Spring 6-10-2017

TOWARDS AN ANALYTICS-DRIVEN INFORMATION SECURITY RISK MANAGEMENT: A CONTINGENT RESOURCE BASED PERSPECTIVE

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

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

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

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

TOWARDS AN ANALYTICS-DRIVEN INFORMATION SECURITY RISK MANAGEMENT: A CONTINGENT RESOURCE BASED PERSPECTIVE

Research in Progress

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

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

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

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

Abstract

Information security risk management (ISRM) is a continuous process that integrates identification and analysis of risks to which an organisation is exposed, assessment of likelihood of potential threats and their impact on the business, and deciding what actions need to be taken to eliminate or reduce risk to an acceptable level. Our review of the literature highlights two trends in organizational practice of ISRM: (1) security risks are not analysed and monitored continuously and historically (2) security risks are assessed based on speculation rather than evidence. Business analytics (BA) provides organizations with a unique opportunity to develop specialised capabilities (security analytics) and thereby enable the practice of analytics-driven evidence-based decision making in ISRM. In this study, we utilize a contingent resource based view to develop a research model that explains how security analytics capabilities and ISRM capabilities indirectly influence enterprise security performance through mediating role of analytics-driven ISRM capabilities. Risk assessment complexity moderates the process by which security analytics capabilities and ISRM capabilities influence the enterprise security performance. The model is defined based on an extensive analysis of BA and ISRM literature. The model provides a foundation for future empirical work including multiple case studies and a survey.

Keywords: Security Analytics, Risk Management, Enterprise Security Performance, Information Security

1 Introduction

A critical objective of the information security risk management (ISRM) process is to provide security managers with crucial insights so as to ensure that the right information assets are identified for protection and appropriate controls are implemented to reduce the likelihood of a security breach and its subsequent impact (Spears and Barki 2010). This process is important as it helps security managers in their decision making related to enterprise-wide information security. Our review of the literature highlights two trends in the organizational practice of ISRM: (1) security risks are not analysed and monitored continuously and historically (Ahmad et al. 2012; Baskerville et al. 2014) and (2) security risks are assessed on the basis of speculation rather than evidence (Shameli-sendi et al. 2016; Webb et

al. 2014). This implies that security managers are not incorporating important security data into their ISRM decision making process, do not have complete security awareness, and therefore require holistic security insights to make informed enterprise security related decisions.

Organizations use business analytics (BA) capability for analysing data and generating insights for business managers to help them make more informed business decisions (Holsapple et al. 2014). The capability to store data quickly is not new. What is new is the capability to do something meaningful with that data, quickly and cost effectively (Davenport et al. 2010; Shollo and Galliers 2016) and that is why the interest in the research of business analytics use has been increasing (Chen et al. 2012). 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 (Seddon et al. 2016; Sharma et al. 2014). This study develops a process-level construct of BA following Oliveira et al. (2012) and Bronzo et al. (2013) 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 concept of security analytics capability as a specialised BA capability for enterprise security process. In addition, we conceptualise security analytics capability in the context of using BA in the process of 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 et al. 2014). Security analytics capabilities assist in this transition with a potential to contribute to superior security process performance as it does in other business processes such as supply chain management (using supply chain analytics capabilities), marketing (using marketing analytics capabilities) and customer relationship management (using customer analytics capabilities) (Chen et al. 2012; Germann et al. 2013; Holsapple et al. 2014; Trkman et al. 2010).

Another argument in the BA literature is whether BA-related capabilities influence competitive advantage directly or indirectly (Işik et al. 2013; 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., Kevin et al. 2014; Trkman et al. 2010). Extending this indirect view, we utilize the contingent resource based view (RBV) to propose a model that explains how security analytics capabilities and ISRM capabilities indirectly influence enterprise security performance through mediating role of analytics-driven ISRM capabilities.

