Towards a Development of Cybersecurity Risk-Responsibility Taxonomy of Small Enterprises for Data Breach Mitigation

Emergent Research Forum (ERF)

Keiona Davis  
Nova Southeastern University  
keiona@mynsu.nova.edu

Yair Levy  
Nova Southeastern University  
levyy@nova.edu

Boštjan Delak  
University of Maribor  
bostjan.delak@fis.unm.si

Abstract

Research studies tend to focus their efforts on large organizations while overlooking smaller organizations. This work-in-progress study addresses the failure to prevent data breaches in small enterprises (SEs). SEs contribute significantly to the economy, however, are more prone to cyber attacks due to the limited risk mitigations on their systems and low cybersecurity skills of their employees. SEs utilize Point-of-Sale (POS) systems that are exposed to cyber threats, and can result in exposure to the risk of a data breach. The absence of federal laws forcing organizations to adhere to standards such as the payment card industry data security standard (PCI DSS) leaves it up to the discretion of the SEs to invest in cybersecurity countermeasures toward preventing a data breach. Therefore, this work-in-progress study investigates the role corporate cybersecurity social responsibility plays in motivating these companies to engage in cybersecurity measures toward preventing data breaches.

Keywords

Data breach risk mitigation, corporate cybersecurity social responsibility, cybersecurity of small businesses.

Introduction

Organizations are benefitting greatly from the advancement of information systems (IS) (Earl and Feeney 2012). However, such reliance on IS also increases the organizational exposure to data breaches (Gordon et al. 2014; Jang-Jaccard and Nepal 2014; Shim 2011). Moreover, the United States (U.S.) government defined organizational data breach as:

A data breach is a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in the unauthorized acquisition (via the Internet) of sensitive personally identifiable information; or access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization (Whitehouse.gov 2015, p. 1)

According to Shim (2011), there has been an explosion of malicious activities that endanger the soundness of organizations’ IS security. The Joint Task Force on Cybersecurity Education (2017) defined cybersecurity as “computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries” (p. 16). The need for IS security and in particular cybersecurity, is becoming far more widespread and of tremendous importance as data breaches become more prevalent (Van Niekerk and Von Solms 2010; Von Solms and Van Niekerk 2013). Small enterprises (SEs) are particularly at risk of data breaches due to the simplicity of their security measures (Harris and Patten...
2014). Straub and Welke (1998) defined an IS risk as “the likelihood that a firm’s information systems are insufficiently protected against certain kinds of damage or loss” (p. 441). A cybersecurity risk stems from the interaction of these systems with cyberspace (Von Solms and Van Niekerk 2013). One significant challenge faced by SEs is that of data breaches. Criminals target businesses to gain access to consumer data including credit card information by way of Point-of-Sale (POS) systems connected to the Internet. This information is then used to commit fraud or identity theft (Conner 2013; Pragati 2015; Strauss 2015).

