (Head of cybersecurity incident response team, FinBank)

A cybersecurity senior manager in FinBank explained the importance of conducting triage in early part of a cybersecurity incident investigation:

> "The primary role of tier 1 analysts in the SOC team is to conduct triage in early part of an incident investigation. They [security analysts] need to classify each event quickly and then prioritize them and escalate critical events that require additional investigation to appropriate personnel." (Cybersecurity senior manager, FinBank)

The general manager of cybersecurity risk management in FinBank highlighted the importance of situational awareness in identifying and responding to cybersecurity incidents:

> "Situational awareness is very important for strong incident response as we cannot consider every cybersecurity incident as a cyber security attack. Some incidents can be easily detected such as malware infections, whereas advanced targeted attacks may occur over a long period of time and may remain undetected for many days, months and even years." (General manager of cybersecurity risk management, FinBank)

The director of global cyber forensics in FinInsuranceB explained how they are using cyber threat intelligence to understand the focus, methodology and intent of cyber-attackers and detect cybersecurity incidents in the reconnaissance phase as follows:

> "Using [cyber] threat intelligence, our incident response team tries to understand the methodology, intent and focus of the attack and in some cases, can detect an incident during the reconnaissance phase". (Director of global cyber forensics, FinInsuranceB)

A cybersecurity senior manager in FinInsuranceA explained how they use analytics to generate cyber threat intelligence that in turn improves their cybersecurity detection and response capability:

> "To improve our detection and response capabilities, we started collecting and analysing events data from as many sources as possible to generate threat intelligence; combining that as a superset of data and applying some types of rules to gain insight into what is an actionable information. Not just collecting data for the sake of it but trying to determine whether there were events taking place in the organisation that may constitute a breach or a potential breach that would require further investigation and response." (Cybersecurity senior manager, FinInsuranceA)

Thus, the dynamic capabilities enabled by real-time analytics including cyber threat intelligence generation, dynamic risk assessment and real-time situational awareness together play a critical role in shaping dynamic cybersecurity incident detection and response strategies. These capabilities in turn help focal organizations to execute dynamic cybersecurity incident response strategies and thereby respond to dynamic cyber threat environment in a swift, flexible, innovative, effective and proactive manner.

4.6. Supporting Factors

The ability to develop real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies discussed above was fostered by several cybersecurity incident response process factors as well as the essential characteristics of analytical capability.

4.6.1. Cybersecurity Incident Response Process

The supporting factors related to cybersecurity incident response process that facilitate the development of real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies using real-time analytics include incident response process maturity and collaboration among different stakeholders.

First, a mature incident response process which has been designed to support real-time analytics enables organizations to evaluate their state of readiness in responding to cybersecurity incidents in a swift and effective manner. Specifically, the level of maturity of incident response process in people, process, technology and information determines the way in which they respond to different types of cybersecurity incidents. The general manager of cybersecurity strategy and governance in FinInsuranceA noted that:

> "Identifying what our current level of capability maturity is helps us to identify what our gaps are. We can then formulate our strategy to fill these gaps and improve our capability for cyber security services over time. We translate that into an actionable roadmap of investment in technology, processes, people and skills development to try and achieve that outcome to continuously improve our detection, protection, response and recovery capabilities to protect our information systems and assets." (General manager of cybersecurity strategy and governance, FinInsuranceA)

The manager of cybersecurity strategy and governance in FinInsuranceA further explained how they use an industry cybersecurity framework to measure their capability maturity level, identify the gaps and then devise a strategy to fill the gaps as follows:

> "We are maturing our capabilities against an industry recognised framework and in this case, we use the NIST cyber security framework. Our way of being proactive is to do the self-assessment using this framework. The framework is just a tool that translates the commonly accepted best practice into a meaningful context. So, we use the framework just as a tool to

> measure our capabilities maturity level and the coverage of our capabilities to find the gaps. We then take those gaps and use them to determine what our strategy needs to be to fill these gaps." (Manager of cybersecurity strategy and governance, FinInsuranceA)

Second, collaboration among different stakeholders involved in the incident response was considered crucial for the development of analytical capabilities in incident response process by the Director of global cyber forensics in FinInsuranceB.

> "The first step we did to improve the analytical capability in incident response process was to collaborate and establish a relationship with our analytics team. We started embedding some of their practices and processes and even using some of their services. By building stronger relationships and leveraging the capabilities of analytics team, we were able to improve and drive our decisions based on the data." (Director of global cyber forensics, FinInsuranceB)

The general manager of cybersecurity strategy and governance in FinInsuranceA emphasized that collaboration with threat intelligence sharing communities also plays a vital role in becoming proactive and responding to cybersecurity attacks in a dynamic manner:

> "We also participate in threat intelligence sharing communities. So, through our participation in these forums and collaboration on threat intelligence feeds that we have, we can also analyse and then take proactive counter measures before those attacks are actually experienced by our organisation. So, on the daily basis we are getting feeds on things like trustworthy IP addresses, and domain names. We are getting feedback from our peers across industry around phishing campaigns and new emerging malware. Then our cyber defence and response team is proactively taking and analysing that information and then translating that into changes in our security services to try and provide a counter measure before we actually see those attacks hit our enterprise."

4.6.2. Characteristics of analytical capability

The following two essential characteristics of analytical capability facilitate the development of real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies: self-service analytics and key risk indicators. First, the self-service feature of real-time analytics allows decision makers to explore data and interact with it by creating their own reports and dashboards. The general manager of data and analytics in FinBank stated that:

> “Self-service analytics is definitely a useful approach to make data-driven decision in real-time, but it is something that comes with at a very high maturity level”. (General manager of data and analytics, FinBank)

The head of cybersecurity incident response team in FinBank explained the critical role of self-service analytics in their cybersecurity incident response process as follows:

> “Self-service analytics is one of the tactics that our threat hunting team use to deal with cybersecurity threats. Without this [self-service] capability, we need to rely on data scientists to do analysis and create reports.” (Head of cybersecurity incident response team, FinBank)

Second, defining and analysing the right key risk indicators is critical as they play an important role in incident reporting and in identifying emerging threats.

> “Being able to measure the cybersecurity operations or processes using key risk indicators is crucial. So, until we get to a point where we have meaningful key risk indicators that are measurable, comparable, informational and predictable, we cannot get full benefit out of analytics.” (Manager of cybersecurity strategy and governance, FinInsuranceA)

Finally, real-time tracking of key risk indicators helps organizations to better understand their cybersecurity environment.

> “The immediate opportunity that we see in applying more advanced analytics techniques is to develop more efficient and robust risk assessment models that enable the tracking of key risk indicators in real-time to track the changes in risk profile and monitor effectiveness of security controls.” (Chief Security Architect, FinInsuranceB)

4.6.3. Challenging Factors

It should be noted that the focal organizations also faced several potential challenges in developing real-time analytics enabled dynamic capabilities and in executing dynamic incident detection and response strategies. The narrative that follows explains in detail how the studied organizations addressed these challenges.

First, there are multiple stakeholders involved in the cybersecurity incident response process who have different priorities. Getting the stakeholders buy-in to dedicate the required resources and budget in making the incident response analytics-driven can be challenging. The general manager of cybersecurity strategy and governance in FinInsuranceA noted that:

> "If we went to the board and said that we want to spend some money to invest on some technology or product to develop a capability and the project is not mandatory [compliance requirement], getting their support and involvement is very difficult. That is why we need to convince them regarding why this project is of high priority so that they can give required budget and resources (General manager of cybersecurity strategy and governance, FinInsuranceA).

A similar concern was raised by a cybersecurity senior manager in FinBank:

> "If the stakeholders do not understand the goals of project and are not committed to achieve them as the security team, this means that the stakeholders do not fully understand "why" behind the project." (Cybersecurity senior manager, FinBank)

The focal organizations addressed this challenge by educating the stakeholders regarding the need for the project with evidence from the industry and case studies of the organizations that were attacked and did not know about the breach for considerable amount of time. The general manager of cybersecurity strategy and governance in FinInsuranceA noted that:

> "We were able to show just broad evidence of from cross industry that there are many organisations that are ill prepared in been able to detect and respond to security breaches. In addition, we showed case studies of organizations that had been breached but had not discovered the breach for some time and then not particularly well prepared and been able to respond when they were aware that a loss event had taken place." (General manager of cybersecurity strategy and governance, FinInsuranceA)

The manager of cybersecurity strategy and governance in FinInsuranceA further explained that:

> "The approach we take in communicating with key stakeholders is helping articulate their shared understanding of what the problem is, by providing some facts whether they are internal facts or broader industry weight of evidence, helping them understand what the options are and proposing or making a recommendation to our key stakeholders on what the solution may be. Now obviously when we are talking about board level directors, we are not talking at a deep technology level. We are basically talking about the capabilities that we want to develop and

> how that helps support our business." (Manager of cybersecurity strategy and governance, FinInsuranceA)

Second, misaligned analytics and cybersecurity skills can be a challenge for organizations when they embark upon the journey of adding analytical capabilities in cybersecurity incident response. The manager of IT and information security in FinInsuranceA highlighted the mismatch between their existing and required cybersecurity and analytics skills as follows:

> "We have got people from the security infrastructure background and from the threat intelligence background. That does not necessarily mean that they are strong data analysts." (Manager of IT and information security, FinInsuranceA)

Similarly, the head of global insider threat in FinInsuranceB explained that they need personnel that have strong analytical and communications skills and business acumen so that they can understand their business and then analyse cybersecurity threats effectively:

> "In this day and age, we really need a person that has very strong analytical and communication skills, and business acumen. Someone that actually understands our business and cybersecurity processes and has the ability to analyse data effectively." (Head of global insider threat, FinInsuranceB)

The focal organizations addressed this issue by hiring and/or training their analytics and cybersecurity personnel:

> "So, we have got three choices here. One is we upskill and teach those people that come from traditional security background that how to understand and utilise the more advanced information analyst capabilities. Second, we have to hire-in the people that come from the information analytics background and then teach them security; and third, we can actually go to a Vendor if we really don't have any expertise and even it is temporarily while we build our own capabilities in this area. That is buy the skills rather than build the skills. Just hire someone and get things done and develop the capabilities and then transition (General manager of cybersecurity strategy and governance, FinInsuranceA);

> "To me it makes more sense to actually get data analytics people and educate them to security vs educating security people to do data analytics." (Manager of cybersecurity strategy and governance, FinInsuranceA);

> "I would agree with that. I think that would be the better outcome because they would also then be able to use some of that information that they could garner from the security landscape and then feed that back to the rest of the business to create value (General manager of cybersecurity strategy and governance, FinInsuranceA).

Third, understanding the role and use of technology in building analytical capabilities in cybersecurity incident response can be a challenge for organizations. The manager of cybersecurity strategy and governance in FinInsuranceA noted that:

> "The problem that I see from day to day basis is that, the assumption that the SIEM engine is a silver bullet and that sometimes we may have some weak controls compared to other controls and then the design might be that we ship the logs off to the SIEM so that is fine…shipping the logs off to the SIEM is one thing and what about all the analytics and all the tuning of the analytics behind that to actually get some meaningful information (fine tuning to get insights is a major challenge), what happens is they just say I have sent the logs to the SIEM and the job is done." (Manager of cybersecurity strategy and governance, FinInsuranceA)

He further explained how they addressed this challenge as follows:

> "In terms of how we addressed that challenge, it happens quite often, and it is mainly due to ignorance or due to some lazy short cuts. So, it is just educating the people in the design of these applications to fully understand the capabilities of the products and not to entirely rely on one control and there are other things which are also important, and we need to consider them as well to implement a full range of controls." (Manager of cybersecurity strategy and governance, FinInsuranceA)

The Senior cybersecurity analyst in FinBank reported that:

> "SIEM products in the industry have a reputation of being very expensive and reason why they are expensive is because of the charges on data ingestion model. So, it's not just the case of just throw everything at the ingestion and it is you have to actually choose the data you send to it.

> Therefore, there is an opportunity that we miss events in trying to save money and in doing so we are throwing away the data we actually needed." (Senior cybersecurity analyst, FinBank)

Finally, the general manager of data and analytics in FinBank highlighted the challenge in implementing real-time analytics applications as follows:

> "The biggest challenge in implementing real-time analytics applications is achieving the low response times and high availability. These applications need to handle large quantity of data of different types and still return answers to queries within just seconds." (General manager of data and analytics, FinBank)

The focal organizations addressed this challenge by storing the raw data in big data platform. The manager of cybersecurity strategy and governance in FinInsuranceA explained that as follows:

> "So, instead of just deleting the data after 30 or 90 days in our SIEM as we can only store that much data. Instead of just throwing it away, it goes into our big data platform and as well out of the security analytics from big data platform can go back into SIEM basically enrich the data that is in our SIEM to detect anomalies or potential breaches more easily." (Manager of cybersecurity strategy and governance, FinInsuranceA)

4.7. Enterprise Security Performance

This section examines how focal organizations reaped strategic and economic benefits and improved their overall enterprise security performance as a result of developing real-time analytics enabled dynamic capabilities and dynamic incident response strategies using real-time analytics.