Although most of the RBV literature investigates the critical role of capabilities in achieving competitive advantage and/or creating value, ISRM is primarily a value/competitive advantage protection activity (Stoll 2015). For that reason, we propose analytics-driven ISRM as a specific capability that allows organizations to better identify, analyse and manage risks to which the organisation is exposed and thereby sustain their competitive advantage.

Recent theorizing within organizational capability development and orchestration also argues that there are contingencies that impact the outcomes or effectiveness of capabilities interaction/integration processes (Sirmon et al. 2011). Environmental factors for instance dynamism may change the effect of capabilities on competitive outcomes (Sirmon and Hitt 2009). Our research is consistent with this logic and explores the contingent effects of risk assessment complexity on the outcomes of analytics-driven ISRM. Since the ISRM process is increasingly complex (Baskerville et al. 2014), we argue that analytics-driven ISRM will contribute to superior enterprise security performance when risk assessment is complex.

The paper proceeds as follows: Section 2 describes our theoretical perspective (contingent RBV). 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 capabilities and ISRM capabilities indirectly influence competitive advantage in ISRM through mediating role of

analytics-driven ISRM capabilities that in turn influence enterprise security performance. Finally, section 5 concludes the paper with directions for future research.

2 Theoretical Framing – Contingent Resource Based View

The RBV argues that organizations can generate competitive advantage by developing bundles of resources (Barney 1991; Newbert 2007). These resources may be tangible or intangible, and consist of assets and capabilities. Assets include applications, infrastructure, data and people, while capabilities include organisational processes, routines, skills and knowledge of the people that utilise assets to perform a task. While many assets are readily available and some are commodities, an organisation's superior performance can be mainly attributed to the unique, valuable, rare, inimitable and non-substitutable capabilities that enable the organisation to perform activities more efficiently and effectively than its competitors (Wade and Hulland 2004).

Although the RBV is prevalent within the extant literature, it has been suggested that the theory has context insensitivity (Kevin et al. 2014). This implies that RBV is not able to identify the conditions in which capabilities can be most valuable. The idea of contingent conditions is addressed in contingency theory which suggests that external and internal conditions will influence how an organization is managed (Kevin et al. 2014) and can affect the capabilities required to drive the performance under dynamic conditions. Furthermore, contingency theory argues that organizations must adapt depending on the environmental conditions in which they exist. Scholars have proposed the contingent RBV as it addresses the rather static nature of the RBV (Aragon-Correa and Sharma 2003).

The development of contingent RBV 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). Sirmon and Hitt (2009) argue that contingencies are crucial in the realization of competitive advantage generated by capabilities, specifically in relation to their selection and deployment. Contingency research is highlighted as necessary for the development of secure information systems (Dhillon and Backhouse 2001); however until now, contingent perspective on the RBV is underdeveloped in information security and risk management literature.

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', 'big data analytics', 'security analytics' 'risk assessment' and 'information security risk management'. These searches identified over 90 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 enterprise security performance be improved using business analytics in information security risk management?). This resulted in 60 articles for in-depth review and coding. To extend the search outside the original set of journals, 10 additional papers of potential interest were also identified from reference list of reviewed articles. We used contingent 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 Security Analytics – A Specialised Business Analytics Capability

Organisations use the practice of BA to develop reporting and analysis applications that enable them to analyse important business data in order to generate new insights about business and markets (Chen et al. 2012). The new insights can be used to take informed actions and thus make practice of 'evidence-based decision making' possible in business (Davenport et al. 2010). The overall value of BA practice in any organization can be explained as a simple workflow, turning data into insights and then into actions (preferably profitable actions) (Eckerson 2012). The reporting and analytical solutions that organizations develop to help them in generating new insights include data warehouses, data marts, OLAP, dashboards, scorecards, visualization, and data mining (Popovič et al. 2012).

