2016

Enhancing Information Security Risk Management with Security Analytics: A Dynamic Capabilities Perspective

Humza Naseer
University of Melbourne, humza.naseer@unimelb.edu.au

Graeme Shanks
University of Melbourne, gshanks@unimelb.edu.au

Atif Ahmad
University of Melbourne, atif@unimelb.edu.au

Sean Maynard
University of Melbourne, sean.maynard@unimelb.edu.au

Enhancing Information Security Risk Management with Security Analytics: A Dynamic Capabilities Perspective

Humza Naseer
Department of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: humza.naseer@unimelb.edu.au

Graeme Shanks
Department of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: gshanks@unimelb.edu.au

Atif Ahmad
Department of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: atif@unimelb.edu.au

Sean Maynard
Department of Computing and Information Systems
The University of Melbourne
Melbourne, Australia
Email: sean.maynard@unimelb.edu.au

Abstract

The importance of information security risk management (ISRM) and its potential strategic role in protecting organisational information assets is widely studied in literature. Less attention is given to how ISRM can be enhanced using security analytics to contribute to a competitive advantage. This paper proposes a model showing that security analytics capabilities (the ability to effectively use security data for informed security related decision making) and ISRM capabilities (the ability to effectively identify and protect organizational information assets) indirectly influence competitive advantage in ISRM through two key mediating links: *analytics-enabled ISRM capabilities* (the ability to effectively leverage insights gleaned from security data to make informed ISRM decisions) and *ISRM dynamic capabilities* (the ability to reconfigure analytics-enabled ISRM capabilities to address turbulent environments). Environmental turbulence moderates the process by which security analytics and ISRM capabilities influence competitive advantage. The paper concludes by calling for evaluation and refinement of the research model.

Keywords Security Analytics, Strategic Risk Management, Environmental Turbulence, Dynamic Capabilities, Information Security Management

1 Introduction

Information Security Risk Management (ISRM) is a continuous process that enables an organisation to identify, analyse and control risks to its information assets (such as a manufacturing process, a product design, a negotiating strategy or sensitive personal data) (Spears and Barki 2010). Effective ISRM is essential to the success of any organisation. Despite numerous studies that examine the critical role of ISRM in protecting the organisational information assets (Anderson and Choobineh 2008; Shedden et al. 2011; Webb et al. 2014), the question of how the ISRM process can be enhanced using security analytics and thereby contribute to a competitive advantage has received relatively less attention. This perspective is important as answers to this question enable organisations to better understand the strategic role of ISRM and the importance of developing suitable *ISRM capabilities* (the ability to effectively identify and protect organisational information assets).

Organisations use business analytics (BA) in order to achieve their business objectives by building two types of applications (1) reporting and (2) analysis (Davenport et al. 2010; Eckerson 2012). These applications assist in building predictive models to forecast and optimise business processes for enhanced business performance (Chen et al. 2012; Davenport and Harris 2007). Most of the extant BA literature has predominantly analysed the BA capabilities at a firm-level and argues that BA capabilities provide benefits to organizations and contribute to firm performance. This study develops a process-level construct of BA following Oliveira et al. (2012), Pavlou and El Sawy (2006) who argue that a process-level analysis, as opposed to firm-level analysis is the most appropriate level for realising the strategic benefits of BA.

Building on the BA capabilities literature, we introduce and develop the construct of *security analytics capabilities* and define it as the ability to effectively use data in generating security-related insights and actions based on security data. We conceptualise the security analytics capabilities construct in the context of using BA in ISRM. As information security risks and threats are dynamic in nature and are increasing on a daily basis in terms of frequency and complexity, organisations need to transition from a reactive to a proactive ISRM approach (Baskerville 2005). Security analytics capabilities assist in this transition with a potential to contribute to a competitive advantage in ISRM as it does in other business processes including supply chain management (using supply chain analytics capabilities), marketing (using marketing analytics capabilities) and customer relationship management (using customer analytics capabilities) (Germann et al. 2013; Naseer et al. 2016; Piccoli and Watson 2008; Trkman et al. 2010).

