Top Manager’s Perspectives on Cyberinsurance Risk Management for Reducing Cybersecurity Risks

Extended Abstract

Obi Ogbanufe
University of North Texas
Denton, TX 76201, USA
obi.ogbanufe@unt.edu

Dan J. Kim
University of North Texas
Denton, TX 76201, USA
dan.kim@unt.edu

Keywords: Cyberinsurance, risk management, data breach, security risk

Data breaches are adversely affecting organizations’ reputation and market value (Cavusoglu et al. 2004; Mukhopadhyay et al. 2013). According to a Forbes report, 46 percent of companies have suffered reputational damage due to a data breach (Forbes 2014). In addition, a recent survey of 2,000 consumers found that nearly 87 percent are unlikely to do business with organizations impacted by data breach (NCI 2016). Ponemon (2015) notes that the average cost of each stolen record is $217. The cost of data breaches include notification of individuals impacted by the breach, legal fees, regulatory fines, and the cost of recovery. These costs can be damaging and difficult to recover from, especially for small and medium sized organizations. This is perhaps why it is argued that 60 percent of small businesses close their businesses within half a year of being impacted by cybercrime (Aguilar 2015). These costs are also one of the reasons organizations are driven to protect their businesses from the impact of data breaches by using cyberinsurance. Cyberinsurance as a risk transfer approach is one of the many security risk management strategies used by organizations. Cyberinsurance is an insurance product used to protect organizations from risks derived from the use of the internet and information systems. Cyberinsurance is defined as the transfer of financial risk associated with security/data breaches to a third party (Böhme and Schwartz 2010).

There are at least two reasons why cyberinsurance should matter for information security. First, traditional approaches to security risk management through technology (Lee and Larsen 2009), policies (Vance et al. 2012) and procedures (Spears and Barki 2010) is limited in preventing or eliminating security risks. It is widely understood that identifying and protecting against cyberattacks by technical approaches alone do not provide an overall solution (Majuca et al. 2006; Siegel et al. 2002). Insurance risk management has since focused on reducing the impact and severity of damage through financial means (Siegel et al. 2002). Hence, Majuca et al. (2006) argue that an overall risk management strategy must include cyberinsurance. Second, insurance risk management minimizes the impact of financial losses from security and data breaches, allowing organizations to recover quickly from devastating losses and business interruption, thereby contributing to the economic stability of the business environment as a whole. In addition, practitioners and regulators (Bolot and Lelarge 2008; Department of Homeland Security 2012; Gordon et al. 2003) argue that cyberinsurance increases security management by encouraging the adoption of security best practices. The notion is that the requirements for receiving a policy encourages the implementation of best practice security measures.

Consequently, since we know relatively little about how top managers in organizations form estimates of the likelihood of adopting cyberinsurance, this study identifies the determinants and outlines a nomological network that top managers follow in their decision to use cyberinsurance.
as a security risk management strategy. Our focus is on the top managers’ assessment of the use of cyberinsurance to protect the organizations information assets. There are two reasons this research seeks the top managers perspective. First, organizations consists of individuals that may account for the performance of organizations. Strategic management literature notes that the omission of the individual factors in examining organizations has prevented a thorough understanding of the role individuals actually play in determining firm performance (Mollick 2012). Specifically, it has been shown that top managers are considered to be important in determining firm performance (Bertrand and Schoar 2003; Hambrick et al. 1996; Mollick 2012). The notion is that top managers have a strong influence on how their organizations respond to external and internal events that affect routines, resources and performance (Bertrand and Schoar 2003; Kettinger et al. 2013). In addition, Goodhue and Straub (1991) argue that an organizations security protective measures should require managerial careful attention. Second, there is a shifting of accountability in industry, such that top managers - and no longer technology departments - are under increased scrutiny for security breaches (Experian 2015). Top managers are nowadays required to understand and perform recommended actions that prevent and manage the threat of security breaches with cyberinsurance. Hence, this study is interested in understanding the top manager’s perspective for the use of cyberinsurance as a risk management strategy. We intend to answer the research question - what are the salient factors that determine the top manager’s intention to use cyberinsurance as a risk management strategy?

Drawing from the valence framework and institutional theory, we propose a research model consisting of organizational, institutional, environmental, individual, and security breach factors. Mayers and Smith (2005) note that assessing the corporate purchase of insurance through risk preferences alone is inadequate, and should include factors such as contracting and transaction costs, and regulation.

Using the valence framework of risk and benefits perspective we identify factors that are inherent in the top manager’s decision to purchase cyberinsurance. By dimensionalizing the risk and benefit factors along the lines of situational relevant factors and product relevant factors, we seek to extend the valence framework. Situation factors are factors specific to the risks and benefit driving the use of cyberinsurance as a risk management option. Whereas, the product factors are specific to the risk and benefits of the cyberinsurance product driving use. The result is a quadrant that incorporates a range of potential determining factors for top managers.

We intend to test the model through a survey of top managers in small and medium sized organizations. This study seeks to highlight the important role of cyberinsurance as an information security risk management approach. In addition, we intend to shed light on the use of cyberinsurance as a reinforcement for security best practice implementation. Contributions to research include, theoretically identifying and outlining the factors that determine the top manager’s intention to use cyberinsurance in a nomological network. For practice, in shedding light on the relationships between cyberinsurance use and secure behaviors, we hope it spurs small and medium business to consider cyberinsurance as a security risk management strategy.

REFERENCES