In 2013, criminals stole credit card and debit payment information of over 70 million Target consumers through the payment card system (Zioboro 2014). Home Depot and Supervalu also reported similar breaches in 2014 (Banjo 2014; Sidel 2014). The theft of personal financial information results in the merchant, the consumer, or a financial institution facing negative or costly ramifications (Gordon and Loeb 2002; Son 2011). A data breach resulting in loss of consumer personal financial information can cause a merchant to experience damage to their reputation as well as an unforeseeable recovery time. However, very little is discussed in the popular media on the significant breaches going on in SEs (Kauffman et al. 2011). Requiring businesses to follow information security standards can help to facilitate cybersecurity responsibility and reduce data breaches (Coburn 2010). This study will develop a classification methodology that serves as a benchmarking tool to classify SEs based on their cybersecurity social responsibility as well as their risk of data breach. Cybersecurity social responsibility is derived from of the CSR theory, which implies that organizations are not only responsible to its direct stake holders, but also to the wider society (Carroll and Shabana 2010). Thus, the research problem that this study will address is the large financial damages resulting from failure to prevent data breaches, particularly in SEs (Bhattacharya 2011; Hovav and Gray 2014; Shim 2011). In the U.S. there is no standard definition of an SE. The U.S. Small Business Administration (SBA) offered different classifications to determine eligibility for SBA assistance and financing. According to the SBA (2014), an SE may have no more than 500 employees for most manufacturing industries and less than $7.5 million in annual returns for many non-manufacturing industries. However, clearly when it comes to traditional SEs, the focus is around 50 or less employees. This study will adopt the European Commission’s definition of a small enterprise as those enterprises that employ fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed 10 million Euros (~ $12.2 million) (European Commission 2016). Data breaches are not limited to large organizations, however, there is a gap in IS security research on cybersecurity in SEs (Groner and Brune 2012; Gupta and Hammond 2005). This may result from an evolution in cybercrime, where the perception is that cybercriminals primarily targeted larger organizations. Given that over the past few years these organizations heightened their cybersecurity measures cyber-attacks shifted to smaller companies (Bhattacharya 2011). SEs are especially exposed to data breaches because they tend to be less equipped to handle complex cybersecurity threats due to a smaller structure and limited IS expertise (Cragg et al. 2011; Harris and Patten 2014). In the event of a data breach, SEs can face exorbitant costs that put them at risk of going out of business. A cyber-attack in 2014 cost a small t-shirt manufacturer 80stees.com over $200,000 to resolve the issue, financial incident that can bankrupt many SEs (Berr 2014). The main goal of this work-in-progress research is to develop and validate a cybersecurity risk-responsibility taxonomy using SEs’ cybersecurity social responsibility and risk of data breach. The five specific research questions for this study are:

RQ1 What specific organizational characteristics will be identified by subject matter experts as being important for SEs in reducing the risk of data breach?

RQ2 What specific organizational characteristics will be identified by subject matter experts as being important for SEs to maintain high level of cybersecurity social responsibility?

RQ3 How will the aggregated scores of SEs’ cybersecurity social responsibility and risk of data breach be positioned on the cybersecurity social risk-responsibility taxonomy?

RQ4 Will significant differences exist in SEs’ cybersecurity social responsibility and risk of data breach based on three organizational demographics: (1) type of industry, (2) implementation of chip technology, (3) compliance with PCI DSS.
Literature Review

Cyber Threats

A cyber threat is frequently the result of Internet based activities and may affect those technologies connected directly or indirectly to computers and networks (Ilvonen and Virtanen 2013). Unlike a physical attack, which takes place in a single physical location, a cyber-attack extends beyond organizational and geographical boundaries thus its impact is more far reaching (Hovav and Gray 2014). A cyber threat can originate from multiple sources on different platforms and its impact is felt by individuals, government, and organizations alike and, as such, a cyber threat is considered to be a major crime and national security issue (Choo 2011b). Malicious software (malware), phishing and, insider abuse are among the most common forms of cyber threats (Choo 2011a). Over time the number of attacks continued to grow and became more complex, however, even though they are complex they were easier to launch resulting in multiple groups of attackers - some of whom are inexperienced but could still cause damage (Hansman and Hunt 2005).

Data Breach

A data breach happens as a result of personally identifiable confidential information such as names, social security numbers, and credit card information being acquired through unauthorized access via theft or accident (Romanosky, Telang, and Acquisti 2011). According to Sen and Borle (2015), in the US a single data breach can cost organizations as much as $5.9 million. The privacy rights clearing house has been reporting on data breaches affecting consumers in the US dating back to 2005. Since 2005 5,113 data breaches have been reported in the US. In the year 2015, there were 2,122 confirmed data breaches across 61 countries (Verizon 2015 Data Breach Investigations report). The frequency and magnitude of data breaches have continued to increase over the years. According to Symantec (2016), in 2015 there were nine mega breaches which included the largest breach ever to be publicly reported. In addition to disruption, a data breach incident can result in tangible or intangible costs to the breached organizations that can inhibit the firm's financial performance (Ko and Dorantes 2006).