This research utilises the dynamic-capability view (DCV) by extending the resource-based view (RBV) to examine the influences of dynamic markets (Barney 1991). The RBV suggests that organisations can achieve competitive advantage by creating unique capabilities through the bundling of resources (Barney 1991). The DCV however argues that the organisations should build, integrate and reconfigure resources in order to adapt to the volatile environment (Helfat et al. 2009). Therefore, in situations involving dynamic and fast changing environments such as information security risks and threats, DCV explains firm competitiveness more effectively than RBV (Teece et al. 1997). For this reason, we propose that security analytics and ISRM are specific capabilities that can help organization to (1) better protect their information assets and thus sustain their competitive advantage and (2) innovate and develop new information assets to achieve competitive advantage in turbulent environments.

Another argument in the BA literature is whether BA-related capabilities influence competitive advantage indirectly or directly (Wade and Hulland 2004). Recent BA literature has questioned a direct impact of BA-related capabilities on competitive advantage, arguing for the existence of mediating links (e.g., Shanks et al. 2010; Someh and Shanks 2013). Extending this indirect view, we propose a model to explain the mechanism by which security analytics and ISRM capabilities can contribute to a competitive advantage in ISRM within turbulent environments.

The paper proceeds as follows: Section 2 describes our theoretical perspective. Section 3 introduces and conceptualises the proposed constructs by reviewing the extant literature on BA and ISRM. Section 4 describes the research model and explains how security analytics and ISRM capabilities indirectly influence competitive advantage in ISRM through the two proposed capabilities i.e. ISRM dynamic capabilities and analytics-enabled ISRM. Finally, section 5 concludes the paper by calling for further empirical work to evaluate and refine the research model.

2 The Resource Based View and Dynamic Capabilities

The RBV argues that organizations can gain competitive advantage by developing bundles of resources and/or capabilities (Barney 1991; Newbert 2007; Wade and Hulland 2004). Organisational resources may be tangible or intangible, and include organisational routines and processes, people and their skills and knowledge, and technology including data infrastructure and applications. BA systems and ISRM processes have been recognized as having the potential for creating and sustaining competitive advantage (Ahmad et al. 2014; Davenport and Harris 2007), given that the resources or capabilities have the attributes of being valuable, rare, inimitable and non-substitutable (VRIN properties) (Barney 1991; Newbert 2007).

Within the RBV, organisational capabilities are a critical contributing factor of firm performance (Aral and Weill 2007). However, this view has been criticised as being too static in turbulent environments and dynamic capabilities were proposed as a means of renewing and reconfiguring organisational resources to respond to rapidly changing environments (Teece et al. 1997). Dynamic capabilities are defined as “the capacity of an organisation to purposefully create, extend or modify its resource base” (Helfat et al. 2009, p. 4). Wheeler (2002) decomposes dynamic capabilities into four simpler capabilities: choosing new technologies; matching technologies with economic opportunities; executing business innovation for growth; and assessing customer value.

3 Literature Review

A systematic literature review was conducted using a methodology commonly used in information systems as described by Webster and Watson (2002). The manner in which articles are identified, interpreted, and analysed is clearly articulated *a priori*, making the study (to a degree) repeatable and reduces the possibility of bias (Watson 2015). The resulting study appraises the BA and ISRM literature to investigate the research question by developing and refining the research model (see Figure 1).

As a first step, we examined articles from key information systems journals and conferences using the keywords: ‘business analytics’, ‘security analytics’ ‘risk assessment’ and ‘information security risk management’. These searches identified over 120 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 (how can the use of security analytics contribute to a competitive advantage in information security risk management?). This resulted in 50 articles for in-depth review and coding. In an effort to extend the search outside the original set of journals, 20 additional papers of potential interest were also identified from reference list of reviewed articles. We used DCV and RBV to synthesize the literature conceptually. Out of 70 coded articles, 45 included variables of interest. These articles were analysed and classified into the paths shown in Figure 1.

3.1 From Business Analytics to Security Analytics Capabilities

Organisations use the practice of BA to develop two types of applications (reporting and analysis) that help them to analyse critical business data to generate new insights about the business and markets (Chen et al. 2012). These new insights can then be used to take actions and thus enable the practice of ‘evidence-based decision making’ (Davenport and Harris 2007). The real value of BA practice in any organization can be described as a simple workflow, turning data into insights and then into actions (preferably profitable actions) (Eckerson 2012). The technologies and solutions that organizations build as part of a BA initiative to generate new insights include data warehouses, data marts, on-line analytical processing, visualization, big data analytics, and data mining (Chen et al. 2012; Eckerson 2012).