The manager of cybersecurity strategy and governance in FinInsuranceA stated that:

> "The concept of cybersecurity risk management is so that we can operate our business processes in a manner with some assurance that we can actually be very confident in doing our daily business operations. The analogy is like where you have brakes on a car, it is actually the brakes that are there to allow you to go faster, it is not to slow you down. So, the benefit of using analytics is that we can actually manage our risks appropriately and we can have the confidence to innovate and operate our business processes in a manner that they can be very effective and efficient." (Manager of cybersecurity strategy and governance, FinInsuranceA)

The general manager of cybersecurity strategy and governance in FinInsuranceA explained that real-time situational awareness and dynamic risk assessment enabled by real-time analytics capability significantly improved their cybersecurity awareness both at tactical and operational level:

> "Using analytics, we are improving our security awareness and that is changing the perception that risk management is a valuable capability in the organisation and not what we call a handbrake on the happiness." (General manager of cybersecurity strategy and governance, FinInsuranceA)

He further elaborated that:

> "The key point for us with real-analytics is the thing that is really important is being able to change some of our decisions from experience and intuition to fact very quickly. That is the critical piece." (General manager of cybersecurity strategy and governance, FinInsuranceA)

> "So, what we are doing is turning our cybersecurity risk management and incident response capability into it is almost like an opportunity, it is the upside instead of the downside, so if we have not managed our risks appropriately we would not have availed ourselves the business opportunities. We do not have the confidence of saying we have millions of customers if we don't have appropriate risk management controls and how we manage our data." (General manager of cybersecurity strategy and governance, FinInsuranceA)

The General manager of cybersecurity risk management in FinBank noted that real-time analytics helped them to handle cybersecurity threats in a proactive manner as follows:

> "Real-time analytics to us is like an early warning system. It helps us to identify what the next credible or significant threat to us might be. We can then take proactive approach and implement additional controls to prevent them from happening. So, it is managing the risk in a proactive way so that it does not become an issue." (General manager of cybersecurity risk management, FinBank)

He further explained that:

> "I think we have started getting real benefits of using analytics in our cybersecurity incident response in last 12 months. We also had the managed service, I mentioned that we have got an external service provider that has been doing some of the analysis for us. We have been able to

> use that information to better inform ourselves around what our gaps are. What our weaknesses are? And I can say in last 3 years we have got an evidence that we have been able to use analytics to proof a gap. And invest in a security controls that have reduced our security exposure or reduced the number of incidents that we have seen." (General manager of cybersecurity risk management, FinBank)

Manager of cybersecurity strategy and governance in FinInsuranceA also highlighted that the use analytics has helped them to develop more efficient and robust user access models and thereby improve their access management:

> "I think the real benefits that we are seeing from cybersecurity analytics right now like immediate term future is helping us our access management. So, our immediate opportunity that we see in applying more advanced analytics techniques is to try and develop more efficient and robust access models. That will then help us progressively reduce our risk of thing like fraud or accidental disclosure of information." (Manager of cybersecurity strategy and governance, FinInsuranceA)

The chief security architect of FinInsuranceB provided an example of how the use of real-time analytics in the right manner can help organizations to gain economic benefits as follows:

> "Organizations who invest in the analytics and do it the right way, of course they can lower their cost. So, if an organization is spending 25% of their budget in dealing with security incidents, breaches and penalties versus another organization that is only spending 10% because they are using the right tools and analytics to prevent incidents, breaches and not paying penalties. That means they already have economic benefit over their competitors." (Chief security architect, FinInsuranceB)

When asked about the role of analytics in improving overall enterprise security performance, the manager of cybersecurity strategy and governance reported that:

> "It depends. If it is the commodity analytics then no. I will put it this way, if we don't invest in analytics we cannot improve our security [performance] and we are at a competitive disadvantage. I think that our peer organisations will all be making similar investments in such technology to improve their security performance and if we don't, then we are at competitive disadvantage." (Manager of cybersecurity strategy and governance, FinInsuranceA)

General manager of cybersecurity strategy and governance in FinInsuranceA explained that using analytics to improve cybersecurity is also a demand from the customers and it helps them to gain their trust:

> “I don’t think analytics is something we will market as a differentiator because for our customers, we are supposed to do that anyway. So, I think it is more of a case of just a necessity for us to business… One thing that is worth calling out is insurance is a trust product. We are a trust business. So, you trust us with a lot of information. You have to tell me a lot about you and your life so that I can help protect you. It is a necessary part of our business that we maintain that trust. One of the ways that we maintain that trust is by protecting the information that you gave to us is using analytics.” (General manager of cybersecurity strategy and governance, FinInsuranceA)

Finally, head of cybersecurity incident response team at FinBank identified two critical components that drive the overall cost in incident response process and explained that:

> “If we analyse the cybersecurity incident response process carefully, there are two critical components that drive overall cost in the incident response process, (1) once the attacker first gain access in the network, how long does it take to detect the intrusion; and (2) Once we have detected the intrusion or incident, how quickly can we execute a response and remediate the incident. Real-time analytics helps us in addressing both of these questions by reducing the time it takes to detect and respond to cybersecurity incidents and that can also lead to cost savings and better protection of data.” (Head of cybersecurity incident response team, FinBank)

In summary, the use of real-time analytics to develop real-time analytics enabled dynamic capabilities and dynamic incident response strategies at the focal organizations of this study’s investigation has helped them to improve their overall enterprise security performance by realizing economic benefits in terms of reducing the cost and time to detect and respond to cybersecurity incidents and strategic benefits in terms of building customer trust, improving security awareness and handling cybersecurity incidents proactively.

4.8. A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility

Up to this point, the aforementioned narrative described how focal organizations used real-time analytics to develop real-time analytics enabled dynamic capabilities and dynamic incident response strategies that helped them to improve their overall enterprise security performance. Combining these insights with extant literature informs a framework of dynamic cybersecurity incident response, as depicted in Figure 4-2 (see next page). Incident response can be considered dynamic as organizations apply real-time analytics to develop situational awareness and cyber threat intelligence regarding potential threats and then execute an appropriate incident response strategy before the threats become significant. The narrative that follows further develop this framework in more depth.

Cybersecurity threat landscape is constantly evolving, and organizations are increasingly exposed to more sophisticated attacks such as insider attacks, APTs, cybercrimes and fraud. Traditional security approaches and solutions are not sufficient to deal with today's dynamic threat environment. Scholars have proposed the combination of prevention, detection and response approaches to deal with both predictable and unpredictable cybersecurity threats. Ultimately, whatever response strategy is chosen by the cybersecurity executives, it must be agile and timely so that it can influence the outcome.

The data in this study suggests that one way to achieve agile and rapid incident response is by quickly going through the value workflow of business analytics. The value workflow of business analytics can be described as a simple process of turning data into insights, analysing the insights in a specific context to make them meaningful, and then taking decision based on meaningful insights that can create value (Eckerson 2012; Sharma et al. 2014). As Figure 4-2 depicts, real-time analytics capabilities, real-time analytics enabled dynamic capabilities, and dynamic incident response strategies help organizations to improve their incident response agility by instilling the value workflow of BA in their incident response process and thereby enhance the overall enterprise security performance.

Turning data into insights: The first step in value workflow of business analytics is to collect data from relevant source systems and then analyse the data to understand what is happening in cyber threat landscape in real-time. As Figure 4-2 depicts, the data from this study revealed four key features of real-time analytics capability in cybersecurity incident response process including real-time context, supporting architecture, automated decision making, and on-demand and continuous data analysis

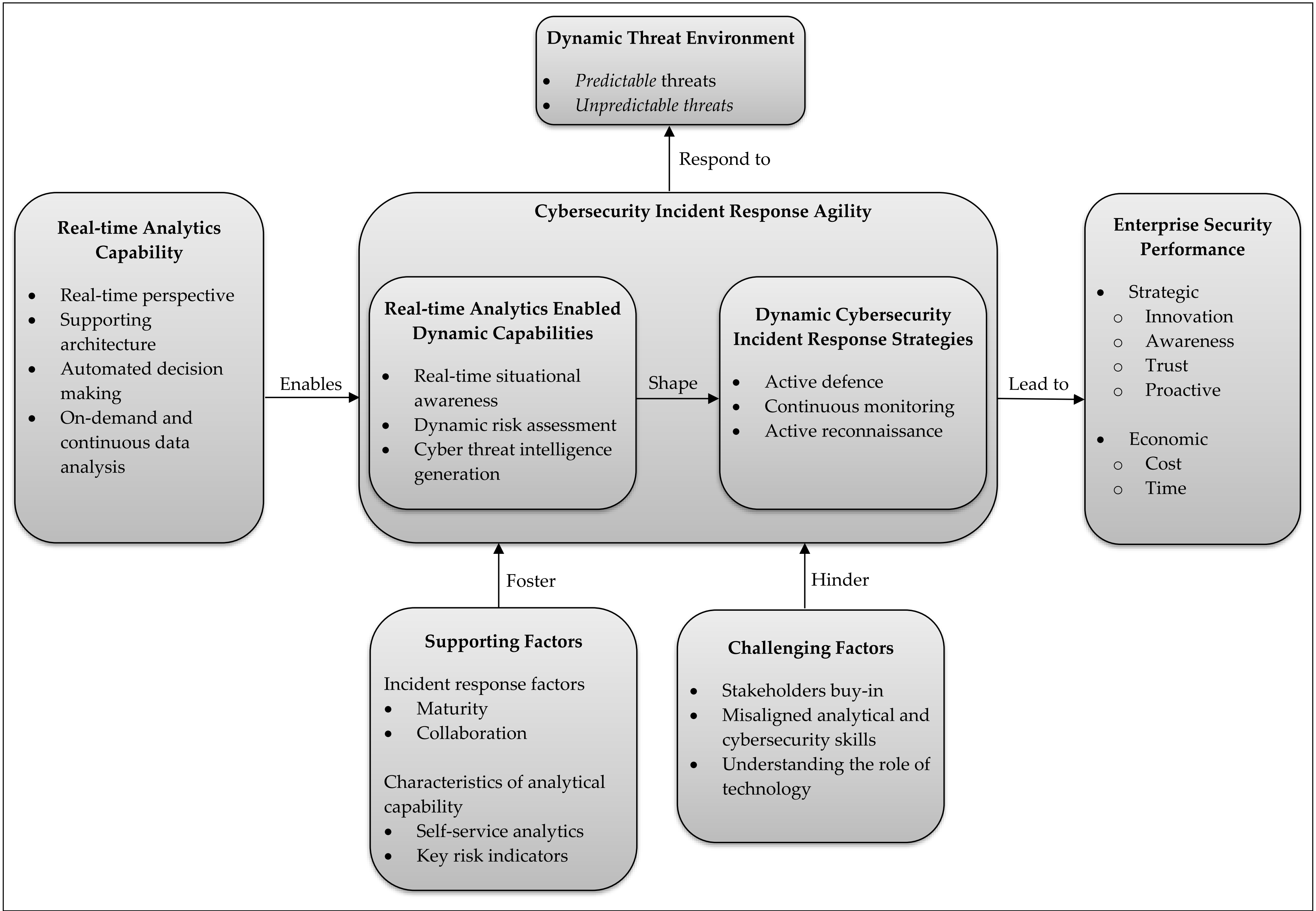

Dynamic Threat Environment
• *Predictable* threats
• *Unpredictable threats*
Respond to
Real-time Analytics Capability
• Real-time perspective
• Supporting architecture
• Automated decision making
• On-demand and continuous data analysis
Enables
Cybersecurity Incident Response Agility
Real-time Analytics Enabled Dynamic Capabilities
• Real-time situational awareness
• Dynamic risk assessment
• Cyber threat intelligence generation
Shape
Dynamic Cybersecurity Incident Response Strategies
• Active defence
• Continuous monitoring
• Active reconnaissance
Lead to
Enterprise Security Performance
• Strategic
○ Innovation
○ Awareness
○ Trust
○ Proactive
• Economic
○ Cost
○ Time
Foster
Hinder
Supporting Factors
Incident response factors
• Maturity
• Collaboration
Characteristics of analytical capability
• Self-service analytics
• Key risk indicators
Challenging Factors
• Stakeholders buy-in
• Misaligned analytical and cybersecurity skills
• Understanding the role of technology

Figure 4-2. A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility

that provide organizations the visibility to understand and generate insights regarding what is happening in their cybersecurity environment.

A key insight from these data depicts how incident response teams defined the real-time perspective and used the supporting architecture to extract data from relevant sources such as security software and logs to consolidate and analyse it and then present it in useful formats for decision making. The real-time perspective is the timeframe within which incident response teams need to deliver a response to cybersecurity incidents before they can cause any damage. Automated decision making is critical to generate automatic threat alerts and trigger actions based on the business rules. As the data shows, by automating event analysis and their classification across cyber kill chain, incident response teams were able to prioritize the incidents for effective response.

Real-time analytics capability provides two types of data analysis in real-time (1) On-demand and (2) Continuous (Russom et al. 2014). On-demand real-time analytics waits for the systems or users to request a query and then the analytical results are delivered. As the data shows, the incident response teams used on-demand data analysis to pull data from communication mediums to analyse different types of phishing attacks. Continuous real-time analytics is more proactive and alerts users or triggers responses as events happen (Russom et al. 2014). Incident response teams used continuous real-time analytics to monitor user activities in order to detect any anomalies or changing patterns.

Therefore, both on-demand and continuous data analysis allow incident response teams to rapidly observe attacks for monitoring and analysing their progression. Cybersecurity incidents are not standardized and all of them exhibit different characteristics. The more the incident response teams observe what is happening across their cybersecurity environment using real-time analytics, the more they can understand the cybersecurity threats and thereby can be more successful in their cybersecurity incident detection and response.

Analysing the insights in a specific context: All the insights that incident response teams collect during the first step is crucial to detect cybersecurity events that require immediate investigation. However, information without the context of what the attack means is not enough for a comprehensive incident response. During the analysis phase, the incident response teams tries to understand what the attack means in a broader context, for example both in the context of the organization and in the context of the threat intelligence community.

As Figure 4-2 depicts, this study identified three real-time analytics enabled dynamic capabilities including real-time situation awareness, cyber threat intelligence, and dynamic risk assessment that organizations in this study developed to gain contextual information regarding cybersecurity incidents. Real-time situational awareness enabled incident response teams to understand the scope and impact of the attack so that they can orient their response strategies against the attack specific tools and tactics employed by the attacker. With dynamic risk assessment, incident response teams continuously monitored the key risk indicators to analyse the cybersecurity events in the context of other activities across the cybersecurity threat landscape and thereby identify the related events and establish a timeline. Real-time cyber threat intelligence feeds provided incident response teams both local and global information regarding cyber threats so that they can better understand the source of the threats and the extent and impact of the damage.