Many case studies and success stories in both research and practitioners literature provide the evidence that BA capabilities provide significant benefits to organizations and contribute to firm performance (Holsapple et al. 2014; Seddon et al. 2016; Sharma et al. 2014). 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 that are recently catching 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 (Naseer, Maynard, et al. 2016; Talabis et al. 2014). BA provides organizations with a unique opportunity to develop specialised security analytics capabilities and thereby enable the practice of analytics-driven evidence-based decision making in ISRM.

The concept of security analytics has recently been highlighted in the BA and information security management literature, and there is no clear definition of what exactly security analytics entails (Chen et al. 2012; Holsapple et al. 2014; Pierazzi et al. 2016). We propose security analytics as a capability that organizations can develop and define it as the ability to effectively collect and analyse security data, and generate security related insights to drive fact-based management, planning, decisions, execution, learning and measurement of enterprise security events (Holsapple et al. 2014; Pierazzi et al. 2016). 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 executives (security insights dissemination), and (3) the decision-making of security executives is subsequently based on the security insights gleaned from the enterprise 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 enterprise security performance is a contribution to the literature.

3.2 Information Security Risk Management Capabilities

Information security risk management is a continuous process that helps organisations to identify, integrate and analyse the risks to which the organisation is exposed, assess the likelihood and impact of potential threats on the business, and decide what actions should be taken to reduce or eliminate risk to an acceptable level (Bojanc and Jerman-Blažič 2013; Spears and Barki 2010). Organizations use the information security risk assessment process, a subset of the ISRM process to (1) gather data for security risk assessment (2) identify assets and their value for the business, (3) identify threats that might impact the assets, (4) identify security vulnerabilities in the assets that might be exploited, and (5) identify specific risks 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 (Bojanc and Jerman-Blažič 2008). Therefore, we define ISRM capabilities as the ability to effectively leverage (people, process, and technology) that helps in identifying, analysing, controlling, monitoring and protecting organisational information assets. The

concept of ISRM capabilities in this research is adopted from (Stoll 2015). Risk assessment capability and security control monitoring capability are the two key dimensions of ISRM capabilities (Bojanc and Jerman-Blažič 2008).

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 (Bojanc and Jerman-Blažič 2008). Finally, complexity also increases when there are different types of data that provide information about information assets (Pierazzi et al. 2016; Talabis et al. 2014).

There is considerable evidence in the literature that suggests two trends in ISRM organisational practice (1) security risks are not assessed and monitored continuously and historically (Ahmad et al. 2012; Baskerville et al. 2014; Naseer, Shanks, et al. 2016; Webb et al. 2014) and (2) security risks are assessed on the basis of speculation rather than evidence (Rees and Allen 2008; Shameli-sendi et al. 2016; Webb et al. 2014). This implies that security managers are not incorporating important security data into their ISRM decision making process, do not have complete security awareness, and thus require holistic insights to practice evidence-based decision making in ISRM. Therefore, we propose that the interaction between security analytics capabilities and ISRM capabilities can enable organisations to develop analytics-driven ISRM capabilities that can help them to conduct risk assessments continuously and historically and thereby practice evidence-based decision making in ISRM.

3.3 Analytics-Driven Information Security Risk Management Capabilities

Analytics-driven decision making approach deals with the discovery and communication of meaningful patterns in the data and combines both quantitative and qualitative data analysis techniques (Davenport et al. 2010). The key benefit of analytics-driven decision making approach in ISRM is the capability to turn large volumes of security data into smaller amount of information and insights that security managers can use and analyse to make informed ISRM related decision.

Therefore, we define analytics-driven ISRM capabilities as the ability to effectively leverage security insights gleaned from applied analytics disciplines (for example, statistical, contextual quantitative, predictive, cognitive and other models) to make informed ISRM decisions (Kiron et al. 2012). This is based on the RBV which suggests that security analytics capabilities and ISRM capabilities interact with each other to generate organizational benefits by developing higher-order analytics-driven ISRM capabilities with emergent properties (Wade and Hulland 2004). These higher-order analytics-driven ISRM capabilities, in turn, contribute to superior enterprise security performance. 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-driven risk assessment capability and analytics-driven security control monitoring capability are the two key dimensions of analytics-driven ISRM capabilities.