Many case studies and success stories in both research and practitioner literature provide the evidence that BA capabilities deliver significant benefits to organizations and contribute to firm performance (Davenport and Harris 2007; Piccoli and Watson 2008; Shanks et al. 2010; Trkman et al. 2010). These success stories are further encouraging organizations to collect and analyse new sources of data as they provide new insights. Security data is one of the new data sources recently gaining a lot of attention (Chen et al. 2012). 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). BA presents organizations with a unique opportunity to harness this security data by using ‘security analytics capabilities’ and thereby enabling the practice of evidence-based decision making in the process of ISRM. Therefore, this study develops a process-level construct of BA following Oliveira et al. (2012), Pavlou and El Sawy (2006) who argue that a process as opposed to firm-level of analysis is the most appropriate level for observing the strategic benefits of BA.

The notion of security analytics has recently been highlighted in the BA and ISRM literature, however, there is no clear definition of what exactly security analytics entails (Chen et al. 2012; Naseer et al.

2016). We propose security analytics as a capability organizations can develop, and we define it as the ability to effectively use data in generating security-related insights and actions based on security data. Thus, a security analytics capability exists in an organization if: (1) it collects and analyses security data using BA (security intelligence generation), (2) distributes the security insights to security managers (security insights dissemination), and (3) security managers decision-making is subsequently based on the security insights gleaned from the aforementioned security data (responsiveness to security insights). We identify security insights generation, security insights dissemination, and responsiveness to security insights as the three key dimensions of security analytics capabilities. Since the construct of security analytics capabilities is relatively new and unexplored, understanding the relationship between security analytics capabilities and competitive advantage is a contribution to the literature.

3.2 ISRM Capabilities

Information security risk management is a continuous process that helps organizations to identify, prioritize and control risks specific to their information assets (Alberts and Dorofee 2002; Spears and Barki 2010). Organizations use the information security risk assessment process, a subset of the ISRM process to (1) identify the information assets that need protection, (2) identify threats that might impact the assets, (3) identify security vulnerabilities in the assets that might be exploited, and (4) identify specific risks (scenarios) and estimate their likelihood and potential impact (Shedden et al. 2011). Based on the risk assessment, appropriate controls are implemented and then monitored to measure the effectiveness of ISRM process (Shedden et al. 2011). ISRM Capabilities are therefore defined as the ability to effectively identify, analyse, control and protect organisational information assets. Risk assessment capability and security control monitoring capability are the two key dimensions of ISRM capabilities.

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 information 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. Risk assessment complexity increases when organizations need to protect a large number of information assets (Baskerville et al. 2014). Different types of information 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 information assets among different targets, such as networks, software, data and physical components increases the threats and thereby complexity (Jerman-Blažič 2008). Finally, complexity also increases when there are different types of data that provide information about information assets (Talabis et al. 2014).

There is considerable evidence in the literature that suggests two trends in ISRM organisational practice (1) ISRM lacks evidence based decision making (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 (Khansa and Liginlal 2009; Naseer et al. 2016; Rees and Allen 2008). This implies that security managers are not incorporating important security data into their ISRM decision making process, do not have holistic security awareness, and are therefore not practicing evidence-based decision making in ISRM.

The ISRM process is not a separate entity isolated from other business processes; rather it is an integral part of managing a modern business that helps organizations in generating and sustaining competitive advantage over their business rivals (Chen et al. 2012; Talabis et al. 2014). The traditional approach to address information security risks and threats by building bigger walls (antivirus software and firewalls) while still crucial is no longer sufficient. A holistic approach to ISRM across the whole organisation including its supply chains, networks and the larger ecosystem is required. Therefore, we argue that organisations need to move the ISRM process from a mid-level technical function up to the board room and top management where strategic decisions are made. Furthermore, we propose that the interaction between security analytics and ISRM capabilities can help organisation to practice evidence based decision making in ISRM and conduct risk assessments on continuous basis.

3.3 Analytics-Enabled ISRM Capabilities

Analytics-enabled ISRM capabilities include skills and practices of business managers in leveraging analytical tools, methods and security insights gleaned from security data to make informed ISRM decisions (Talabis et al. 2014). This is based on the RBV which suggests that security analytics and ISRM capabilities interact with each other to generate organizational benefits by developing higher-order analytics-enabled ISRM capabilities with emergent properties (for example sophisticated analysis on security data to build statistical models, high-quality reporting for monitoring security controls and visualization) (Wade and Hulland 2004). These higher-order analytics-enabled ISRM capabilities, in turn, contribute to competitive advantage in ISRM. The concept of higher-order capabilities was coined by Grant (1996) that explains how IT provides a basis for developing hierarchy of higher-order business capabilities. Analytics-enabled risk assessment capability and analytics-enabled security control monitoring capability are the two key dimensions of analytics-enabled ISRM capabilities.