Therefore, the first two phases of the value workflow of BA emphasize on continuous monitoring and analysis of cybersecurity threats. During these two phases, incident response teams need to collect and analyse all relevant data related to cybersecurity threats and then place it in the context of local and global risks to generate meaningful insights that can help them to make the best decision possible.

Decision to value: During the first two phases, incident response teams use real-time analytics and real-time analytics enabled dynamic capabilities to generate the meaningful cybersecurity threat intelligence insights. The final decision and execution of appropriate incident response strategy based on this intelligence needs to happen in this phase. Cybersecurity incident response decisions often involve security executive's input, so it is crucial that incident response teams provide these executives the insights they need regarding cybersecurity incidents quickly and efficiently.

In this phase, incident response teams provide all the consolidated insights to the key decision makers together with possible response strategies so that they can decide quickly. This information allows them to select and execute the optimum response strategy that meets the organizational goals. As the Figure 4-2 depicts, the dynamic incident response strategies used by the incident response teams include (1) active reconnaissance (leveraging threat intelligence feeds to detect cybersecurity incidents during the reconnaissance phase, before the organization is actually been attacked); (2) continuous monitoring (continuously monitor the attack by gathering more intelligence about both attacker and attack through passive means); and (3) active defence (to defend the attacked enterprise assets through active means by harnessing more intelligence about the attack and pacify the attacker infrastructure).

The last step is to implement the response plan selected in the decision phase. If the incident response is successful, then it may contribute towards improvement of overall enterprise security performance by delivering strategic and economic benefits.

The following example described by Senior Cybersecurity Analyst in firm A illustrates how their incident response team detect and respond to different types of phishing attacks by quickly going through the value workflow of BA. He explained that the most common type of cybersecurity incidents their organizations encounter on daily basis are spear-phishing and phishing attacks. The security analysts in tier 1 of their SOC team use security monitoring tools to continuously monitor and analyse the data from email servers to generate insights related to phishing attacks (data into insight). As soon as a phishing attack is detected by tier 1, their tier 2 security analysts use threat intelligence tools to understand what the attack means in a broader context and further investigates if it is a spear-phishing or traditional phishing attack. Tier 2 then classifies the events and activities related to the incident across cyber kill chain (an industry standard) and prepares the incident investigation reports (analysing the insights in a specific context). Tier 3 security experts then review the incident discovery and assessment reports and quickly decides on a plan of action. Finally, the most suitable response plan is executed, and they improve the incident response process and procedures based on the lessons learnt (decision to value).

This study therefore resulted in the crucial insight that the main goal of incident response team is to provide both a high-level of cyber situational awareness to understand and detect cyber-attacks as well as a rapid, flexible, innovative and effective response capability to minimize the harm from cyber-attacks. Real-time situational awareness, dynamic risk assessment and cyber threat intelligence are the real-time analytics enabled dynamic capabilities that infuses swiftness, flexibility and innovation (agile characteristics) in incident response process and thereby shape dynamic incident response strategies. Improved IR agility provides organizations with a unique opportunity to quickly detect the cyber-attacks and respond to them in diverse ways.

In summary, instilling the value workflow of BA in cybersecurity incident response process provides a unified framework which brings people, process, and technology together in such a way that enables incident response teams to not only improve agility but also transition from a reactive approach of responding to cybersecurity threats, to a proactive approach of hunting for threats where likely attacks are identified and managed or minimised before they can cause any damage.

4.9. Summary

This chapter presented an illustrative story of cybersecurity incident response units of FinBank, FinInsuranceA and FinInsuranceB, and analysed their use of real-time analytics in the cybersecurity incident response process. All these organizations experienced dynamic cyber threat environment characterized by the dynamic, sophisticated and evolving nature of cybersecurity threats (predictable and unpredictable) such as advanced persistent threats, insider data theft, zero-day attacks, phishing and spear phasing attacks.

The main narrative in this chapter explained how the use of real-time analytics in the cybersecurity incident response process helped these organizations to develop higher-order real-time analytics-enabled dynamic capabilities and dynamic incident response strategies. In addition, it also described the impact of using real-time analytics capabilities in cybersecurity incident response process on overall enterprise performance. To further support this narrative, a data structure display (Figure 4-1), and a data table (Table 4-1) that supported emergent constructs was also included. Finally, the key findings from the data analysis were integrated with existing literature to build an overall framework of dynamic cybersecurity incident response to improve cybersecurity incident response agility.

Figure 4-2 shows the framework that this study developed based on the analysis of qualitative data. These organizations responded to this dynamic threat environment by using real-time analytics in their cybersecurity incident response process. Specifically, they used real-time analytics capability to develop higher order analytics-enabled dynamic capabilities such as real-time situational awareness, dynamic risk assessment and cyber threat intelligence generation. These three dynamic capabilities, enabled by real-time analytics, helped these organizations to shape three dynamic incident response strategies (namely, active reconnaissance, continuous monitoring, and active defence).

These dynamic capabilities together with dynamic incident response strategies infuse agile characteristics such as swiftness, flexibility and innovation in cybersecurity incident response process, which in turn, lead to positive outcomes in enterprise security performance and delivered both strategic and economic benefits. In addition, the framework also identified two groups of factors (cybersecurity incident response factors and characteristics of analytical capability) that fostered the development of dynamic capabilities and execution of dynamic cybersecurity incident response strategies.

In the next chapter, the findings and results from the three case studies are discussed in the context of the existing IS literature. The implications of the results of this study for IS research and practice are addressed. The final part of the chapter outlines the conclusions of the research as a whole and suggests some directions for future research.

5

"Being a senior manager, I need to be aware of not only any particular cybersecurity incident but also of the whole cyber threat landscape. In this aspect, my cybersecurity awareness is both global and local. This can only happen if we share cybersecurity related information in a structured way."

(Cybersecurity senior manager, FinBank)

CHAPTER 5. DISCUSSION

The overall findings of this study were reported in the previous chapter. The details of these findings enhance our current understanding of the role that real-time analytics plays in improving cybersecurity incident response agility in three ways. First, this study develops a framework that links real-time analytics capability with cybersecurity incident response agility. The framework represents the main contribution of this research. Second, the details of the framework explain how agility is improved by developing dynamic capabilities in the cybersecurity incident response process. And third, this research provides insights that can contribute to cybersecurity incident response practice. This chapter highlights the contribution these findings make to cybersecurity incident response research and practice and to IS research in general.

The chapter starts by discussing the findings and key insights of the study in relation to the existing business analytics capabilities, dynamic capabilities, business process agility, and cybersecurity incident response literature. Where appropriate, the connection of this research to broader debates in the IS literature is explained. The final part of the chapter outlines the implications of this study for both IS research and practice.

5.1. Key Themes and Insights

The current cyber threat environment of modern organizations is dynamic and complex. In order to stay competitive, organizations need to constantly adapt to changes in their cyber threat landscape. As cybersecurity incidents are increasingly impacting organizations, it is crucial that their incident response teams have the ability to detect, investigate, report, respond and, ultimately improve their overall enterprise security by implementing strong preventative strategies as well as proactive response strategies.

One of the essential characteristics of the proactive incident response strategy is to be agile in incident response, and a key part of that is having the right information at the right time to be able to respond in the right manner, however implementing such strategy is complex and challenging for incident response teams. Therefore, the main goal of this research was to better understand how cybersecurity incident response teams improve agility in their incident response process using real-time analytics.

In this study, participants from cybersecurity incident response units of three large financial organizations (FinBank, FinInsuranceA, and FinInsuranceB) were interviewed and the analysis of data across these units informed a framework of dynamic incident response to improve cybersecurity incident response agility. Figure 5-1 (see next page) shows the framework that this study develops based on the analysis of qualitative data.

The details of the framework contribute to the literature on business analytics capabilities by identifying specific dimensions of real-time analytics capability. In addition, the framework also develops a richer understanding of dynamic capabilities enabled using real-time analytics in the cybersecurity incident response such as real-time situation awareness, dynamic risk assessment, and cyber threat intelligence generation.

These real-time analytics enabled dynamic capabilities help organizations to execute dynamic cybersecurity incident response strategies such as active reconnaissance, continuous monitoring, and active defense. The aforementioned dynamic capabilities together with dynamic incident response strategies infuse agile characteristics such as swiftness, flexibility and innovation in cybersecurity incident response process, which in turn, lead to positive outcomes in enterprise security performance and delivers both strategic and economic benefits. Lastly, the framework also contributes to the

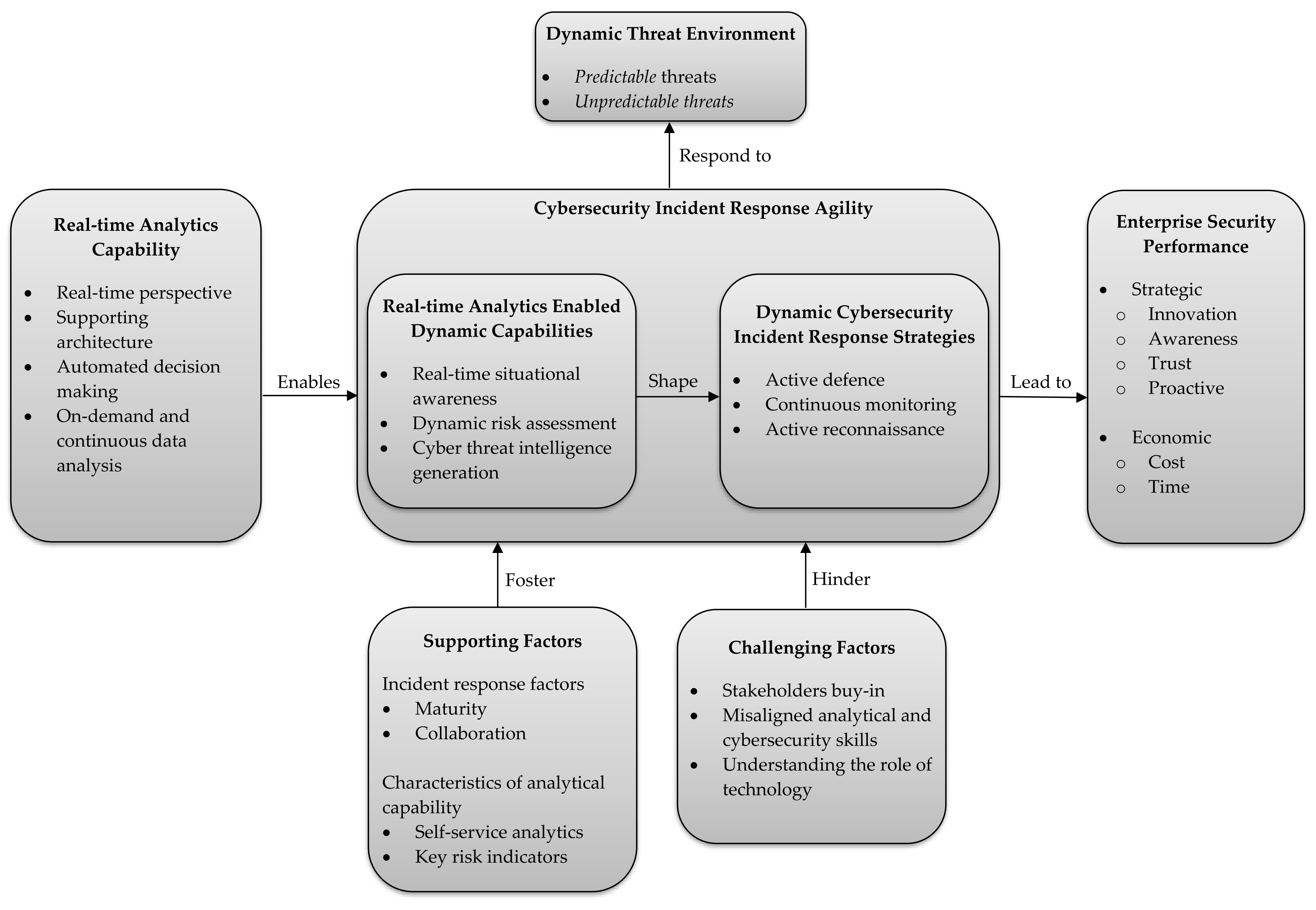

Dynamic Threat Environment
Predictable threats
Unpredictable threats
Respond to
Cybersecurity Incident Response Agility
Real-time Analytics Capability
Real-time perspective
Supporting architecture
Automated decision making
On-demand and continuous data analysis
Enables
Real-time Analytics Enabled Dynamic Capabilities
Real-time situational awareness
Dynamic risk assessment
Cyber threat intelligence generation
Shape
Dynamic Cybersecurity Incident Response Strategies
Active defence
Continuous monitoring
Active reconnaissance
Lead to
Enterprise Security Performance
Strategic
Innovation
Awareness
Trust
Proactive
Economic
Cost
Time
Foster
Hinder
Supporting Factors
Incident response factors
Maturity
Collaboration
Characteristics of analytical capability
Self-service analytics
Key risk indicators
Challenging Factors
Stakeholders buy-in
Misaligned analytical and cybersecurity skills
Understanding the role of technology

Figure 5-1. A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility

literature on cybersecurity incident response strategies in the context of dynamic incident response, an emerging approach of cybersecurity incident response.