3.4 Enterprise Security Performance

Enterprise security relates to all the risks that can affect the core business of an organization, and includes failed software processes, human error and both internal and external security threats (David

and Noble 2016). We are examining the relationship between the interaction of security analytics capabilities and ISRM capabilities, and its impact on enterprise security performance through mediating role of analytics-driven ISRM capabilities. Enterprise security performance is the overall effectiveness and efficiency of all the security processes in an organization. Both ISRM process effectiveness and efficiency have been individually linked to enhance the overall enterprise security performance (by either reducing the cost of prevention, mitigation, and remediation or by reducing the cost of losses) (Harrer and Wald 2016).

4 The Research Model

In the research model (see Figure 1 for research model) we propose that security analytics capabilities and ISRM capabilities indirectly influence enterprise security performance through mediating role of analytics-driven ISRM capabilities. Risk assessment complexity moderates the process by which security analytics and ISRM capabilities influence the enterprise security performance.

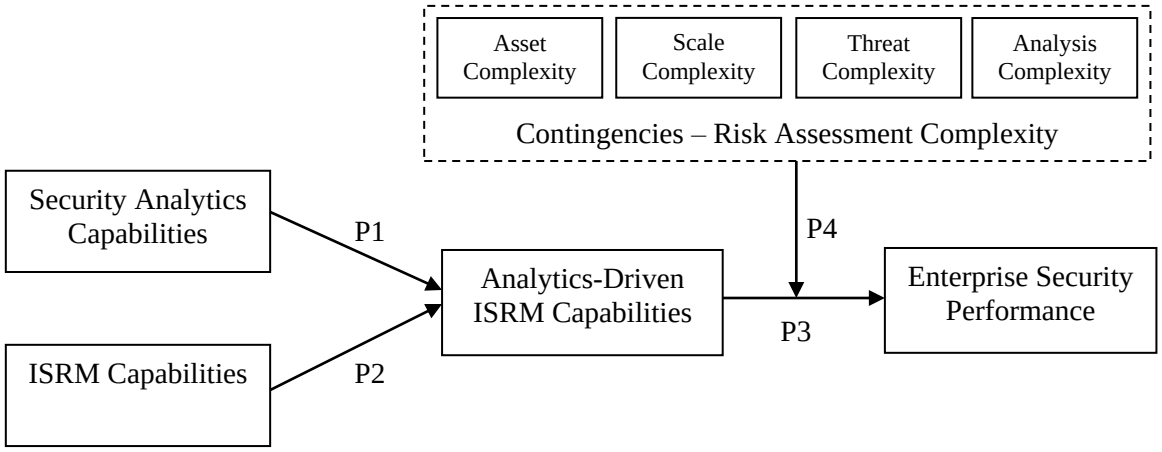

Figure 1. Enterprise Security performance impacts from analytics-driven ISRM capabilities

4.1 The Impact of Security Analytics Capabilities and ISRM Capabilities on Analytics-Driven ISRM Capabilities

Security analytics capabilities is the ability to effectively collect and analyse security data, and generate security related insights to drive fact-based management, planning, decisions, execution, learning and measurement of enterprise security events. The concept of security analytics capabilities in this study is adopted from (Holsapple et al. 2014; Pierazzi et al. 2016). There are four major processes within security analytics capabilities that help in turning security data into insights and then into actions (Davenport et al. 2010): (1) Extracting, transforming and loading security data from disparate sources into an analytical ecosystem (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. We argue that the development of security analytics capabilities develops an evidence-based decision making culture in enterprise security management and helps security managers become proactive and make timely, data-driven decisions related to enterprise security. Therefore, we propose that:

P1: Security analytics capabilities have a positive impact on analytics-driven ISRM capabilities.