3.4 ISRM Dynamic Capabilities

In contrast with analytics-enabled ISRM capabilities that help organisations to leverage reporting and analysis applications in ISRM, dynamic capabilities are strategic processes whose purpose is to shape analytics-enabled ISRM capabilities. Dynamic capabilities have been defined as “the ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments” (Teece et al. 1997, p. 517). Furthermore, dynamic capabilities have been viewed as strategic options (Pavlou and El Sawy 2006), and they can allow organisations to shape their existing analytics-enabled ISRM capabilities when the opportunity or need arises.

In ISRM, dynamic capabilities can help organisations reconfigure existing analytics-enabled ISRM capabilities so they can build reporting and analytics applications that better protect their information assets and recognise opportunities to develop new information assets. Both analytics-enabled ISRM capabilities and ISRM dynamic capabilities are composed of a complementary set of capabilities that reflect the effectiveness in executing ISRM business process.

Wheeler (2002) identified four dynamic capabilities (*choosing* emerging/enabling technologies, *matching* with economic opportunities, *executing* business innovation for growth and *assessing* customer value) in his NEBIC process model that explains how organisations create business value through net-enabled innovations. We have adapted these four capabilities from NEBIC and applied them to ISRM dynamic capabilities. Therefore, four key dimensions of ISRM dynamic capabilities are to (a) *choose the ISRM innovation option*, (b) *build the ISRM innovation business case*, (c) *implement the ISRM innovation solution*, and (d) *define measures for the ISRM innovation value*.

3.5 Competitive Advantage in ISRM

We have chosen the context of using BA in ISRM to examine the relationship between the interaction of security analytics and ISRM capabilities, and competitive advantage. ISRM is the overall process which integrates the identification and analysis of risks to which the organization is exposed, the assessment of potential impacts on the business, and deciding what action can be taken to eliminate or reduce risk to acceptable level (Jerman-Blažič 2008). ISRM is a strategic process as it aims to help safeguard the confidentiality, integrity and availability (CIA) of a firm’s operations and protect its relationship with its customers and suppliers in order to counter existing and new malicious activities, both externally and internally (Anderson and Choobineh 2008).

Competitive advantage in ISRM is a more unambiguous measure of competitive advantage as compared to an aggregate organisation-wide competitive advantage measure. Ray et al. (2004) explain, “Firms can have a competitive advantage in some business activities and competitive disadvantages in others.” Thus, competitive advantage in ISRM is herein introduced as the study’s dependent variable, and the study is conducted at the process-level with the ISRM business unit as the unit of analysis, which can be either inter-firm or intra-firm (Pavlou and El Sawy 2006).

Competitive advantage in ISRM is achieved when an organization has better ISRM process effectiveness and efficiency that its competitors. ISRM process effectiveness is defined as *the ability of the ISRM process to help organizations operate in highly complex, interconnected environments using information assets that organizations depend on to accomplish their missions and to conduct important business-related functions* (Alberts and Dorofee 2002). ISRM process efficiency is defined as *the ability of the ISRM process to detect a security breach, respond to it within an acceptable period of time and return it to normal operational performance* (Whitman and Mattord 2013). Both ISRM process effectiveness and efficiency have been individually linked to enhance the overall information security process performance (Whitman and Mattord 2013).

4 The Research Model and Hypotheses

In the research model (see Figure 1 for research model and Table 1 for construct definitions), we propose two capabilities as missing links in the security analytics and ISRM capabilities-competitive advantage relationship. First, *analytics-enabled ISRM capabilities* (the ability to effectively leverage insights gleaned from security data to make informed ISRM decisions) are proposed to have direct impact on competitive advantage. Second, *ISRM dynamic capabilities* (the ability to build, integrate, and reconfigure existing analytics-enabled ISRM capabilities to address turbulent environments) are hypothesised to have an indirect impact on competitive advantage in ISRM by reconfiguring analytics-enabled ISRM capabilities (Helfat et al. 2009; Teece et al. 1997). In addition, environmental turbulence is also shown to be moderating the process by which security analytics and ISRM capabilities influence the competitive advantage in ISRM.