5.1.1. Real-time Analytics Capability

Anecdotal evidence in both research and practitioner literatures suggest that BA capabilities deliver significant benefits to organizations and contribute to firm performance. For example, Watson et al. (2006) describe a number of benefits that Continental Airlines gained through building real-time applications in flight operations and customer relationship management. Similarly, Kohli (2007) describes benefits that United Parcel Service gained through analysis of data in their highly integrated active data warehouse such as improved speed of delivery and profitability across delivery routes. The findings of this study are consistent with these observations in that the organizations realized both strategic and economic benefits such as gaining customer trust, improving cybersecurity awareness, handling cybersecurity incidents proactively and reducing the cost and time to detect and respond to cybersecurity incidents by building real-time analytics capability in the cybersecurity incident process.

The findings from this research further develops our understanding of real-time analytics capability by identifying its specific dimensions. First, "real-time" has many perspectives or meanings in terms of how fast and frequently data should be fetched and processed to deliver the required business insights. That is why the terms "near real-time" or "right time" or "true real-time" are interchangeably used to reflect the meaning of real-time analytics (Eckerson 2012; Russom et al. 2014). This study suggests that the design of real-time solutions should satisfy business requirements because each business process has different requirements for the freshness of insights.

Second, real-time analytics as an innovative technology requires architectural changes in a traditional business analytics architecture. This study provides empirical evidence for this observation and suggests that implementation of real-time analytics solution requires several additional capabilities in a typical business analytics architecture such as in-memory analytics, data virtualization and interoperability across multiple analytical platforms. For example, when data needs to travel in real-time across multiple analytical platforms, each platform and tool requires some sort of real-time capability (e.g., streaming input and data analysis, complex event processing, and business rules). As such, the findings from this study corresponds closely to use of real-time business intelligence at Continental Airlines (Anderson-Lehman et al. 2004; Watson et al. 2006).

Third, automated decision making is a crucial feature of real-time analytics capability as it helps organizations to generate automatic threat alerts and trigger actions based on the business rules and thereby enable innovation in incident response through building incident response automation systems. This finding supports the earlier conclusion drawn in BA literature that a complete real-time automation system requires both streaming analytics and business rules (Phillips-Wren et al. 2015; Russom et al. 2014). This study, however, extends this earlier work by explaining how the combination of real-time event processing, data warehousing, Hadoop clusters, data marts, incident response strategy, complex algorithms and predictive models provide a data analysis and storage infrastructure that can enable automated decision making in the IR process. In addition, the data from this study highlights that the goal of using automation in the incident response is to accelerate and enrich the process of detection and then intelligently respond to cybersecurity incidents. This is the reason why decision making in the cybersecurity incident response process cannot be fully automated and the involvement of humans (cybersecurity managers) is critical as the complexity of incident response requires human input during the process of assessing the impact, scope and severity of the cyber-attacks.

Fourth, using complex event processing in on-demand and continuous data analysis enables capturing and processing of streaming data and helps in analyzing cause-and-effect relationships among cybersecurity events in real-time and thereby enable flexibility in incident response. Cybersecurity events cannot always be predicted (Baskerville 2005; Baskerville et al. 2014). In complex event processing, events act as a trigger, therefore IR teams can proactively respond to cybersecurity events as they occur by taking effective actions against suspicious events.

In summary, data from this study expand our understanding of real-time analytics capability and extends the prior literature by describing its specific dimensions including defining the real-time perspective, building supporting architecture, automated decision making, and on-demand and continuous data analysis.

5.1.2. *Achieving Dynamic Capabilities in Cybersecurity Incident Response*

Extant research suggests that the level of dynamism within the external environment determines the type of capabilities that organization develop to deal with the dynamic environment. For example, cybersecurity environments that face dynamic and sophisticated attacks requires more response-oriented dynamic capabilities in addition to the existing preventative capabilities (Baskerville et al.

2014). The findings of this study are consistent with this observation in that the organizations that face dynamic threat environment achieved dynamic capabilities such as real-time situation awareness, dynamic risk assessment, and cyber threat intelligence generation through strong coordination, reconfiguration and integration of cybersecurity resources enabled by real-time analytics.

While the traditional incident response capabilities are focused on preventing cybersecurity incidents from happening, the real-time analytics enabled dynamic capabilities are focused on responding to cybersecurity incidents that have happened or are happening. These dynamic capabilities help in the integration and consolidation of information from different cybersecurity systems such as SIEM, log management, intrusion detection and prevention systems with threat intelligence feeds. The analysis of this information using monitoring dashboards improves the situational awareness of cybersecurity managers and empowers them to execute appropriate incident response strategies in a timely manner. This demonstrates the importance of developing analytical information processing capabilities that are enabled by business analytics to innovate in cybersecurity incident response process (Chen et al. 2012; Pierazzi et al. 2016; Tan et al. 2003). While traditional analytical capabilities help organizations to analyse business data to better understand their business and market (Chen et al. 2012), it is the key features of the real-time analytics capability that enables organizations to create dynamic capabilities in their incident response process that are responsive to change, complex, and instill dynamism in their cybersecurity incident response strategies.

The findings from this study correspond closely to the role of dynamic risk assessment that have been observed in practicing proactive cybersecurity risk management (Baskerville 2005; Baskerville et al. 2014). Specifically, in proactive cybersecurity risk management, risk assessment is considered to be a dynamic activity that copes with risks and vulnerabilities that are continuously changing their nature (Baskerville et al. 2014). The data from this study explains that real-time analytics enable organizations to do risk assessment in a dynamic way by helping them analyse and monitor the cybersecurity risks and threats using key risk indicators that provide them the timely information regarding risk exposure, emerging risk trends and changes in risk profile of the organization.

The findings of this study extend Baskerville (2014) work by identifying specific key risk indicators (leading and lagging) that are crucial for dynamic risk assessment as they help in the mitigation and monitoring of cybersecurity risks and facilitate in the risk reporting. The following example illustrates the point when the general manager of cybersecurity strategy and governance in FinInsuranceA analysed the lag indicators to understand the cybersecurity incidents that have happened in their organization such as how much spam they received on monthly basis, the number of desktops that are affected by the malware, the number of malicious URL's that were accessed in a certain period of time. He analysed leading indicators to understand the future so that he can then take preemptive actions such as identifying the number of people that requested a security exemption to formally be non-compliant with a security policy or standard. This indicated to him that their risk appetite is invalid, and he needs to change their risk appetite, or he needs to do more work around employee security awareness and education.

Another lead indicator that he analysed was the percentage of people in their organization that have taken the recent cybersecurity awareness program. If the percentage of completion was small, then it meant that the training was not effective as most of the people have not done it. In this way he could conclude that the likelihood of an event resulting from the poor employee awareness and education is higher because most of employees have not completed the program.

An example of the lead indicator in vulnerability management that he analysed was the number of servers that were not patched in the appropriate service agreed time frames. If the analysis highlighted that the time period in which a server is not being patched was increasing, then it meant that their aggregate risk exposure was increasing. In this way, he was able to raise management awareness that they are becoming more and more exposed on a daily basis and they need to get the appropriate funding or the appropriate management focus to reduce the lag in people patching their servers to demonstrate that they are proactively reducing the risk exposure. Therefore, the analysis of key risk indicators played an important role in enabling dynamic risk assessment by identifying potential high-risk areas and taking timely actions.

Prior research has highlighted the critical role of situational awareness in enabling informed decision making in the process of information security risk management (Webb et al. 2014). This study extends the prior research by presenting real-time situational awareness as a dynamic capability that is enabled by the use of real-time analytics in the cybersecurity incident response process. While this study identifies several mechanisms for developing real-time situational awareness in dynamic threat landscape, it also provides some interesting insights into how real-time analytics may be used by organizations to generate cyber threat intelligence to develop a comprehensive understanding of their cybersecurity threat environment. Specifically, real-time analytics enables rapid and continuous innovations in cybersecurity incident response by making it possible to combat advanced cybersecurity threats by analyzing log data from security systems and integrating external threat intelligence feeds with it to generate comprehensive cybersecurity insights that has been identified as crucial in dealing with dynamic threat environments.

Thus, this study contributes to our understanding of how the use of real-time analytics can enable dynamic capabilities in cybersecurity incident response process to deal with dynamic threat environment that encompasses both predictable and unpredictable threats and thus extends the prior literature that has so far focused primarily on combating known threats using preventative controls. In fact, the results of this study suggest the need to reconceptualize the role of disruptive technologies such as real-time analytics in novel ways because not only it can be used to develop dynamic capabilities in cybersecurity incident response process but also to support novel multiple organizational capabilities.

In summary, the findings from this study suggest that real-time analytics may accelerate the ability of an organization to use IT as a platform for achieving dynamic capabilities. This study illustrates the ability of real-time analytics to rapidly integrate, build, and reconfigure organizational cybersecurity resources, skills and functional competencies in ways that were previously infeasible (Eisenhardt and Martin 2000; Teece et al. 1997). Thus, real-time analytics capability serves as an excellent exemplar of a 'digitized platform for processes and knowledge' that enables organizations to create real-time situational awareness and cyber threat intelligence on both external and internal cyber threats that helps them to detect cyber-attacks as they happen and respond to them in a timely manner.

5.1.3. *Improving Cybersecurity Incident Response Agility Through Dynamic Capabilities*

This study may also be viewed as a response to the call by Teece et al. (2016) to empirically examine how strong dynamic capabilities can yield organizational agility. A form of organizational agility that is of particular relevance to IS research is business process agility, which means the extent to which organizations can quickly and easily retool their business processes.

This study investigates how organizations have been able to improve agility in their incident response process by developing dynamic capabilities using real-time analytics. For example, the leverage gained through building real-time analytics capabilities for an organization to 'reconfigure, build, and integrate external and internal resources in creating the higher order capabilities' is illustrated in the three types of real-time analytics enabled dynamic capabilities presented in the results of this study. These dynamic capabilities, in turn, help organizations to execute dynamic cybersecurity incident response strategies and thereby improve incident response agility by efficiently and effectively redirect/redeploy their incident response resources to detect and respond to unknown, unexpected and unpredictable cybersecurity threats. The data from this study identifies three ways through which the combination of real-time analytics capability, real-time analytics enabled dynamic capabilities and dynamic incident response strategies help organizations to improve agility in cybersecurity incident response process: (1) enabling rapid incident detection and response, (2) facilitating flexibility in incident response, and (3) enabling innovation in incident response.

First, agility is the most important feature of an organization making rapid business decisions. In addition, Baskerville et al. (2014) have highlighted agility as a key characteristic of incident response capability in response mode. As most of the security data are streaming data that come from various sources in the form of logs such as firewalls, intrusion detection and prevention systems, servers, applications, and databases; the challenge for IR team is to analyse this ever-growing stream of data swiftly. Being able to swiftly detect the dynamic cybersecurity threats and responding to them quickly can be a decisive factor in incident response success or failure.

The data in this study suggests that one way to achieve agile and rapid incident detection and response is by rapidly going through the value workflow of business analytics. The value workflow of business analytics can be described as a simple process of turning data into insights, analyzing the insights in a specific context to make them meaningful, and then taking decision based on meaningful insights that can create value (Eckerson 2012; Sharma et al. 2014; Wixom et al. 2013). This study suggests that real-time analytics capabilities, real-time analytics enabled dynamic capabilities, and dynamic incident response strategies help organizations to improve their incident response agility by instilling the value workflow of BA in their incident response process and thereby enhance the overall enterprise security performance.

Second, real-time analytics capability can also enable flexibility in incident as it provides two types of data analysis in real-time (1) On-demand and (2) Continuous. On-demand real-time analytics waits for the systems or users to request a query and then the analytical results are delivered (Russom et al. 2014). This is useful for incident response teams when they want to know what is happening at a certain moment. For example, incident response teams can pull data from communication mediums to analyse phishing and spear phishing attacks. In contrast, continuous real-time analytics is more proactive and alerts users or triggers responses as events happen (Russom et al. 2014). For example, continuous real-time analytics can be used to monitor user activity to detect any changing patterns (i.e. behavioral analytics). Therefore, the results of this this study suggest that both on-demand and continuous data analysis feature of rea-time analytics provide flexibility in cybersecurity incident response process and can be used in executing an effective and dynamic incident response strategy.

Third, in terms of enabling innovation in cybersecurity incident response process, the findings of this study suggest that real-time analytics and real-time analytics enabled dynamic capabilities help organizations to reconfigure their incident response process, create new incident response plans, and continuously look out for innovative ways to respond. Therefore, the findings from this study corresponds closely to the role of IT capability as enabler of business process agility described in Sambamurthy et al. (2003) in that, IT capability could be 'driving the modularization and atomization of business processes and enabling their combination and recombination to create new business processes' (Sambamurthy et al. 2003, p. 265).

Dynamic capabilities theory extends the resource based view (RBV), which theorizes that 'when firms have resources that are valuable, rare, inimitable, and non-substitutable (VRIN), they can achieve sustainable competitive advantage by implementing fresh value-creating strategies that cannot be easily duplicated by competing firms' (Barney et al. 2001; Newbert 2007). The data from this study explains how the incident response agility achieved through dynamic capabilities exhibit the VRIN characteristics of RBV. Agility in the IR process can be demonstrated by swiftness in anticipating and detecting the cybersecurity threats, understanding the motivation and consequences behind cybersecurity attacks, exploring options and making informed decisions and then implementing appropriate responses.

Even though organizations are paying increasing attention to enable IR agility, not enough is known about how agility can be realized in cybersecurity incident response (Grispos et al. 2014). In this aspect, IR agility is a rare capability. Interestingly, this study illustrates how strong dynamic capabilities help organization to redesign their existing IR process and prepare for quick and effective reactions for new types of unpredictable cybersecurity threats. By their very nature, every new cyber-attack is inherently unpredictable. The practice of IR in an agile way gets rooted in organizational routines, thereby making it very hard for a cyber-attacker to understand fully how a new attack is going to be dealt with by the IR team. As such, the diversity of responses by the incident response team is varied, therefore makes it quite valuable, inimitable and non-substitutable for the organization. To conclude, cybersecurity incident response process agility has the characteristics of a strategic organizational capability that can help organizations to better acquire and deploy resources to deal with dynamic cyber threat environment.