ISRM capabilities is the ability to effectively leverage (people, process, and technology) that helps in identifying, analysing, controlling, monitoring and protecting organisational information assets(Stoll 2015). ISRM capabilities empower 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 (Stoll 2015). Information security risk assessment and security controls monitoring are two key processes within ISRM capabilities that helps to identify prioritize and monitor risks specific to corporate information and assets along with assessing the impact and probability of threats accordance (Shameli-sendi et al. 2016; Shedden et al. 2011). We argue that the development of ISRM capabilities ensures that an enterprise has the capability required to protect its business processes, informational assets, and accomplish its mission and business objectives. We therefore propose that:

P2: ISRM capabilities have a positive impact on analytics-driven ISRM capabilities.

4.2 The Impact of Analytics-Driven ISRM Capabilities on Enterprise Security Performance

Security analytics capabilities and ISRM capabilities are complementary to each other in ways that generate higher-order analytics-driven ISRM capabilities. We define *Analytics-driven ISRM capabilities* as the ability to effectively leverage security insights gleaned from applied analytics disciplines (for example, statistical, contextual quantitative, predictive, cognitive and other models) to make informed ISRM decisions. This interaction between security analytics capabilities 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 superior firm performance (Teece 2007). We argue that higher-order analytics-driven ISRM capabilities will contribute to superior enterprise security performance. Therefore, we propose that:

P3: Analytics-driven ISRM capabilities have a positive impact on enterprise security performance.

4.3 The Moderating Role of Risk Assessment Complexity

Kraaijenbrink et al. (2010, p.365) argue in their review and assessment of RBV that "the moment we try to explain or predict the firm's actual performance . . . the RBV turns out to be incomplete because it ignores the material contingencies of the firm's situation". Our research responds to this challenge by examining the contingent effect of risk assessment complexity on the relationships between analytics-driven ISRM and enterprise security performance (see Figure 1). *Risk assessment complexity* relates to the number of assets (scale complexity), different types of assets (asset complexity), types of threats and vulnerabilities (threat complexity), and multiple types of data regarding the assets (analysis complexity). Complexity increases when organizations need to protect a large number of assets. Different types of assets and the different media where these assets reside result in an increased risk assessment complexity (Ahmad et al. 2005). Furthermore, distribution of 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 assets (Pierazzi et al. 2016).

We argue that each dimension of risk assessment complexity creates greater uncertainty and thus an additional opportunity for analytics-driven ISRM to benefit business managers. Organizations with a smaller number of information assets and lower risk exposure have less uncertainty and thereby low risk assessment complexity. However, organizations with a larger number of business assets and higher risk exposure have greater uncertainty. Analytics-driven ISRM will make greater contribution in such organizations by providing comprehensive insights about assets to identify, measure, and monitor risks to make informed enterprise security related decisions. Therefore, we propose that:

P4: Risk assessment complexity positively moderates the relationship between analytics-driven ISRM and enterprise security performance: the higher the complexity, the greater the beneficial effects of analytics-driven ISRM capabilities on enterprise security performance.

5 Conclusion and Future Work

In this research-in-progress paper we utilised the contingent RBV to show how security analytics capabilities and ISRM capabilities indirectly influence enterprise security performance through mediating role of analytics-driven ISRM capabilities and how this effect is dependent on the risk assessment complexity. Furthermore, we proposed security analytics as a specialised BA capability for analysing security data and generating specific insights for security managers to help them make analytics-driven enterprise security related decisions. In particular, our research has contributed to the literature in BA and information security management by providing detailed definitions of concepts and propositions in the model, grounded in the contingent RBV.

This study offers several useful implications for security managers. First, the development of security analytics capabilities enable organisations to harness security data to generate security insights that can help security managers to assess and monitor security risks both continuously and historically. Second, the research model considers ISRM as an integral part of enterprise security processes. This perspective is important as it helps in continuous monitoring, analysis and reporting of security risks and events thereby increasing the likelihood of threat detection and enabling descriptive, predictive and prescriptive components of BA (Holsapple et al. 2014). Finally, the overall result of security analytics practice in organizations will be evidence-based decision making in ISRM at both the business process and at whole enterprise levels.