This perspective is crucial for dynamic and fast changing environments such as information security risks and threats. Therefore, we propose that security analytics and ISRM are the specific capabilities that help organization to (1) better protect their information assets and thus sustain their competitive advantage and (2) innovate and develop new information assets to build competitive advantage in turbulent environments.

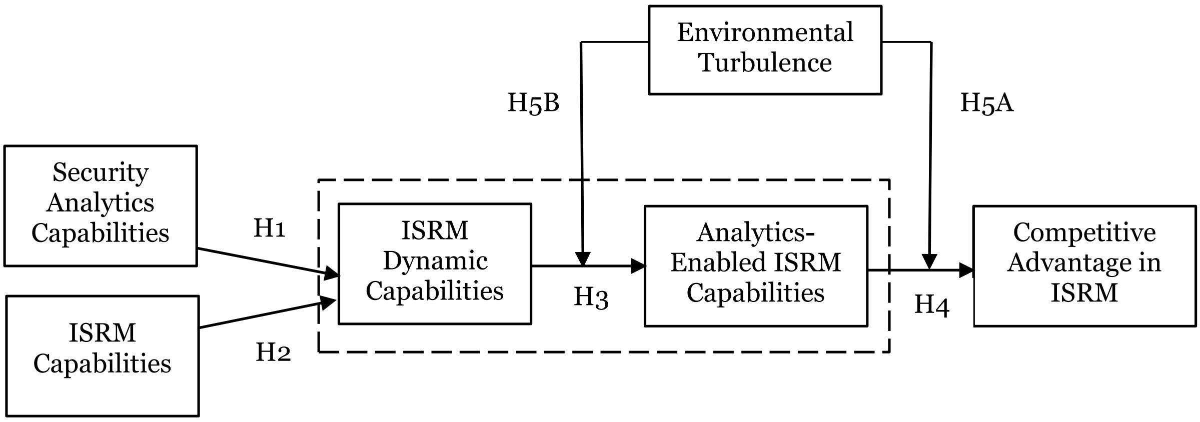
Environmental Turbulence
H5B
H5A
Security Analytics Capabilities
H1
ISRM Dynamic Capabilities
Analytics-Enabled ISRM Capabilities
Competitive Advantage in ISRM
H3
H4
ISRM Capabilities
H2

Figure 1: The Proposed Research Model

Construct	Definition	Reference
Security Analytics Capabilities	The ability to effectively use data in generating security-related insights and actions based on security data	(Davenport and Harris 2007)
ISRM Capabilities	The ability to effectively identify, analyse, control and protect organisational information assets	(Alberts and Dorofee 2002)
ISRM Dynamic Capabilities	The ability to build, integrate, and reconfigure existing analytics-enabled ISRM capabilities to address turbulent environments	(Teece et al. 1997)
Analytics-Enabled ISRM Capabilities	The ability to effectively leverage insights gleaned from security data to make informed ISRM decisions	(Talabis et al. 2014)
Competitive Advantage in ISRM	Benefits an organisation receives from using security analytics in ISRM i.e. when an organisation has better ISRM process effectiveness and efficiency than its competitors	

Table 1. Definitions of Constructs in the Research Model

4.1 The Impact of Security Analytics Capabilities and ISRM Capabilities on ISRM Dynamic Capabilities

Security analytics capabilities include skills and practices of business units (BA and security) in collecting, analysing, generating insights and taking security actions based on security data. The notion of security analytics in this study is adopted from Davenport and Harris (2007), and Talabis et al. 2014). There are four major processes within security analytics capabilities that help in turning security data into insights and actions: (1) Extracting, transforming and loading security data from disparate sources into a data warehouse (2) Performing advanced analysis on it using analytical tools and methods (3) Generating security insights and reporting them to the right people at the right time and (4) Taking actions based on the security insights. Security analytics capabilities creates a fact-based decision making culture and help security managers become proactive and make timely, data driven decisions in all information security processes.

ISRM capabilities include skills and practices of the security unit in identifying, controlling, and minimizing the impact of uncertain events (Alberts and Dorofee 2002). It empowers the functional owners (senior management of a department, business unit or group) of the organizational assets to perform their fiduciary responsibility of protecting the enterprise's informational assets in a reasonable and prudent manner (Whitman and Mattord 2013). Information security risk assessment is a major process within ISRM resources that helps in identifying and prioritizing risks specific to corporate information and assets along with assessing the impact and probability of threats occurring (Shedden et al. 2011). ISRM capabilities ensure that an enterprise has the ability required to protect its business processes, informational assets, and accomplish its mission and business objectives. Therefore, we argue that interaction of security analytics and ISRM capabilities enhance each of the four dimensions of dynamic capabilities:

Choosing ISRM innovation option: This involves identification of the opportunities for the effective use of security insights that can help an organisation to do better ISRM than its competitors. Innovation may come from new developments in BA technologies, security managers, insights generated by security, and BA experts from security data or business users (Shanks and Bekmamedova 2013; Wheeler 2002).