Countermeasures

The ability to prevent or protect themselves from cyber-attacks and data breaches is one of the biggest issues organizations are faced with (Gupta and Hammond 2005; Jang-Jaccard and Nepal 2014). Countermeasures help to lessen the impact of such data breaches (Sawik 2013; Viduto, Maple, Huang, and López-Peréz 2012). Technical and operational countermeasures prevent physical access, as well as, those that block virtual access to networks and computers can be employed (Rees, Deane, Rakes, and Baker 2011). Technical countermeasures include those controls that are built into hardware, software, and firmware such as identification, authentication and intrusion detection software while operational countermeasures are those controls that are managerial or procedural such as security policies and operational procedures (Blank and Gallagher 2012). There are numerous standards aimed at specifying or recommending control measures, including British Standard 7799, NIST Special Publication 800–53, the Graham–Leach–Bliley Act of 1999, and the North American Electric Reliability Council's Urgent Action Standard 1200 (Rees et al. 2011). However, standards by themselves have not proven to be sufficient (Fenz, Ekelhart, and Neubauer 2011; Rees et al. 2011; Silva and Backhouse 2003).

Risk, Risk Management, and Risk of Data Breach

Risks in an organization can be in the form of natural disasters, security breaches, or financial failure. A risk may have one or more causes and, if it occurs, one or more impacts. The process of identifying risks and applying the appropriate countermeasures is known as Risk Management (Spears and Barki 2010). Information security risk management ensures that all possible threats and vulnerabilities, as well as the valuable assets, are taken into consideration (Fenz et al. 2011). This process is generally initiated by top management within organizations, however, managers are oftentimes unaware of how to deal with IS risks (Straub and Welke 1998). In addition, managers are oftentimes not committed to IS security (Hu, Dinev, Hart, and Cooke 2012; Puhakainen and Siponen 2010; Smith et al. 2010). Therefore, it is suggested that IS research focus on risk management guidelines to develop key principles aimed at aiding in the prevention
of IS security breaches and in turn help to manage information security (Dhillon and Backhouse 2001). Companies become exposed to data breaches either as they engage in ecommerce activities or, with internal POS transaction and IS running on computers connected to the Internet. A risk of a cybersecurity data breach stems from the interaction of these ISs with cyberspace (Von Solms and Van Niekerk 2013). Despite local state and federal laws regarding data breach notification and such, incidents of data breaches continue to happen in the United States. At the forefront of issues resulting from a cyber-attack is concerns for privacy which extend beyond an organization’s use of personal information to now include risk of data breaches (Culnan and Williams 2009). Other research studies looked at the impact of disclosure laws, however, according to (Culnan and Williams 2009), such studies do not contribute to the theoretical understanding of a risk of data breach.

**Corporate Social Responsibility**

Corporate social responsibility has been a topic of concern for several years. The work of Bowen (1953) ensued from the belief that the several hundred largest businesses were vital centers of power and decision-making and that the actions of these firms touched the lives of citizens at many points. “It refers to the obligations of businessmen to pursue those policies, to make those decisions, or to follow those lines of action which are desirable in terms of the objectives and values of our society” (p. 6). Numerous philosophies and definitions have been suggested over there years, mainly from different areas of study deriving different meanings (Geva 2008). CSR research has been challenging partly because it is difficult to develop valid measures. Rather than utilizing what was previously suggested, researchers tend to create their own measures which make it difficult to compare and analyze different studies (Aupperle, Carroll, and Hatfield, 1985). Despite varying philosophies and definitions, the premise of CSR is that companies have ethical and moral obligations to society that, while not required, are expected (Carroll 2004).

**Cybersecurity Social Responsibility**

Consumers become vulnerable to different kinds of data breaches by dealing with organizations. In addition to achieving positive economic gains, companies are also expected to demonstrate social responsibility and are therefore responsible for safeguarding private information through CSR (Hovav and Gray 2014). Culnan and Williams (2009), believe that it is the moral responsibility of the organizations to ensure that necessary precautions are in place to prevent such events, and that when an organization has a keen sense of moral responsibility it is more likely to implement processes aimed at preventing data breaches from occurring.