Recent research observes that firms that have built process-oriented dynamic capabilities are able to improve their business process agility so that they are better able to detect changes, threats and opportunities in the environment which in turn help them to exploit opportunities for innovation and competitive action (Battleson et al. 2016; Park et al. 2017). Further, it is argued that business process agility achieved through dynamic capabilities is an important mechanism through which firms can outperform competitors by responding more effectively to changing environments with the help of enhanced communication, coordination, and information sharing (Teece et al. 2016; Teece 2007).

This study reinforces these findings by analyzing organizations that may develop real-time analytics enabled dynamic capabilities such as real-time situation awareness, dynamic risk assessment and cyber threat intelligence that enhance communication, coordination, and information sharing in cybersecurity incident response process. Although most of the dynamic capabilities literature investigates its role in achieving competitive advantage and/or creating value, this study suggests that real-time analytics enabled dynamic capabilities are crucial for sustaining or protecting competitive advantage.

In summary, the findings from this study suggests that dynamic capabilities enable organizations to adopt to changes in their cyber threat environment and agile in responding to cybersecurity incidents. Improving agility through dynamic capabilities instill the characteristics of speed, flexibility, and innovation in cybersecurity incident response process. It provides organizations with the ability to respond quickly to dynamic and emerging cyber threats. With improvement in cybersecurity incident response agility, organizations can rapidly and flexibly redesign existing processes or create new ones to cope with dynamic threat environment (Park et al. 2017; Sambamurthy et al. 2003). This kind of agility can be demonstrated by swiftness in sensing relevant events, interpreting what is happening and assessing the impact and consequences for the organization, exploring options and making decisions, and implementing appropriate responses (Chen et al. 2013).

5.1.4. Dynamic Cybersecurity Incident Response

Extant research highlights the shortcomings in traditional (reactive) approaches in cybersecurity incident response and calls for more dynamic (proactive) approaches to better deal with both predictable and unpredictable cybersecurity attacks. Baskerville et al. (2014) have called for the development of dynamic capabilities in cybersecurity environments that face dynamic and sophisticated attacks. The real-time analytics enabled dynamic capabilities observed in this study enable organizations to implement dynamic incident response strategies such as:

(1) active reconnaissance (leveraging threat intelligence feeds to detect cybersecurity incidents during the reconnaissance phase, before the organization is actually been attacked);
(2) continuous monitoring (continuously monitor the attack by gathering more intelligence about both attacker and attack through passive means); and
(3) active defence (to defend the attacked enterprise assets through active means by harnessing more intelligence about the attack and pacify the attacker infrastructure). Implementing a dynamic response strategy requires organizations to tap into all available information about the cyber threats to develop situational awareness, perform dynamic risk assessment to discover the potential of a threat, detect the actual threat using cyber threat intelligence, and then execute an enterprise-wide response before the threat becomes significant.

One of the critical challenges in implementing a dynamic incident response is to develop a high degree of situational awareness and cyber threat intelligence on both internal and external threats to an organization. This study illustrates the ability of real-time analytics to help incident response teams quickly sift through massive amounts of data, both inside and outside the enterprise and thereby develop situation awareness and cyber threat intelligence. For example, real-time situational awareness enabled by real-time analytics helps in understanding the cyber threat landscape, such as which information assets must be protected immediately and why, what threat actors exist and threaten these assets, what value these assets have to a potential attacker and how to provide protection and vulnerability identification and mitigation for these assets. Similarly, cyber threat intelligence enabled by real-time analytics helps in uncovering hidden relationships, detecting attack patterns, stamping out security threats and setting priorities for remediation.

5.2. Implications of the Study

What is the theoretical and practical significance of the findings of this research? How and why are these findings and insights useful? How do these develop our understanding of improving agility in cybersecurity incident response process using real-time analytics? And how are they different from what was known about improving cybersecurity incident response agility before the commencement of this study? The purpose of this section is to address these important questions, beginning with the theoretical and then the practical implications of the findings.

5.2.1. *Implications for Research*

The findings of this study offer several important implications for the literature on information systems research, with its examination of improving agility in cybersecurity incident response using real-time analytics.

First, this study identifies specific dimensions of real-time analytics capability and demonstrate how organizations develop dynamic capabilities in their incident response process by investing and using real-time analytics capability. It highlights how real-time analytics enabled dynamic capabilities may help organizations to shift from a reactive approach to a proactive approach for cybersecurity incident response.

Second, following Teece et al. (2016) call for studies to examine how strong dynamic capabilities can yield agility, this study examines how real-time analytics enabled dynamic capabilities help organizations integrate, build, and reconfigure their resources to improve agility in their cybersecurity incident response process. Specifically, this study introduces real-time analytics enabled dynamic capabilities and dynamic incident response strategies to explain how organizations may improve agility in their cybersecurity incident response process and thereby enhance their overall enterprise security performance. In particular, this study addresses the research question (*How can enterprises improve agility in their cybersecurity incident response process using real-time analytics?*) by developing a framework (see Figure 5-1) that represents this study's main research contribution by linking real-time analytics capabilities and cybersecurity incident response agility.

Through the framework, this study explains how organizations using real-time analytics are able to develop higher order real-time analytics enabled dynamic capabilities in incident response. This study further explains how real-time analytics enabled dynamic capabilities enable agile characteristics of innovation, flexibility and swiftness in incident response that shape dynamic incident response strategies. This study presents interesting and applicable findings related to the use of real-time analytics for improving incident response agility. Specifically, this study findings shed light on how organizations with dynamic capabilities enabled by the use of real-time analytics improve incident response agility which, in turn, enhance overall enterprise security performance by delivering strategic and economic benefits. The framework also provides a comprehensive view of the factors that both facilitate and inhibit the development of dynamic capabilities in cybersecurity incident response process.

This study expands our understanding of real-time analytics capability and extends the prior literature by identifying its specific dimensions in cybersecurity incident response process including defining the real-time perspective, building supporting architecture, automated decision making, and on-demand and continuous data analysis. In addition, this study contributes to the literature on dynamic capabilities and incident response strategies by identifying real-time analytics enabled dynamic capabilities that enable agility in incident response and shape dynamic incident response strategies. Three real-time analytics enabled dynamic capabilities include real-time situation awareness, dynamic risk assessment, and cyber threat intelligence generation. Three dynamic incident response strategies include active defence, continuous monitoring, and active reconnaissance.

While Baskerville et al. (2014) work highlights agility as key characteristics of dynamic incident response and calls for the development of dynamic capabilities in cybersecurity environments that face dynamic and sophisticated attacks, this study extends the prior literature by identifying three specific real-time analytics enabled dynamic capabilities in incident response and explaining how to implement dynamic incident response strategies using these dynamic capabilities and thereby improve agility in cybersecurity incident response.

This study identifies how the essential factors of cybersecurity incident response process and characteristics of analytical capability support the development of real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies. *Incident response process maturity and collaboration* among different stakeholders involved in the cybersecurity incident response process support the development of dynamic risk assessment capability. Organizations which have a mature cybersecurity incident response process and collaborate with threat intelligence sharing communities have more visibility into cybersecurity threat landscape and can respond to cybersecurity incidents proactively.

Self-service analytics feature of analytical capability supports the development of real-time situation awareness. Self-service analytics empowers incident response teams to run queries and analyse incident related data independently with little help from IT or BA team. Finally, measuring the right *key risk indicators* feature of analytical capability support the development of cyber threat intelligence. Defining and analysing the right key risk indicators helps organizations to identify and report emerging threats, monitor effectiveness of their security controls and therefore better understand their cybersecurity environment.

5.2.2. *Implications for Practice*

The results of this study have considerable practical significance and contribute to three groups of stakeholders in cybersecurity incident response practice. For incident response teams, this study's implications include the nuanced view of the role of real-time analytics. Rather than pursuing real-time analytics at operational level only as a way to continuously monitor cyber threat environment, incident response teams need to recognize the more innovative role of real-time analytics at strategic level in implementing both protective and detective response strategies. The utilization of the range of capabilities that are enabled by real-time analytics will help incident response teams implement the combination of prevention, detection and response approaches that can help them to better deal with both predictable and unpredictable cybersecurity threats.

For cybersecurity vendors, the findings from this study suggest that they should recognize the potentially far-reaching innovative role that their cybersecurity solutions may provide to enterprises. Creating cybersecurity solutions that can integrate threat intelligence data, automate investigations and forensic analysis, apply complex algorithms and visual analytics to discover the potential threats will help their clients create innovative incident response strategies that can deal with dynamic threat environment. The far-reaching potential of the capabilities enabled by real-time analytics such as real-time situational awareness, dynamic risk assessment, and cyber threat intelligence generation, however, will also increase the demand for data integration, automation, visualization and analytics. Therefore, vendors who develop cybersecurity solutions need to carefully consider these requirements when developing their solutions.

For cybersecurity managers, the results from this study highlight that in order to build analytical capabilities in cybersecurity incident response, managers need to hire and/or train cybersecurity or analytics personnel with skills and knowledge needed to develop security analytics solutions and integrate and acquire analytical solutions provided by external vendors. To do so, managers (1) can upskill and teach their current cybersecurity personnel who have traditional cybersecurity background that how to understand and utilize the more advanced information analyst capabilities; (2) can recruit the personnel that come from the business analytics background and then teach them cybersecurity processes; and (3), can go to a vendor or managed security services providers if they cannot hire or train existing employees to buy these skills and knowledge while they build their our own analytical capabilities in incident response.

5.3. Summary

This chapter presented the key insights of the study through a synthesis of the findings presented in previous chapter. The key findings in relation to each of the key concepts of interest in this study were summarized. The results of the study were also discussed in the context of the existing IS research. The main contributions of the study to both theory and practice were discussed. And finally, the chapter outlined the implications of this study for both IS research and practice. The next chapter concludes the dissertation by summarising the research background, research method and key contribution of this research project. The chapter also outlines directions for future research and highlights limitations of this study.

6

"The concept of cybersecurity risk management is so that we can operate our business processes in a manner with some assurance that we can actually be very confident in doing our daily business operations. The analogy is like where you have brakes on a car, it is actually the brakes that are there to allow you to go faster, it is not to slow you down. So, the benefit of using analytics is that we can actually manage our risks appropriately and we can have the confidence to innovate and operate our business processes in a manner that they can be very effective and efficient."

(Manager of cybersecurity strategy and governance, FinInsuranceA)

CHAPTER 6. CONCLUSION

This research project sought to answer the following research question: *How can organizations improve agility in their cybersecurity incident response process using real-time analytics?* Answering this research question is important for both academia and practice. In today's complex and dynamic cybersecurity environment, organizations are increasingly facing complex and evolving cybersecurity threats, both external and internal, such as theft, fraud, sabotage, embezzlement, and industrial espionage. The traditional cybersecurity incident response approach that primarily focus on react, respond and recover strategy can no longer deal with this modern threat landscape. Organizations can improve agility in their cybersecurity incident response process by shifting from a reactive approach to a proactive approach using real time analytics that can help them to anticipate, detect and respond to complex and evolving cybersecurity threats in a timely, agile and cost-effective manner.

Shifting to a proactive approach and mindset requires organizations to harness all available data related to cybersecurity threats and analyse it to discover the potential of a threat, detect the actual threat, gather intelligence about the attack, and then execute an enterprise wide response before the threat becomes significant. Even though organizations are paying considerable attention to improve incident response agility and develop proactive cybersecurity incident response strategies, not enough is known about the role that analytics plays in improving agility in the cybersecurity incident response process and in developing dynamic cybersecurity incident response strategies.

This study answers the aforementioned question and applies the lens of dynamic capabilities theory to explain how a specialized business analytics capability (in this case real-time analytics) helps organizations to develop real-time analytics enabled dynamic capabilities and dynamic incident response strategies and thereby improve agility in the process of cybersecurity incident response. This study also focuses on two groups of factors (cybersecurity incident response factors and characteristics of analytical capability) that foster the development of dynamic capabilities and execution of dynamic cybersecurity incident response strategies.

6.1. Contributions

The first key contribution of this study is a careful integration, synthesis and analysis of interdisciplinary IS literature on business analytics, dynamic capabilities, business process agility and cybersecurity incident response. However, more importantly, this study has sought to answer the research problem empirically by conducting an exploratory field study. By adopting a qualitative approach, this study has been able to provide critical insights on "how" organizations improve agility in their cybersecurity incident response using real-time analytics. The use of multiple case study approach allowed the researcher to gain in-depth insights by exploring the use of real-time analytics in the cybersecurity incident response process in different organizational contexts. By combining the insights gleaned from qualitative data with extant literature, this study develops a framework of dynamic cybersecurity incident response to improve incident response agility.

The details of the framework contribute to the literature on business analytics capabilities, dynamic capabilities, cybersecurity incident response strategies, and business process agility. First, this study identifies four specific dimensions of real-time analytics capability such as defining the real-time perspective, building supporting architecture, automated decision making and on-demand and continuous data analysis. Second, this study identifies three real-time analytics enabled dynamic capabilities including real-time situation awareness, dynamic risk assessment, and cyber threat intelligence generation. Third, this study identifies three dynamic cybersecurity incident response strategies such as active defence, continuous monitoring, and active reconnaissance. Finally, this study explains how organizations execute dynamic cybersecurity incident response strategies using real-time analytics enabled dynamic capabilities and thereby improve agility in their cybersecurity incident response.

