Exploring the Impact of Information Security Practices on Competitive Advantage

Emergent Research Forum (ERF)

Dejan Kosutic
Grenoble Ecole de Management
dejan.kosutic@grenoble-em.com

Federico Pigni
Grenoble Ecole de Management
federico.pigni@grenoble-em.com

Abstract

While previous research has explained the effectiveness of information security investment and has put an emphasis on the need for a holistic approach to information security management, the existing contributions fail to advance such integrative view. Further, the relationship between information security and competitive advantage is rarely explored and remains largely unresearched.

With this research we aim at developing an integrative model for holistic information security management, and exploring the relationship between information security and the success of organizations. We argue there are two main reasons for this low effectiveness of information security: the first is the overemphasized focus on security technology, and the second is that information security is not perceived as contributing to firm’s success. We argue that managing information security in a holistic way can contribute to the competitiveness of a company, and propose the SORP Cybersecurity Model to address both problems.

Keywords

Information security, cybersecurity, information security management, competitive advantage.

Introduction

More than half of IT security professionals expect a security breach in the next 12 months (Cyber Security Incident Response: Are we as prepared as we think? 2014), while both the number of security threats and the size of incidents are on the rise (2017 Cost of Data Breach Study: Global Overview, 2017). Additionally, the advent of cloud and mobile computing compels companies to change their security approach (International trends in cybersecurity, 2016, Cybersecurity Challenges, Risks, Trends, and Impacts, 2016).

Despite the strategic importance of security to current business, and the existence of industry standards like ISO 27001 (“ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems,” 2013) that advance a holistic approach to information security management, the investment in information security has been often disappointing – security incidents are almost never eliminated, and the costs of the implementation are usually much higher than initially planned.

While previous research has explained the effectiveness of information security investment, with an emphasis on the need for a holistic approach to information security management, the existing contributions fail to advance an integrative view. Further, the relationship between information security and competitive advantage is rarely explored and remains largely unresearched. Therefore, with this research we aim to develop an integrative model for information security management, while exploring the relationship between information security and the success of organizations.

We argue that there are two main reasons for this lack of effectiveness of information security. The first reason is the overemphasized focus on security technology while neglecting other crucial elements of information security management (Singh et al. 2013)—therefore, we argue that a model is needed that would clearly show the necessity of a more holistic (organizational) approach. The second reason is that information security is not perceived as contributing to a firm’s success, leading top management to minimize its importance. We argue that managing information security in a holistic way can indeed contribute to the competitiveness of a company. We then propose the SORP Cybersecurity Model to address both mentioned problems.
Literature Review

Academic literature on information security is vast, but only a few articles explore the relationship between information security and company success or failure.

For example, for an investment in information security to provide optimal results, it must depend on the vulnerability of the information and the potential loss if such information is compromised—information security is not economically justifiable for very high or very low levels of vulnerabilities (Gordon and Loeb 2002); in other words, only the investment in mitigating mid-range vulnerabilities makes sense.

In financial terms, information security can significantly impact a company’s stock price in two ways. The first is the drop in share price that typically comes as a consequence of a disclosed security breach—this effect will differ depending on the industry, the type of security breach, and the time frame of analysis (Yayla and Hu 2011). Secondly, voluntary public disclosure of information security items (e.g., in annual reports) positively affects the stock price, especially if the company operates in an industry that depends heavily on e-commerce activities, and if the disclosure is related to proactive security measures (Gordon et al. 2010).

The above-mentioned studies provide evidence of a connection between information security activities and benefits for a company; however, they fail to explain how a company can create a sustainable competitive advantage in the marketplace. They also neglect to investigate which types of information security activities are needed to achieve an effective level of security.

Only a few papers hint at how information security contributes to competitive advantage. For example, due to organizational learning, proactive security investment is observed to cause lower failure rates and lower incident costs than investments made as a reaction to a security breach (Kwon and Johnson 2014). However, the relationship between information security and company success accounted only for the technological aspect of security, as Kwon and Johnson (2014) “counted the number of security applications that have been adopted,” and they acknowledge that the influence of human factors, training, and policies were not considered. Nevertheless, this information security activity can be interpreted as supportive of competitive advantage for those companies that compete based on low cost (Porter and Millar 1985).

Further, when knowledge sharing and protection activities are combined, innovation is positively affected, as the company has more incentive to innovate knowing that competitors won’t be able to copy the outputs as easily (Gomes et al. 2017). Therefore, those companies whose competitive advantage relies heavily on innovation can use information security as one of the building blocks of innovation capability.

Other benefits emerging from the deployment of an effective information security strategy include “confidentiality, integrity, and availability of information, and protection of competitive advantage, reputation, and customer trust” (Horne et al. 2017).

A number of papers clarify which elements are needed for effective information security management (Hong et al. 2003; Posthumus and von Solms 2004; Whitman 2004; Rao 2009; Sveen et al. 2009; Van Niekerk and Von Solms 2010; Ahmad et al. 2014; Taylor and Robinson 2014). However, as Horne et al. (2017) conclude, there is no model that would unify and conceptualize all these elements, and “a paradigm shift is required to move from internally-focused protection of organisation-wide information towards a strategic view that considers an organisation’s environment,” while Soomro et al. (2016) state that a more holistic approach to information security management is needed.