**Small Enterprises and Organizations**

Numerous metrics indicate that small and medium business organizations function as the backbone of the U.S. economy. The Small Business Administration (SBA 2014) reported small businesses account for 99% of U.S. employer firms and 49% of private sector employment. As a result, 60,000,000 people are employed in small or medium business (United States Census Bureau 2008). Job creation is a frequently cited indicator of the U.S. economy and SMEs created 63% of the net new jobs between 1993 and mid-2013 (Small Business Administration 2014). These statistics portray the economic and societal significance of SMEs and, consequently, validate the need for research focused on SMEs.

**Data Breaches and Cyber-attacks at Small Enterprises and Organizations**

It is a common misconception that that large corporations are more likely to be at risk of cyber-attacks and data breaches than smaller enterprises (Bhattacharya 2015). However, while the information from larger enterprises may be desirable, the lax security practices of smaller enterprises make them desirable to cyber criminals (Gupta and Hammond 2005). According to the Verizon 2012 Data Breach Investigation Security Report, small enterprises were the primary victims of data breaches.

**Methodology**

This study will employ a mixed methods research approach that combines qualities of both quantitative and qualitative research methods. The main idea of this mixed methods approach is that the combination of qualitative and quantitative approaches provides a more complete understanding of the research problem than either approach by itself (Creswell 2014). According to Venkatesh et al. (2013), a mixed methods approach is suitable for IS research as it provides a means to offer explanation and valuable insight into their area of study which would have been otherwise difficult with existing theories. Phase 1 of this work-
in-progress research study will use an expert panel review process via Delphi technique to review criteria and rankings for risk of data breach and cybersecurity social responsibility. The Delphi method is useful to conduct complex research studies where there isn’t sufficient understanding about a phenomenon (Skinner et al. 2015). There are instances where pretests and pilot tests are carried out but are often times not validated, however, in IS research instrument validation is highly recommended in order to strengthen the findings of the study (Straub 1989). Therefore, phase 2 of this study will utilize the expert validated rankings and criteria from the previous stage to conduct a pilot test to further validate the instruments. Researchers are encouraged to conduct pilot tests to avoid unexpected problems (Boudreau et al. 2001). The main goal of this work-in-progress research is to develop and validate a cybersecurity risk-responsibility taxonomy using SEs’ cybersecurity social responsibility and risk of data breach. Therefore, the final quantitative phase of this work-in-progress research study will be to collect data from 100 SEs in the US and conduct data analysis using the taxonomy developed to classify them based on the measures. The cybersecurity risk-responsibility taxonomy classifies SEs in terms of their cybersecurity social responsibility, i.e. whether they display concern for society (legal, ethical and discretionary responsibility) or concern for economic performance (profitability), and their associated risk of a potential data breach. Each cell of the cybersecurity social risk-responsibility taxonomy represents the possibility that an SE’s social responsibility may contribute to a risk of data breach. The first cell C1, consists of a low risk of data breach when SEs show a concern for society. This cell has been labeled ‘accountable’, suggesting that SEs in this cell demonstrate ethical awareness and are considered accountable. The second cell C2, consists of a low risk of data breach when SEs show concern for economic performance. This cell has been labeled ‘dependable’, suggesting that while responsibility focus is geared toward economic performance, SEs in this cell are still aware of the importance of securing against data breaches. The third cell C3 is labeled ‘engaged’, with a medium risk of data breach when SEs show concern for society. SEs in this cell participate in activities that put them at medium risk of a data breach. The fourth cell C4, consists of a medium risk of data breach when SEs demonstrate a concern for economic performance. This cell is labeled ‘liable’, suggesting that there may be a likely risk of data breach. The fifth cell C5, demonstrates a high risk of data breach SEs demonstrates a concern for society. This cell is labeled ‘lax’, suggesting that SEs in this cell are not strict in safeguarding against a Data breach. The sixth cell C6, represents SEs that are at high risk for a data breach when they demonstrate concern for economic performance. This cell is labeled ‘relaxed’, suggesting that SEs in this cell are oblivious to the potential of a risk of data breach.

![Figure 1: Cybersecurity Social Risk-Responsibility Taxonomy](image)

REFERENCES