We are conducting a mixed-method research approach consisting of two phases (multiple case studies and a survey) to further refine and evaluate the research model (Venkatesh et al. 2013). The purpose of conducting mixed-method research in this study is 'developmental' (Venkatesh et al. 2013) and a qualitative and quantitative sequence strategy is employed. Inferences drawn from the first study (qualitative research) will inform the second study (quantitative research).

In the first phase, we will conduct multiple case studies to further improve the concepts and mechanisms underlying the propositions in the model. A case study with specific organizational context will add depth in the research by providing rich insight on (1) the factors that enable the interaction between security analytics and ISRM capabilities, (2) the conditions which affect the utility of analytics-driven ISRM capability, (3) the new properties that emerge from the interaction of security analytics and ISRM resources over time, and (4) the dimensions that can comprehensively represent the constructs in the model. The objective is to develop specific hypotheses in relation to dimensions, interaction factors and properties that emerge with the development of higher-order analytics-driven ISRM capability.

In the second phase, we will develop detailed measures for constructs and test the hypotheses in research model by conducting a survey. The objective of the survey is to measure the impact of using BA on ISRM process and enterprise security performance in a large sample of organizations. Furthermore, a survey will also add breadth in the study and help in generalizing the findings of this research.

References

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

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.*

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.

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

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.

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.

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.

David, W., and Noble, T. 2016. "Planning for the Known, Unkown and Impossible-Responsible Risk Managment to Maximize Organizational Performance," *Journal of Business Behavioral Sciences*, (28:1), pp. 40–48.

Dhillon, G., and Backhouse, J. 2001. "Current directions in IS security research : towards socio-organizational perspectives," *Information Systems Journal*, (11:1), pp. 127–153.

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

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.

Harrer, J., and Wald, A. 2016. "Levers of enterprise security control : a study on the use, measurement and value contribution," *Journal of Management Control*, (27), pp. 7–32.

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.

Işik, Ö., Jones, M. C., and Sidorova, A. 2013. "Business intelligence success: The roles of BI capabilities and decision environments," *Information and Management*, (50:1), pp. 13–23.

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.

Kiron, D., Shockley, R., Kruschwitz, N., Finch, G., Haydock, M., Kiron, B. D., Shockley, R., Kruschwitz, N., Finch, G., and Haydock, M. 2012. "Analytics: The Widening Divide," *MIT Sloan Management Review*, (53:2), pp. 1–23.

Kraaijenbrink, J., Spender, J., Groen, A., Spender, J., and Groen, A. J. 2010. "The resource-based view: A review and assessment of its critiques," *Journal of Management*, (36:1), pp. 349–372.

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.

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*.

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.

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.

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.

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.

Seddon, P. B., Constantinidis, D., Tamm, T., and Dod, H. 2016. "How does business analytics contribute to business value?," *Information Systems Journal*.

Shameli-sendi, A., Aghababaei-barzegar, R., and Cheriet, M. 2016. "Taxonomy of information security risk assessment (ISRA)," *Computers and Security*, (57), pp. 14–30.

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., 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.

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.

Sirmon, D. G., and Hitt, M. A. 2009. "Contingencies within dynamic managerial capabilities: interdependent effects of resource investment and deployment on firm performance," *Strategic Management Journal*, (30), pp. 1375–1394.

Sirmon, D. G., Hitt, M. A., Ireland, R. D., and Gilbert, B. A. 2011. "Resource Orchestration to Create Competitive Advantage: Breadth, Depth, and Life Cycle Effects," *Journal of Management*, (37:5), pp. 1390–1412.

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*, (313), pp. 9–16.

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

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.

Venkatesh, V., Brown, S. A., and Bala, H. 2013. "Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems," *MIS Quaterly*, (37:3), pp. 855–879.

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," *MIS Quarterly*, (26:2), pp. xiii–xxi.