In conclusion, information security appears to contribute to a firm’s competitive advantage; however, little is known about how this is achieved, and no integrative concept is advanced to support the investigation.

Advancing the SORP Cybersecurity Model

To address the gap in the existing literature, we developed the preliminary SORP Cybersecurity Model that addresses both the issue of holistic information security management (Horne et al. 2017; Soomro et al. 2016), as well as the relationship between information security and competitive advantage. This model is the result of a systematic review of the literature on information security, the analysis of a first wave of interviews with three cybersecurity experts, and the professional experience of one of the authors.

Figure 1 depicts the SORP Cybersecurity Model. The model emphasizes the importance of balancing four main aspects of effective information security management (Strategic, Organizational, Risk, and People),
thereby addressing the need for holistic information security management (Soomro et al. 2016 and Horne et al. 2017). This model also shows how information security influences competitive advantage of companies through protecting the existing competitive advantage, enhancing product development, and enabling lower cost (Campbell et al. 2003, Kwon and Johnson 2014, Horne et al. 2017, Gomes et al. 2017).

Contribution of this model for security professionals is that they will more easily understand what are the necessary elements of information security management, what are the main inputs, and what are the factors that can influence the success of their activities. Top management can use this model to understand how to position information security within a company, and how to use it to achieve competitive advantage.

Antecedents and Moderating Factors

A company needs to consider various inputs to manage its information security successfully, which includes finding ways to mitigate the disabling factors while taking advantage of the enabling factors that will contribute to effective information security.

The antecedents that a company needs to consider when managing its information security include threats that could compromise its information, its business strategy, stakeholders and their requirements, laws and regulations related to information security and privacy and, finally, market opportunities (McFadzean et al., 2007, Acuna, 2016, Soomro et al., 2016, Horne et al., 2017).

Moderating factors include the perception about information security consisting of lack of understanding from top management, employee resistance and awareness of information security risks; as well as a lack of resources, availability of industry standards, and shared information about information security threats (Soomro et al., 2016, Horne et al., 2017).

Information Security Management

There are four key aspects of information security management to consider. Briefly, the strategic aspect of information security makes the connection between business objectives and information security. The organizational aspect must provide a structure for information security activities to become effective. The risk management aspect must provide a decision-making process regarding which safeguards are needed, while the people aspect must overcome barriers and provide necessary competences for implementation.

The strategic aspect of information security needs to consider potential business benefits, align the security strategy with the business strategy (Ahmad et al. 2014), make sure that operational security will fit with the security strategy, include setting up security objectives and their measurement, and develop a top-level security policy that documents the whole strategic element (Hong et al. 2003).
The organizational aspect must define where to position the information security function within the company, provide clear definition of roles and responsibilities, set up security processes and align them with other operational processes, and include project management techniques when starting with the initial implementation of information security (Hong et al. 2003).

The risk management aspect must include two main components: risk assessment, where the risks are identified and evaluated, and risk treatment, where the mitigation for unacceptable risks is determined (“ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements,” 2013). Controls that are selected during the risk management activities include technical controls (e.g., anti-malware, backup, secure software development, etc.), in addition to non-technical (e.g., managing suppliers, classification of data, etc.) (Hong et al. 2003; Whitman 2004; Posthumus and von Solms 2004; Sveen et al. 2009).

The people element needs to include security training and awareness, as well as communication of all important information—all of this should enable building up a security culture within the company (Taylor and Robinson 2014; Van Niekerk and Von Solms 2010; Whitman 2004).

**Competitive Advantage**

If implemented properly, holistic information security can support a sustainable competitive advantage of a company in the following ways:

2. Product development—by enabling greater innovation, setting barriers for competitors, and creating additional or new revenue streams (Ezingeard et al. 2007; Gomes et al. 2017).
3. Lowering costs—by decreasing the frequency and impact of information security incidents (Kwon and Johnson 2014).

**The Methodology for the Research**

To validate the Model, we adopt a mixed-method research design—in particular, multi-wave survey, complemented by a qualitative exploratory phase and a confirmatory quantitative phase (Miles, et al., 2014; Walsh, 2014). In the exploratory phase of the research we intend to build a model, using qualitative methods to analyze semi-structured interviews with at least 20 business executives and security professionals in various positions, companies, and industries. The main challenge in this phase will be to find enough executives and professionals from different industries to have a representative sample (Miles, et al., 2014).

In the confirmative phase of the research we will perform quantitative analysis by administering the questionnaires to a selected set of IT and security professionals (around 50,000 contacts), with the purpose to prove the impact of holistic information security on competitive advantage. The main challenge here will be to develop a comprehensive and context-specific survey instrument (Hoehle & Venkatesh, 2015).

**Next Steps**

Besides the need to validate the SORP Cybersecurity Model and its influence on competitive advantage, it remains to be seen if the three elements of competitive advantage from the Model can be related with resourced-based view, with Porter’s generic competitive strategies (Porter and Millar 1985), or with some other model of competitive advantage. Further research would be needed to develop a model that will explain to which industries information security is more applicable, and for which information within the companies it would be more appropriate. Finally, the terminology dilemma of whether to use information security, IT security, cybersecurity, data security, or information assurance should be clarified.

**References**