The second key contribution links real-time analytics capability and cybersecurity incident response agility with enterprise security performance and presents cybersecurity incident response agility as a manifested type dynamic capability. Real-time analytics enabled dynamic capabilities help organizations integrate, build, and reconfigure their resources to improve agility in their cybersecurity incident response process. The improved agility in cybersecurity incident response enables organizations to redeploy and redirect its cybersecurity resources, change its existing incident response processes, routines and techniques, or create new ways of responding to both predictable and unpredictable cybersecurity threats in a swift and timely manner. In this way, real-time analytics enabled dynamic capabilities instil agile characteristics of innovation, flexibility and swiftness in incident response that shape dynamic cybersecurity incident response strategies. Therefore, the use of real-time analytics to develop real-time analytics enabled dynamic capabilities and dynamic incident response strategies help organizations to improve their overall enterprise security performance by realizing economic benefits in terms of reducing the cost and time to detect and respond to cybersecurity incidents and strategic benefits in terms of building customer trust, improving security awareness and handling cybersecurity incidents in a proactive manner.

The third key contribution relates to the essential factors of cybersecurity incident response process and characteristics of analytical capability that support the development of real-time analytics enabled dynamic capabilities and dynamic incident detection and response strategies. Incident response process maturity and collaboration among different stakeholders involved in the incident response process support the development of dynamic risk assessment capability. Organizations which have a mature incident response process and collaborate with threat intelligence sharing communities have more visibility into cybersecurity threat landscape and can respond to cybersecurity incidents proactively. Self-service analytics feature of analytical capability supports the development of real-time situation awareness. Self-service analytics empowers incident response teams to run queries and analyse incident related data independently with little help from IT or BA team. Finally, measuring the right key risk indicators feature of analytical capability support the development of cyber threat intelligence. Defining and analysing the right key risk indicators helps organizations to identify and report emerging threats, monitor effectiveness of their security controls and therefore better understand their cybersecurity environment.

This research delivers important insights to cybersecurity managers in terms of building analytical capabilities in the process of cybersecurity incident response. In order to deal with today's dynamic cyber threat landscape, cybersecurity managers need personnel in their cybersecurity team that have strong analytical and communications skills and business acumen so that they can understand their business and analyse cybersecurity threats efficiently and effectively. Therefore, cybersecurity managers need to hire and/or train cybersecurity or analytics personnel with skills and knowledge needed to develop security analytics solutions and integrate and acquire analytical solutions provided by external vendors. One of the interviewees stated that educating data analytics personnel with cybersecurity knowledge is a better option as they can leverage the insights garnered from the cybersecurity landscape and feed them back to the rest of the business to create value.

This research can also guide cybersecurity incident response teams in using real-time analytics not only at operational level in analysing and monitoring cyber threat environment, but also at tactical and strategic level in developing and implementing proactive cybersecurity incident response strategies. For cybersecurity vendors, the findings from this study suggest that they should recognize the potentially far-reaching innovative role that their cybersecurity solutions may provide to enterprises. Creating cybersecurity solutions that can integrate threat intelligence data, automate investigations and forensic analysis, apply complex algorithms and visual analytics to discover the potential threats will help their clients create innovative incident response strategies that can deal with dynamic threat environment.

6.2. Limitations and Future Research

This section is aimed at encouraging further research on the theme of how organizations improve agility in their cybersecurity incident response, an area offering rich opportunities for academic enquiry. Although this study has taken a step towards addressing the important research gap, many opportunities for improving or expanding on the findings remain. The possible directions for future research based on the findings and limitations of this study are discussed below.

The context of this study raises questions about the generalizability of the proposed model and suggests possibilities for future research. It is not possible to generalize from interpretive research in the way one might generalize from quantitative research based on statistical sampling methods.

Therefore, the generalization of the findings of this study in other contexts that involve the adoption of real-time analytics should be carried out with caution because the findings may be particularistic to the specific characteristics of incident response process, and to the sites that were studied in this research. For example, this study acknowledges that the selection of organizations from financial sector, the use of similar incident response strategies in the organizations studied as well as their high-levels of maturity in cybersecurity incident response and in adopting real-time analytics may limit the generalizability of this study's findings.

This study's findings may not apply well to organizations that use different incident response strategies and are at different level of maturity in their adoption of real-time analytics. Therefore, future research is needed that would extend, support or reject this study's findings in other organizational and industry sectors. Despite these limitations, this research suggests that the practice of business analytics in cybersecurity incident response process opens up a new departure for incident response research that considers the implications of business analytics capabilities in implementing dynamic incident response, and the findings from this study will serve as a basis for future research that can be undertaken to challenge, confirm and extend this study's conclusions.

Future research is needed to further investigate the conditions that facilitate or hinder the implementation of dynamic cybersecurity incident response. For example, the incident response units in this study had a dedicated SOC that used SIEM tools and security analytics solutions to deal with cyber threats. Additional research might investigate how different skills and practices of incident response units impact the development of dynamic incident response capability. In addition, each of the incident response units in this study launched a data-driven incident response strategy no less than nine months and no more than 2 years before beginning this study. As a result, many of the insights that emerged in this study represent the output of that strategy. Future research is needed to investigate the specific characteristics of data-driven incident response strategy.

Finally, this study provides a fertile foundation for large-scale quantitative research that can investigate specific factors that help organizations improve incident response agility through dynamic capabilities. The link between achieving agility through dynamic capabilities and organizational performance is a subject of ongoing research. Further research is also needed to identify key difference between real-time analytics and other disruptive technologies to gain insights into how real-time analytics may offer distinct capabilities. As the adoption of real-time analytics facilitates a paradigm shift in decision making process, more detailed studies are required to investigate its potential as well as the challenges in poses to organizations, both large and small.

To conclude, the author hopes that findings of this study make useful contribution to both theory and practice in the pursuit of a better understanding of how real-time analytics improve agility in the process of cybersecurity incident response. The cybersecurity threat environment is dynamic and complex and does not lend itself to being easily understood or pinned down in rules. There is no way that organizations can know what type of cyber threats and attacks they are going to face in the future. However, what they can do is develop proactive approach towards cybersecurity incident response making use of analytics. This will ensure that they are swift, flexible, and innovative in their cybersecurity incident response.

This study offers novel insights into how a specialized business analytics capability such as real-time analytics may enable organizations to quickly detect and respond to cyber threats by developing dynamic capabilities in cybersecurity incident response such as situation awareness, dynamic risk assessment, and cyber threat intelligence. These capabilities help organizations improve incident response agility and better deal with both predictable and unpredictable cybersecurity threats by implementing dynamic incident response strategies such as active defence, continuous monitoring, and active reconnaissance. Together, these ideas contribute to existing research and invite future research on business analytics, dynamic capabilities and cybersecurity incident response management.

REFERENCES

Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers and Security* (42), pp. 27–39.

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

Ahmad, A., Maynard, S. B., and Park, S. 2014. "Information Security Strategies: Towards an Organizational Multi-Strategy Perspective," *Journal of Intelligent Manufacturing* (25:2), pp. 357–370.

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., Ruighaver, T., and Teo, W. T. 2005. "An Information - Centric Approach to Data Security in Organizations," in *In TENCON 2005-2005 IEEE Region 10 Conference. IEEE.*

Alavi, M., and Carlson, P. 1992. "A Review of MIS Research and Disciplinary Development," *Journal of Management Information Systems* (8:4), pp. 45–62.

Anderson-Lehman, R., Watson, H. J., Wixom, B. H., and Hoffer, J. A. 2004. "Continental Airlines Flies High With Real-Time Business Intelligence," *MIS Quarterly Executive* (3:4), pp. 163–176.

Anderson, E. E., and Choobineh, J. 2008. "Enterprise Information Security Strategies," *Computers & Security* (27:1–2), pp. 22–29.

Aragon-Correa, J. A., and Sharma, S. 2003. "A Contingent Resource-Based View of Proactive Corporate Environmental Strategy," *Academy of Management Review* (28:1), pp. 71–88.

Bärenfänger, R., Otto, B., and Österle, H. 2014. "Business Value of In-Memory Technology-Multiple-Case Study Insights," *Industrial Management and Data Systems* (114:9), pp. 1396–1414.

Barney, J. 1991. “Firm Resources and Sustained Competitive Advantage,” *Journal of Management* (17:1), pp. 99–120.

Barney, J. B., Wright, M., and Ketchen, J. D. 2001. “The Resource-Based View of the Firm: Ten Years after 1991,” *Journal of Management* (27:6), pp. 625–641.

Barreto, I. I. 2010. “Dynamic Capabilities: A Review of Past Research and an Agenda for the Future,” *Journal of Management* (36:1), pp. 256–280.

Baskerville, R. 2005. “Information Warfare,” *Journal of Information System Security* (1:1), pp. 23–50.

Baskerville, R., Spagnoletti, P., and Kim, J. 2014. “Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response,” *Information and Management* (51:1), pp. 138–151.

Battleson, D. A., West, B. C., Kim, J., Ramesh, B., and Pamela, S. 2016. “Achieving Dynamic Capabilities with Cloud Computing : An Empirical Investigation,” *European Journal of Information Systems* (25:3), pp. 209–230.

Bharadwaj, A. S. 2000. “A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation,” *MIS Quarterly* (24:1), p. 169.

Bojanc, R., and Jerman-Blažič, B. 2008. “An Economic Modelling Approach to Information Security Risk Management,” *International Journal of Information Management* (28:5), pp. 413–422.

Bojanc, R., and Jerman-Blažič, B. 2013. “A Quantitative Model for Information-Security Risk Management.,” *Engineering Management Journal* (25:2), pp. 25–37.

Bronzo, M., de Resende, P. T. V., de Oliveira, M. P. V., McCormack, K. P., de Sousa, P. R., and Ferreira, R. L. 2013. “Improving Performance Aligning Business Analytics with Process Orientation,” *International Journal of Information Management* (33:2), pp. 300–307.

Cao, G., Duan, Y., and Li, G. 2015. “Linking Business Analytics to Decision Making Effectiveness: A Path

Model Analysis," *IEEE Transactions on Engineering Management* (62:3), pp. 384–395.

Carson, D. 2001. *Qualitative Marketing Research*, SAGE.

Casey, E. 2005. "Case Study: Network Intrusion Investigation - Lessons in Forensic Preparation," *Digital Investigation*, pp. 254–260.

Casey, E. 2006. "Investigating Sophisticated Security Breaches," *Communications of the ACM* (49:2), pp. 48–55.

Chakravarty, A., Grewal, R., and Sambamurthy, V. 2013. "Information Technology Competencies, Organizational Agility, and Firm Performance: Enabling and Facilitating Roles," *Information Systems Research* (24:4), pp. 976–997.

Chen, H., Chiang, R. H., and Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact," *MIS Quarterly* (36:4), pp. 1165–1188.

Chen, P., Desmet, L., and Huygens, C. 2014. "A Study on Advanced Persistent Threats," *Communications and Multimedia Security* (8735), pp. 63–72.

Chen, Y., Wang, Y., Nevo, S., Jin, J., Wang, L., and Chow, W. S. 2013. "IT Capability and Organizational Performance: The Roles of Business Process Agility and Environmental Factors," *European Journal of Information Systems* (23:January 2012), pp. 326–342.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. 2008. "Performance Measurement Guide for Information Security," *NIST Special Publication* (800–55:July).

Cichonski, P., Millar, T., Grance, T., and Scarfone, K. 2012. "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800-61. Revision 2," *NIST Special Publication* (800–61).

de Corbiere, F., and Rowe, F. 2013. "From Ideal Data Synchronization to Hybrid Forms of Interconnections: Architectures, Processes, and Data.," *Journal of the Association for Information*

Systems (14:10), pp. 550–584.

Cosic, R., Shanks, G., and Maynard, S. 2012. "Towards a Business Analytics Capability Maturity Model," *ACIS 2012 : Location, Location, Location : Proceedings of the 23rd Australasian Conference on Information Systems 2012*, pp. 1–11.

Cosic, R., Shanks, G., and Maynard, S. 2015. "A Business Analytics Capability Framework," *Australasian Journal of Information Systems* (19), pp. S5–S19.

Creasy, J., and Glover, I. 2013. "Cyber Security Incident Response Guide," *CREST*.

Darke, P., Shanks, G., and Broadbent, M. 1998. "Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism," *Information Systems Journal* (8:4), pp. 273–289.

Davenport, T. H., and Harris, J. G. 2007. "Competing on Analytics: The New Science of Winning," *Harvard Business Press*, Harvard Business Press.

Davenport, T. H., Harris, J. G., and Morison, R. 2010. "Analytics at Work: Smarter Decisions, Better Results," *Harvard Business Press*, Harvard Business Press.

Dobrev, K., and Hart, M. 2015. "Benefits, Justification and Implementation Planning of Real-Time Business Intelligence Systems.," *Electronic Journal of Information Systems Evaluation* (18:2), pp. 104–118.

Dube, L., and Paré, G. 2003. "Rigor in Informatin Systems Positivist Case Research: Current Practices, Trends, and Recommendations," *MIS Quarterly* (27:4), pp. 597–635.

Eastman, R., and Versace, M. 2015. "Big Data and Predictive Analytics : On the Cybersecurity Front Line," *IDC White Paper* (February).

Eckerson, W. 2010. *Performance Dashboards : Measuring, Monitoring, and Managing Your Business*, John Wiley & Sons, Inc.

Eckerson, W. 2012. *The Secrets of Analytical Leaders: Insights from Information Insiders*, Technics Publications.

Eckerson, W. W. 2004. “Gauge Your Data Warehouse Maturity.,” *DM Review* (14:11), pp. 34–51.

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.

Eisenhardt, K. M., and Martin, J. A. 2000. “Dynamic Capabilities: What Are They?,” *Strategic Management Journal* (21:10–11), pp. 1105–1121.