Build ISRM innovation business case: This involves matching economic opportunities with the ISRM innovation option by developing a business case (Wheeler 2002) that includes alignment with objectives and business strategy (Davenport and Harris 2007). Furthermore, it includes assessing each ISRM innovation option in terms of capital commitment required, risk assessment, and allocation of resources including time, people and management attention (Wheeler 2002).

Implement ISRM innovation solution: This includes the reconfiguration, integration, acquisition and divestment of resources to align with the new innovation (Wheeler 2002). It requires organisational routines for project management, change management including user training, and a culture that embraces change (Wheeler 2002).

Defining Measures for ISRM Innovation Value: This enables an organisation to assess the impact of the implemented ISRM Innovation solution. Typically the measures involve financial (e.g. revenue, costs), perceptual (e.g. customer satisfaction) and behavioural measures (e.g. rate of usage of security insights). Each of these measures has a time lag from the initial implementation of the ISRM Innovation solution. Some financial indicators will not be apparent for some time, and some perceptual measures are forward looking indicators (Wheeler 2002).

Therefore, we argue that superior security analytics and ISRM capabilities are likely to lead to superior ISRM dynamic capabilities. Subsequently we hypothesise:

H1: Security analytics capabilities have a positive impact on ISRM dynamic capabilities.

H2: ISRM capabilities have a positive impact on ISRM dynamic capabilities.

4.2 The Impact of ISRM Dynamic Capabilities on Analytics-Enabled ISRM Capabilities

In order to relate ISRM dynamic capabilities with analytics-enabled ISRM capabilities and competitive advantage in ISRM, we draw on the strategy literature that identifies the critical role of dynamic capabilities as reconfiguring functional capabilities and shaping more promising ones that better match the environment (Eisenhardt and Martin 2000). Applied to ISRM, security and BA units compete on the basis of timeliness, efficiency, and appropriateness by which their analytics-enabled ISRM capabilities can be shaped into superior new capabilities that better match the environment. For example, by innovating and recognising opportunities for reconfiguring and developing new analytics-enabled ISRM capabilities, organisation can protect their information assets proactively and efficiently than the competitors. Therefore, we argue that superior ISRM dynamic capabilities are likely to lead to superior analytics-enabled ISRM capabilities. Subsequently we hypothesise:

H3: ISRM dynamic capabilities have a positive impact on analytics-enabled ISRM capabilities.

4.3 The Impact of Analytics-Enabled ISRM Capabilities on Competitive Advantage in ISRM

Security analytics and ISRM capabilities are complementary to each other in ways that generate higher-order analytics-enabled ISRM capabilities. This interaction between security analytics and ISRM capabilities also possesses the characteristics of 'capability interconnectedness' (Teece et al. 1997). This creates causal ambiguity which makes it specifically difficult for competitors to understand the source of an organization's observed competitive advantage (Morgan et al. 2009). This implies that a competitor needs to acquire both the interconnected security analytics and ISRM capabilities of a high-performing organization to develop higher-order analytics-enabled ISRM capability so as to be able to compete away its competitive advantage (Holsapple et al. 2014; Morgan et al. 2009). We argue that higher-order analytics-enabled ISRM capability will contribute to superior competitive advantage in ISRM. Therefore, we hypothesise that:

H4: Superior analytics-enabled ISRM capabilities have a positive impact on competitive advantage in ISRM.

4.4 The Moderating Role of Environmental Turbulence

Environmental turbulence describes the general conditions of uncertainty or unpredictability because of the complexity and dynamic nature of information security risks and threats (Pavlou and El Sawy 2006). Environmental turbulence in ISRM arises from two primary sources (Baskerville 2005): First, market turbulence creates unpredictability in a sense that a risk is typically something transient that arises uniquely in each organization's environment. Second, environmental turbulence creates uncertainty that makes risk (likelihood and impact) estimation impossible.