Elahi, E. 2013. “Risk Management: The next Source of Competitive Advantage,” *Foresight* (15:2), pp. 117–131.

Elbashir, M. Z., Collier, P. A., and Davern, M. J. 2008. “Measuring the Effects of Business Intelligence Systems: The Relationship between Business Process and Organizational Performance,” *International Journal of Accounting Information Systems* (9:3), pp. 135–153.

Elyas, M., Ahmad, A., Maynard, S. B., and Lonie, A. 2015. “Digital Forensic Readiness: Expert Perspectives on a Theoretical Framework,” *Computers and Security* (52), pp. 70–89.

Elyas, M., B., M. S., Atif, A., and Andrew, L. 2014. “Towards A Systemic Framework for Digital Forensic Readiness,” *Journal of Computer Information Systems* (54:3), pp. 97–105.

Eriksson, T. 2014. “Processes, Antecedents and Outcomes of Dynamic Capabilities,” *Scandinavian Journal of Management* (30:1), pp. 65–82.

Fink, L., and Neumann, S. 2007. “Gaining Agility through IT Personnel Capabilities : The Mediating Role of IT Infrastructure Capabilities,” *Journal of the Association for Information Systems* (8:8), pp. 440–462.

Fink, L., Yogev, N., and Even, A. 2017. “Business Intelligence and Organizational Learning: An Empirical

Investigation of Value Creation Processes," *Information and Management* (54:1), pp. 38–56.

Friedberg, I., Skopik, F., Settanni, G., and Fiedler, R. 2014. "Combating Advanced Persistent Threats : From Network Event Correlation to Incident Detection," *Computers & Security* (48), pp. 35–57.

Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the Financial Impact of IT Security Breachesnull," *Information Management & Computer Security* (11:2), pp. 74–83.

George, Alexander and Bennet, A. 2005. *Case Studies and Theory Development in the Social Sciences*, MIT Press. Cambridge.

Germann, F., Lilien, G. L., and Rangaswamy, A. 2013. "Performance Implications of Deploying Marketing Analytics," *International Journal of Research in Marketing* (30:2), pp. 114–128.

Gioia, D. a., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15–31.

Gonzalez, J. J. 2005. "Towards a Cyber Security Reporting System – A Quality Improvement Process," in *International Conference on Computer Safety, Reliability, and Security*, Springer, Berlin, Heidelberg, pp. 368–380.

Gordon, L. a., and Loeb, M. P. 2006. "Budgeting Process for Information Security Expenditures," *Communications of the ACM* (49:1), pp. 121–125.

Grant, R. M. R. 1991. "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation," *California Management Review* (33:3), pp. 114–135.

Grispos, G., Glisson, W. B., and Storer, T. 2014. "Rethinking Security Incident Response: The Integration of Agile Principles," in *20th Americas Conference on Information Systems, AMCIS 2014*, pp. 1–9.

Gupta, M., and George, J. F. 2016. "Toward the Development of a Big Data Analytics Capability," *Information and Management* (53:8), pp. 1049–1064.

Hackathorn, R. 2004. "The BI Watch: Real-Time to Real Value," *DM Review* (14:1), pp. 1–4.

Hahn, G. J., and Packowski, J. 2015. "A Perspective on Applications of In-Memory Analytics in Supply Chain Management," *Decision Support Systems* (76), pp. 45–52.

Helfat, C. E., Finkelstein, S., Mitchell, W., Peteraf, M., Singh, H., Teece, D., and Winter, S. G. 2009. *Dynamic Capabilities: Understanding Strategic Change in Organizations*, John Wiley & Sons.

Helfat, C. E., and Winter, S. G. 2011. "Untangling Dynamic and Operational Capabilities: Strategy for the (N)Ever-Changing World," *Strategic Management Journal* (32:11), pp. 1243–1250.

Holsapple, C., Lee-Post, A., and Pakath, R. 2014. "A Unified Foundation for Business Analytics," *Decision Support Systems* (64), pp. 130–141.

Humphreys, E. 2008. "Information Security Management Standards: Compliance, Governance and Risk Management," *Information Security Technical Report* (13:4), pp. 247–255.

Inmon, W. H. 2002. *Building the Data Warehouse*, John Wiley & Sons, Inc.

Institution, B. S. 2013. *ISO/IEC 27001:2013 - Information Technology -- Security Techniques -- Information Security Management Systems -- Requirements.*, British International Institute.

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., and Longva, O. H. 2009. "A Framework for Incident Response Management in the Petroleum Industry," *International Journal of Critical Infrastructure Protection* (2:1), pp. 26–37.

Jalali, M. S., Siegel, M., and Madnick, S. 2018. "Decision-Making and Biases in Cybersecurity Capability Development: Evidence from a Simulation Game Experiment," *The Journal of Strategic Information Systems*, pp. 1–17.

Johnson, L. R. 2013. *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*, Newnes.

Kevin, B., Yang, C., Olson, D., and Sheu, C. 2014. "The Impact of Advanced Analytics and Data Accuracy on Operational Performance: A Contingent Resource Based Theory (RBT) Perspective," *Decision Support Systems* (59), pp. 119–126.

Khansa, L., and Liginlal, D. 2009. "Valuing the Flexibility of Investing in Security Process Innovations," *European Journal of Operational Research* (192:1), pp. 216–235.

Kohavi, R., Rothlender, N., and Simoudis, E. 2002. "Emerging Trends in Business Analytics," *Communications of the ACM* (45:8), pp. 45–48.

Kohli, R. 2007. "Innovating to Create IT-Based New Business Opportunities at United Parcel Service.," *MIS Quarterly Executive* (6:4), pp. 199–210.

Krishnamoorthi, S., and Mathew, S. K. 2018. "Business Analytics and Business Value: A Comparative Case Study," *Information and Management* (55:5), pp. 643–666.

Langley, A. 1999. "Strategies for Theorizing from Process Data," *Academy of Management Review* (24:4), pp. 691–710.

Langley, A. 2007. "Process Thinking in Strategic Organization," *Strategic Organization* (5:3), pp. 271–282.

Lee, O. K., Sambamurthy, V., Lim, K. H., and Wei, K. K. 2015. "How Does IT Ambidexterity Impact Organizational Agility?," *Information Systems Research* (26:2), pp. 398–417.

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

Lim, E.-P., Chen, H., and Chen, G. 2013. "Business Intelligence and Analytics: Research Directions," *ACM Transactions on Management Information Systems* (3:4), pp. 1–10.

Ling-yee, L. 2007. "Marketing Resources and Performance of Exhibitor Firms in Trade Shows: A Contingent Resource Perspective," *Industrial Marketing Management* (36:3), pp. 360–370.

Locke, K., Golden-Biddle, K., and Feldman, M. S. 2008. "Making Doubt Generative: Rethinking the Role of Doubt in the Research Process," *Organization Science* (19:6), INFORMS, pp. 907–918.

Lu, Y., and Ramamurthy, K. R. 2011. "Understanding the Link Between Information Technology Capability and Organizational Agility: An Empirical Examination," *MIS Quarterly* (35:4), pp. 931–954.

Mathiassen, L., and Pries-Heje, J. 2006. "Business Agility and Diffusion of Information Technology," *European Journal of Information Systems*, pp. 116–119.

Maynard, S., Onibere, M., and Ahmad, A. 2018. "Defining the Strategic Role of the Chief Information Security Officer," *Pacific Asia Journal of the Association for Information Systems* (10:3), pp. 61–85.

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

Nazir, S., and Pinsonneault, A. 2012. "IT and Firm Agility: An Electronic Integration Perspective," *Journal of the Association for Information Systems* (13:3), pp. 150–171.

Newbert, S. 2007. "Empirical Research on the Resource-Based View of the Firm: An Assessment and Suggestions for Future Research," *Strategic Management Journal* (28:2), pp. 121–146.

NIST. 2011. "Managing Information Security Risk Organization, Mission, and Information System View," *NIST Special Publication 800-39*.

Nnoli, H., Lindskog, D., Zavarsky, P., Aghili, S., and Ruhl, R. 2012. "The Governance of Corporate Forensics Using COBIT, NIST and Increased Automated Forensic Approaches," in *Proceedings of Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, IEEE., pp. 734–741.

Oliveira, M. P. V. De, McCormack, K., and Trkman, P. 2012. "Business Analytics in Supply Chains - The Contingent Effect of Business Process Maturity," *Expert Systems with Applications* (39:5), pp. 5488–5498.

Onibere, M., Ahmad, A., and Maynard, S. 2017. "The Chief Information Security Officer and the Five Dimensions of a Strategist," in *PACIS 2017 Proceedings*, pp. 1–13.

Van Oosterhout, M., Waarts, E., and Van Hillegersberg, J. 2006. "Change Factors Requiring Agility and Implications for IT," *European Journal of Information Systems* (15:2), pp. 132–145.

Overby, E., Bharadwaj, A., and Sambamurthy, V. 2006. "Enterprise Agility and the Enabling Role of Information Technology," *European Journal of Information Systems* (15:2), pp. 120–131.

Paré, G. 2004. "Investigating Information Systems with Positivist Case Study Research," *Communications of the Association for Information Systems* (13:1), pp. 233–264.

Park, S., Ruighaver, A. B., Maynard, S. B., and Ahmad, A. 2012. "Towards Understanding Deterrence: Information Security Managers' Perspective," in *International Conference on IT Convergence and Security* (Vol. September), pp. 21–37.

Park, Y., El Sawy, O. A., and Fiss, P. 2017. "The Role of Business Intelligence and Communication Technologies in Organizational Agility," *Journal of the Association for Information Systems* (18:9), pp. 648–686.

Parker, D. B. 2007. "Risks of Risk-Based Security," *Communications of the ACM* (50:3), p. 120.

Patton, M. Q. 2015. *Qualitative Evaluation and Research Methods*, Beverly Hills, CA: Sage.

Pavlou, P. A., and El Sawy, O. A. 2006. "From IT Leveraging Competence to Competitive Advantage in Turbulent Environments: The Case of New Product Development," *Information Systems Research* (17:3), pp. 198–227.

Pavlou, P. A., and El Sawy, O. A. 2011. "Understanding the Elusive Black Box of Dynamic Capabilities," *Decision Sciences* (42:1), pp. 239–273.

Peltier, T. R. 2010. *Information Security Risk Analysis*, Auerbach publications.

Peteraf, M., Di Stefano, G., and Verona, G. 2013. "The Elephant in the Room of Dynamic Capabilities: Bringing Two Diverging Conversations Together," *Strategic Management Journal* (34:12), pp. 1389–1410.

Phillips-Wren, G., Lakshmi S., I., Kulkarni, U., and Ariyachandra, T. 2015. "Business Analytics in the Context of Big Data: A Roadmap for Research," *Communications of the AIS* (37:1), pp. 448–472.

Piccoli, G., and Watson, R. T. 2008. "Profit from Customer Data by Identifying Strategic Opportunities and Adopting the 'Born Digital' Approach.," *MIS Quarterly Executive* (7:3), pp. 113–122.

Pierazzi, F., Casolari, S., Colajanni, M., and Marchetti, M. 2016. "Exploratory Security Analytics for Anomaly Detection," *Computers & Security* (56), pp. 28–49.

Popovič, A., Hackney, R., Simões, P., and Jakli, J. 2012. "Towards Business Intelligence Systems Success: Effects of Maturity and Culture on Analytical Decision Making," *Decision Support Systems* (54), pp. 729–739.

Raschke, R. L. 2010. "Process-Based View of Agility: The Value Contribution of IT and the Effects on Process Outcomes," *International Journal of Accounting Information Systems* (11:4), pp. 297–313.

Ray, G., Barney, J. B., and Muhanna, W. A. 2004. "Capabilities, Business Processes, and Competitive Advantage: Choosing the Dependent Variable in Empirical Tests of the Resource-Based View," *Strategic Management Journal*, pp. 23–37.

Rees, J., and Allen, J. 2008. "The State of Risk Assessment Practices in Information Security: An Exploratory Investigation," *Journal of Organizational Computing and Electronic Commerce* (18:4), pp. 255–277.

Roberts, N., and Grover, V. 2012. "Leveraging Information Technology Infrastructure to Facilitate a Firm's Customer Agility and Competitive Activity: An Empirical Investigation," *Journal of Management Information Systems* (28:4), pp. 231–270.

Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., and Perl, S. J. 2014. "Computer

Security Incident Response Team Development and Evolution," *IEEE Security & Privacy* (12:5), pp. 16–26.

Russom, P., Stodder, D., and Halper, F. 2014. "Real-Time Data , BI , and Analytics," *TDWI Best Practices Report, Fourth Quarter* (4).

Sambamurthy, V., Bharadwaj, A., and Grover, V. 2003. "Shaping Agility through Digital Options: Reconceptualizing the Role of Information Technology in Contemporary Firms," *MIS Quaterly* (27:2), pp. 237–263.

Seddon, P. B., Constantinidis, D., Tamm, T., and Dod, H. 2017. "How Does Business Analytics Contribute to Business Value?," *Information Systems Journal* (27:3), pp. 237–269.

Shameli-sendi, A., Aghababaei-barzegar, R., and Cheriet, M. 2016. "Taxonomy of Information Security Risk Assessment (ISRA)," *Computers and Security* (57), pp. 14–30.

Shanks, G., and Bekmamedova, N. 2012. "Achieving Benefits with Business Analytics Systems: An Evolutionary Process Perspective," *Journal of Decision Systems* (21:3), pp. 231–244.

Shanks, G., and Bekmamedova, N. 2013. "Creating Value With Business Analytics In The Supply Chain," *European Conference on Information Systems 2013 Completed Research*, pp. 1–12.

Shanks, G., Sharma, R., Seddon, P., and Reynolds, P. 2010. "The Impact of Strategy and Maturity on Business Analytics and Firm Performance: A Review and Research Agenda," *ACIS 2010 Proceedings*, pp. 1–11.