Environmental turbulence is proposed to moderate the higher-order ISRM capabilities–competitive advantage relationship because it increases the relative advantage of reconfiguring analytics-enabled ISRM capabilities, however decreases the advantages gained from efficiently exploiting existing ones (Teece et al. 1997). Turbulent environments increase the possibility that dynamic capabilities would reconfigure new analytics-enabled ISRM capabilities. Dynamic capabilities can be viewed as strategic options that provide firms the choice to pursue new directions when the opportunities arise (Helfat et al. 2009). The higher the environmental turbulence, the more likely these options will become valuable (Sambamurthy et al. 2003).

On the contrary, stable environments reward the efficient exploitation of existing analytics-enabled ISRM capabilities (Teece et al. 1997). Because analytics-enabled ISRM capabilities demand a time-consuming, costly and often irreversible accumulation of resources, their continuous reconfiguration is likely to disrupt their value potential and efficiency (Pavlou and El Sawy 2006). Hence, environmental turbulence reduces the value of existing analytics-enabled ISRM capabilities, however it increases the value potential of dynamic capabilities. Subsequently we hypothesise:

H5A: The relationship between analytics-enabled ISRM capabilities and competitive advantage in ISRM is negatively moderated (attenuated) by environmental turbulence.

H5B: The relationship between ISRM dynamic capabilities and analytics-enabled ISRM capabilities is positively moderated (reinforced) by environmental turbulence.

5 Conclusion and Future Research

Information security risks are a constantly evolving threat to an organisation's ability to deliver its core functions, achieve its business objectives and sustain its competitive advantage. The traditional approach to address information security risks and threats by building bigger walls (antivirus software and firewalls) while still essential is no longer sufficient. A holistic approach to ISRM across the whole organisation including its supply chains, networks and the larger ecosystem is required. Therefore, effective ISRM process is essential to the success of any organisation.

Despite significant interest and investment in ISRM, there is considerable evidence in the literature that suggests: (1) ISRM lacks evidence-based decision-making, and (2) ISRM is considered to be a cost of doing business rather than an integral part of key business processes. This implies that security managers are not incorporating important security data into their ISRM decision making process, lack holistic security awareness, and are therefore not practicing evidence-based decision making in ISRM. This study addresses this gap and proposes that organisations need to move ISRM from a mid-level technical function up to the board room and top management where strategic decisions are made. Furthermore, it introduces two constructs to enable evidence-based decision-making in ISRM (1) *security analytics capabilities* (the ability to effectively use security data for informed security related decision making) and (2) *ISRM capabilities* (the ability to effectively identify and protect organizational information assets).

In this paper, we propose a model which shows that security analytics and ISRM capabilities indirectly influence competitive advantage in ISRM, an impact that is mediated by two types of capabilities (ISRM dynamic capabilities and analytics-enabled ISRM capabilities). Furthermore, the model also shows that environmental turbulence reinforces the positive impact of ISRM dynamic capabilities on analytics-enabled ISRM capabilities; however it attenuates the impact of analytics-enabled ISRM capabilities on competitive advantage in ISRM.

We also extend the construct of BA capabilities to security analytics capabilities and define it as the ability to effectively use data in generating security-related insights and actions based on security data. In particular, the paper has contributed to the literature in information security risk management and business analytics by providing detailed definitions of constructs and hypotheses in the model, grounded in both RBV and DCV. Furthermore, the research model provides a systematic means of understanding the importance of interaction between security analytics and ISRM capabilities and their contribution to a competitive advantage in ISRM.

Our study has a number of implications for security practitioners. Security managers and business executives need an accurate picture of the risks to information assets that are critical to their firm's success. They also need to have holistic information on the known information security threats and vulnerabilities so that they can make informed information security decisions. The security analytics capabilities harness security data to generate security insights that allow security managers and business executives to make such security decisions. In addition, the research model considers ISRM as an integral part of key business processes. This perspective is important as it helps in continuous monitoring, analysis and reporting of security events thereby increasing the likelihood of threat detection and enabling descriptive, predictive and prescriptive components of BA. Finally, the overall result of security analytics capabilities development in organizations will be evidence-based decision making in ISRM at both the business process and whole enterprise levels.

The research model we propose provides a sound basis for further empirical research into understanding how ISRM process can be enhanced using security analytics and contribute to a competitive advantage. We suggest a number of areas for future research.

First, we have identified a number of dimensions to conceptualise each of the constructs in the research model. Identification of the specific enablers and mechanisms for interaction of security analytics and ISRM capabilities that can contribute to a competitive advantage in ISRM is an important research direction to follow. This can be done by conducting interviews and focus groups with security and BA experts.

Second, we have proposed a research model which explains that security analytics and ISRM capabilities are indirectly related with competitive advantage in ISRM via ISRM dynamic capabilities and analytics-enabled ISRM capabilities. We used environmental turbulence as a moderating factor through which security analytics and ISRM capabilities influence the competitive advantage in ISRM. Therefore, it is important to examine (1) the properties that emerge from the interaction of security analytics and ISRM capabilities over time and (2) the conditions that require renewal and reconfiguration of analytics-enabled ISRM capabilities in order to respond to rapidly changing environments. This can be done by conducting a case study with specific organisational context.

Third, we have developed a research model and five hypotheses that need to be empirically tested. An important aspect of this empirical research will be testing whether the interaction of security analytics and ISRM capabilities contributes to a competitive advantage indirectly via ISRM dynamic capabilities and analytics-enabled ISRM capabilities. This can be done by developing detailed measures for constructs and then testing the hypotheses in the research model by conducting a survey.

Finally, we argue that organisations need to move ISRM process from a mid-level technical function up to the board room and top management where strategic decisions are made. Furthermore, organisation need to practice evidence based decision making in ISRM and conduct risk assessments on a continuous basis. This is important because organisations need to transition from reactive (traditional) to proactive (holistic) ISRM approach. Future research can investigate the important role of executive engagement in defining the risk strategy and levels of acceptable risk on effective management of information security risks and threats.

6 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., 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.*

Alberts, C. J., and Dorofee, a J. 2002. *Managing Information Security Risks: The OCTAVE Approach*, Addison-Wesley Longman Publishing Co., Inc..

Anderson, E. E., and Choobineh, J. 2008. “Enterprise information security strategies,” *Computers & Security* (27:1–2), pp. 22–29.

Aral, S., and Weill, P. 2007. “IT Assets, Organizational Capabilities, and Firm Performance: How Resource Allocations and Organizational Differences Explain Performance Variation.,” *Organization Science* (18:5), pp. 763–780.

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

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), Elsevier B.V., pp. 138–151.

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.

Davenport, T.H., Harris, J.G. and Morison, R. 2010. *Analytics at work: Smarter decisions, better results Harvard Business Press*, Harvard Business Press.

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

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

Eisenhardt, K. M., and Martin, J. A. 2000. “Dynamic capabilities: what are they?,” *Strategic management journal* (21:10–11), pp. 1105–1121.

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.

Grant, R. M. 1996. “Prospering in dynamically-competitive environments: Organizational capability as knowledge integration.,” *Organization science* (7:4), pp. 375–387.

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.

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.

Jerman-Blažič, B. 2008. “An economic modelling approach to information security risk management,” *International Journal of Information Management* (28:5), pp. 413–422.

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.

Morgan, N. A., Vorhies, D. W., and Mason, C. H. 2009. “Market orientation, marketing capabilities, and firm performance,” *Strategic Management Journal* (30:8), pp. 909–920.

Naseer, H., Maynard, S., and Ahmad, A. 2016. “Business Analytics in Information Security Risk Management : The Contingent Effect on Security Performance,” in *ECIS 2016 Research in Progress Papers*, p. Paper 13.

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.

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.

Parker, D. B. 2007. "Risks of risk-based security," *Communications of the ACM* (50:3), p. 120.

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.

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.

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.

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.

Shanks, G., and Bekmamedova, N. 2013. "Creating Value With Business Analytics In The Supply Chain," *European Conference on Information Systems 2013 Completed Research Paper*, 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*, p. 51.

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.

Someh, I. A., and Shanks, G. 2013. "The Role of Synergy in Achieving Value from Business Analytics Systems," *ICIS 2013 Proceedings*, pp. 1–16.

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

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

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

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 Research1," *MIS Quarterly* (28:1), pp. 107–142.

Watson, R. T. 2015. "Beyond being systematic in literature reviews in IS," *Journal of Information Technology* (30:2), Nature Publishing Group, 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," *Source: MIS Quarterly* (26:2).

Wheeler, B. C. 2002. "NEBIC: A dynamic capabilities theory for assessing net-enablement," *Information Systems Research* (13:2), pp. 125–146.

Whitman, M. E., and Mattord, H. J. 2013. *Management of information security*, Nelson Education.