Sharma, R., Mithas, S., and Kankanhalli, A. 2014. "Transforming Decision-Making Processes: A Research Agenda for Understanding the Impact of Business Analytics on Organisations," *European Journal of Information Systems* (23:4), pp. 433–441.

Shedden, P., Ahmad, A., and Ruighaver, A. B. 2010. "Organisational Learning and Incident Response : Promoting Effective Learning through the Incident Response Process," in *Proceedings of the 8th Australian Information Security Mangement Conference*, pp. 131–142.

Shedden, P., Ahmad, A., and Ruighaver, A. B. 2011. "Informal Learning in Security Incident Response Teams," in *Proceedings of 2011 Australasian Conference on Information System (ACIS)*, pp. 1–11.

Shedden, P., Ahmad, A., Smith, W., Tscherning, H., and Scheepers, R. 2016. "Asset Identification in Information Security Risk Assessment: A Business Practice Approach," *Communications of the Association for Information Systems* (39:1), pp. 297–320.

Shedden, P., Ruighaver, T., and Atif, A. 2010. "Risk Management Standards – the Perception of Ease of Use," *Journal of Information System Security* (6:3), pp. 1–13.

Shedden, P., Scheepers, R., Smith, W., and Ahmad, A. 2011. "Incorporating a Knowledge Perspective into Security Risk Assessments," *VINE Journal of Knowledge Management* (41:2), pp. 152–166.

Shedden, P., Smith, W., and Ahmad, A. 2010. "Information Security Risk Assessment: Towards a Business Practice Perspective," in *8th Australian Information Security Management Conference Proceedings*, pp. 555–590.

Shedden, P., Smith, W., Scheepers, R., and Ahmad, A. 2009. "Towards a Knowledge Perspective in Information Security Risk Assessments – an Illustrative Case Study," in *20th Australasian Conference on Information Systems*, pp. 74–84.

Shollo, A., and Galliers, R. D. 2016. "Towards an Understanding of the Role of Business Intelligence Systems in Organisational Knowing," *Information Systems Journal* (26), pp. 339–367.

Smith, W. K. 2014. "Dynamic Decision Making : A Model of Senior Leaders Managing Strategic Paradoxes," *Academy of Management Journal* (57:6), pp. 1592–1623.

von Solms, R., and van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp. 97–102.

Spears, J. L., and Barki, H. 2010. "User Participation in Information Systems Security Risk Management," *MIS Quarterly* (34:3), pp. 503-A5.

Stoll, M. 2015. "From Information Security Management to Enterprise Risk Management," *Innovations and Advances in Computing, Informatics, Systems Sciences, Networking and Engineering* (13:1), pp. 9–16.

Strauss, A., and Corbin, J. 2014. *Basics of Qualitative Research: Tecchniques and Procedures for Developing Grounded Theory*, Sage.

Suddaby, R. 2006. "From the Editors: What Grounded Theory Is Not," *Academy of Management Journal*, pp. 633–642.

Talabis, M., McPherson, R., Miyamoto, I., and Martin, J. 2014. *Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data*, Syngress.

Tallon, P. P. 2008. "Inside the Adaptive Enterprise: An Information Technology Capabilities Perspective on Business Process Agility," *Information Technology and Management* (9:1), pp. 21–36.

Tallon, P. P., and Pinsonneault, A. 2011. "Competing Perspectives on the Link between Strategic Information Technology Alignment and Organizational Agility: Insigths from a Mediation Model," *MIS Quarterly* (35:2), pp. 463–486.

Tan, T., Ahmad, A., and Ruighaver, A. T. 2003. "Incident Handling: Where the Need for Planning Is Often Not Recognised," in *Proceedings of the 1st Australian Computer, Network & Information Forensics Conference*, pp. 1–10.

Tan, T., Maynard, S., Ahmad, A., and Ruighaver, T. 2017. "Information Security Governance: A Case Study of the Strategic Context of Information Security," in *Pacific Asia Conference on Information Systems (PACIS)*, pp. 1–15.

Tan, T., Ruighaver, A. B., and Ahmad, A. 2010. "Information Security Governance: When Compliance Becomes More Important than Security," in *The IFIP TC-11 24th International Information Security Conference*, pp. 55–67.

Teece, D. J. 2000. "Strategies for Managing Knowledge Assets: The Role of Firm Structure and Industrial Context," *Long Range Planning* (33:1), pp. 35–54.

Teece, D. J. 2007. "Explicating Dynamic Capabilities: The Nature and Microfoundations of (Sustainable) EnterprisePerformance," *Strategic Management Journal* (28:13), pp. 1319–1350.

Teece, D. J. 2018. "Business Models and Dynamic Capabilities," *Long Range Planning* (51:1), pp. 40–49.

Teece, D. J., Pisano, G., and Shuen, A. 1997. "Dynamic Capabilities and Strategic Management," *Strategic Management Journal* (18:7), pp. 509–533.

Teece, D., Peteraf, M., and Leih, S. 2016. "Dynamic Capabilities and Organizational Agility: Risk, Uncertainity, and Strategy in the Innovation Economy," *California Management Review* (58:4), pp. 13–36.

Teece, D., and Pisano, G. 1994. "The Dynamic Capabilities of Firms: An Introduction," *Industrial and Corporate Change* (3:3), pp. 537–556.

Tøndel, I. A., Line, M. B., and Jaatun, M. G. 2014. "Information Security Incident Management: Current Practice as Reported in the Literature," *Computers & Security* (45), pp. 42–57.

Townsend, M., Le Quoc, T., Kapoor, G., Hu, H., Zhou, W., and Piramuthu, S. 2018. "Real-Time Business Data Acquisition: How Frequent Is Frequent Enough?," *Information and Management* (55:4), pp. 422–429.

Trauth, E. M. 2001. "Qualitative Research in IS: Issues and Trends," *European Journal of Information Systems* (11:1), pp. 83–83.

Trkman, P., McCormack, K., De Oliveira, M. P. V., and Ladeira, M. B. 2010. "The Impact of Business Analytics on Supply Chain Performance," *Decision Support Systems* (49:3), pp. 318–327.

Wade, M., and Hulland, J. 2004. "Review: The Resource-Based View and Information Systems Research: Review, Extension, and Suggestions for Future Research," *MIS Quarterly* (28:1), pp. 107–142.

Wang, E. T. G., Hu, H. F., and Hu, P. J. H. 2013. "Examining the Role of Information Technology in Cultivating Firms' Dynamic Marketing Capabilities," *Information and Management* (50:6), pp. 336–

343.

Watson, H. 2001. "Recent Developments in Data Warehousing," *Communications of the Association for Information Systems* (8:1), pp. 1–25.

Watson, H. 2014. "Tutorial : Big Data Analytics : Concepts , Technologies , and Applications," *Communications of the Association for Information Systems* (34:1), pp. 1–24.

Watson, H. J., and Wixom, B. H. 2007. "The Current State of Business Intelligence," *IEEE Computer Society* (40:9), pp. 96–99.

Watson, H. J., Wixom, B. H., Hoffer, J. a., Anderson-Lehman, R., and Reynolds, A. M. 2006. "Real-Time Business Intelligence: Best Practices at Continental Airlines," *Information Systems Management* (23:1), pp. 7–18.

Watson, R. T. 2015. "Beyond Being Systematic in Literature Reviews in IS," *Journal of Information Technology* (30:2), pp. 185–187.

Webb, J., Ahmad, A., Maynard, S. B., and Shanks, G. 2014. "A Situation Awareness Model for Information Security Risk Management," *Computers & Security* (44:March 2016), pp. 1–15.

Webster, J., and Watson, R. T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *MIS Quarterly* (26:2), Xiii–Xxi.

Weishäupl, E., Yasasin, E., and Schryen, G. 2015a. "IT Security Investments Through the Lens of the Resource-Based View : A New Theoretical Model and Literature Review," *ECIS 2015 Proceedings* (2014), pp. 1–19.

Weishäupl, E., Yasasin, E., and Schryen, G. 2015b. "A Multi-Theoretical Literature Review on Information Security Investments Using the Resource-Based View and the Organizational Learning Theory," in *Thirty Sixth International Conference on Information Systems*, pp. 1–22.

Werlinger, R., and Botta, D. 2007. "Detecting, Analyzing and Responding to Security Incidents: A

Qualitative Analysis," *Proceedings of the EECE 512 Mini-Conference on Computer Security*, pp. 24–34.

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.

Winter, S. G. S. 2003. "Understanding Dynamic Capabilities," *Strategic Management Journal* (24:10), pp. 991–995.

Wixom, B., and Goul, M. 2014. "The Current State of Business Intelligence in Academia: The Arrival of Big Data," *Communications of the AIS* (34:1), pp. 1–13.

Wixom, B. H., Yen, B., and Relich, M. 2013. "Maximizing Value from Business Analytics.," *MIS Quarterly Executive* (12:2), pp. 111–123.

Xu, Z., Frankwick, G. L., and Ramirez, E. 2016. "Effects of Big Data Analytics and Traditional Marketing Analytics on New Product Success: A Knowledge Fusion Perspective," *Journal of Business Research* (69:5), pp. 1562–1566.

Yin, R. K. 2017. *Case Study Research and Applications: Design and Methods*, Sage publications.

Zahra, S. A., Sapienza, H. J., and Davidsson, P. 2006. "Entrepreneurship and Dynamic Capabilities: A Review, Model and Research Agenda," *Journal of Management Studies* (43:4), pp. 917–955.

Zollo, M., Winter, S. G. 2002. "Deliberate Learning and the Evolution of Dynamic Capabilities," *Organization Science* (13:3), pp. 339–351.

APPENDIX A. INTERVIEW GUIDE

This appendix presents the questionnaire that was used to guide the semi-structured interviews. Please note that this questionnaire was an approximate guide only, and its purpose was to encourage the interviewees to reflect on the research themes, rather than constrain this discussion. The phrasing of the questions varied based on the role of the interviewee and the organizational context. Depending on the interviewee's role and experience (e.g., top-level managers, middle level senior managers, cybersecurity analysts and data analysts), the focal themes also varied from interview to interview. Not all questions were necessarily covered in every interview, and some themes were covered in greater depth than others.

How can organizations improve agility in their cybersecurity incident response process using real-time analytics?

Interview Guide

Interviewee Background

Please describe your background and current role in the organisation (incl. educational and professional background, cybersecurity related experience, business analytics related experience, current role, reporting line, key deliverables).

Theme 1: Real-Time Analytics in Cybersecurity Incident Response

1. What does real-time analytics mean to you?
2. Describe the evolution of analytics in your organisation?
    a. What were the key milestones that you targeted and achieved?
    b. What is the status at present?
3. Describe the potential role that analytics may play in the process of cybersecurity incident response.
4. Describe how you have integrated real-time analytics into your incident response process.
    a. How much were you and other top management team members involved in this integration?
    b. What are the major challenges and obstacles you encountered? How did you or your top leadership team overcome these challenges?
    c. What are the sources of data for real-time analytics? How do you manage your cybersecurity data and analytical architecture?
    d. What kind of reporting and analysis are you performing on cybersecurity data related to risk management and incident response? What type of analytical models are you using?
5. Who are the consumers of insights generated from analytics applications? How are insights delivered? (Dashboards, reports, scorecards etc.)
6. Describe the importance of self-service analytics in building real-time analytics capability?
7. Describe how your analytics and incident response group coordinate with each other (formal meetings, online platforms). Are they co-located?

8. What skillset and character traits do you look for when hiring people for cybersecurity analytics positions in your organisation? How do you determine if the new person will fit and compliment your organisation? How do you determine if you have the right mix of analytics people?

Theme 2: Impact of Using Real-time Analytics on Cybersecurity Incident Response

9. Describe the incident response process from initial identification to closure.
10. Describe how important it is to be proactive and dynamic when it comes to executing cybersecurity incident response?
11. What role does analytics play in becoming dynamic in cybersecurity risk management and incident response?
12. Give some examples of situations when top leadership involvement was critical for implementing a new analytics related initiative. How was leadership involvement solicited and managed?
13. What are some of the key risk indicators that you monitor, analyse and measure? Why?
14. Describe how you determine if your risk management and incident response process is effectively protecting your enterprise.
15. What cybersecurity risk assessment methods and techniques are you using in your organisation?
16. Give a few examples of innovative ideas that you have incorporated into your incident process that have resulted in better execution of your incident response process?
17. Describe what you did in a situation where a significant threat was discovered. Specifically, how was the threat discovered? How did you decide it was significant? How did you decide what to do about it? And how did you determine if your actions were successful or not?

Theme 3: Enterprise Security Performance:

18. What specific benefits have you realized by using analytics in your cybersecurity incident response process?
    a. Can you give some examples on how the use of analytics has influenced the quality of cybersecurity related decisions in your enterprise?
    b. Can you give any figures on the value analytics brings (e.g. $ saved/lost, time saved/wasted, performance optimization etc.)?
19. Describe what measures do you use to evaluate the performance of your cybersecurity processes?

20. Describe how analytics in cybersecurity has impacted your enterprise's security performance during the last 2 or 3 years.
21. What do you think would be the best way to determine Return on Security Investment? Are there any other ways to do it?
22. Describe how you develop your cybersecurity budget? How do you justify spending and resource requests to the business?
23. Give some examples of organisational cybersecurity measures. Which of these measures describe the overall enterprise security performance the best?

Thank you for finding time to contribute to this research project!

Author/s:
Naseer, Humza

Title:
A framework of dynamic cybersecurity incident response to improve incident response agility

Date:
2018

Persistent Link:
http://hdl.handle.net/11343/221356

File Description:
A framework of dynamic cybersecurity incident response to improve incident response agility - Complete Thesis