


2020

Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach

Keiona Davis

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Computer Sciences Commons](#), and the [Health Information Technology Commons](#)

Share Feedback About This Item

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social
Responsibility in Small Enterprises on Risk of Data Breach

by


Keiona Davis

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Keiona Davis conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

Dec 1, 2020

Date

Steven Terrell


Steven R. Terrell, Ph.D.
Dissertation Committee Member

December 1, 2020

Date

Boštjan Delak

Bostjan Delak, Ph.D.
Dissertation Committee Member

 Digitally signed by Boštjan Delak
Date: 2020.12.02 17:23:04 +01'00'

Date

Approved:

Meline Kevorkian

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

December 1, 2020

Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of Dissertation submitted to Nova Southeastern University in Partial
Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach

by
Keiona Davis
November 2020

With much effort being placed on the physical, procedural, and technological solutions for Information Systems (IS) cybersecurity, research studies tend to focus their efforts on large organizations while overlooking very smaller organizations (below 50 employees). This study addressed the failure to prevent data breaches in Very Small Enterprises (VSEs). VSEs 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. VSEs utilize Point-of-Sale (POS) systems that are exposed to cyberspace, however, they are often not equipped to prevent complex cybersecurity issues that can result in them being at risk to a data breach. In addition, the absence of federal laws that force VSEs to adhere to standards such as the Payment Card Industry Data Security Standard (PCI-DSS) leaves it up to the discretion of the VSEs to invest in cybersecurity countermeasures aimed at preventing a data breach. Therefore, this study investigated the role that cybersecurity social responsibility plays in motivating the owners of these companies to engage in cybersecurity measures geared at preventing data breaches.

This study developed and validated using Subject Matter Experts (SMEs) a cybersecurity risk-responsibility taxonomy using the constructs of VSEs' owners' perceived cybersecurity social responsibility (CySR) and risk of data breach (RDB) in order to better understand their level of exposure to a data breach. Exploratory Factor Analysis (EFA) using Principal Component Analysis (PCA) was conducted to extract the significant factors for CySR and RDB. The study also addressed whether there were significant differences in VSEs owners' perceived RDB and perceived CySR based on three demographics: (1) type of industry, (2) implementation of chip technology, (3) compliance with PCI-DSS.

This study was conducted in three phases. Phase 1 utilized a panel of 13 information security SMEs and used the Delphi technique to review characteristics for RDB and CySR that were derived from literature. The results of the expert review were subjected to further validation by means of a pilot study using a small sample of the study population (Phase 2). The pilot study population included 20 organizations with number of employees ranging from less than five to 50 total employees across seven different industries.

Phase 3 of the study included the main data collection using the modified survey instrument from the pilot study. 105 VSEs anonymously participated in the main data collection phase of the study. The collected data was subjected data EFA which identified three factors comprised of 15 items for RDB and two factors comprised of 13 items for CySR. In addition, descriptive statistics was obtained and evaluated to determine if significant

differences exist in VSEs owners' perceived RDB based on type of industry, implementation of Europay, Mastercard and Visa (EMV) chip technology and, compliance with PCI-DSS. One-way Analysis of variance (ANOVA) was used to evaluate whether significant differences existed based on the VSEs demographics.

The results of the study indicated that there was a statistically significant difference in both RDB and CySR for industry, use of EMV Chip and, PCI-DSS compliance. This study demonstrates that there is a relationship between CySR and cybersecurity and that the CySR instrument could be used to assess cybersecurity practices in small businesses. In addition, this study may assist organizations in understanding and mitigating cybersecurity data breaches.

Dedication

To my parents, Cynthia and Alphansus, my first educators and role models for instilling a desire to learn and continue learning. To my husband, Shawn, for your patience and support throughout this difficult and challenging process. To my sister Karyna and my brother Kaeon for your constant encouragement. To my children Joshua and Isabelle, I did this for you.

Acknowledgments

It is a blessing to have completed my doctoral studies. I give all praises to God. I am incredibly grateful to everyone who offered guidance and support throughout this challenging endeavor.

My sincerest gratitude for Dr. Yair Levy, my dissertation advisor, who taught me how to conduct research. For being patient and understanding the challenges I faced, and always encouraging me to continue working toward my goal. Countless times I was overcome with anxiety, and a meeting with Dr. Levy was all I needed to put my mind at ease and get back on track. His passion for teaching has inspired me, and I consider myself fortunate to have learned from him.

My dissertation committee members Dr. Steve Terrell and Dr. Boštjan Delak. Who took the time to review my work and provide extensive feedback. Dr. Delak's expertise in the information systems and cybersecurity field provided thorough guidance that shaped my final dissertation report. Dr. Terrell, whom I consider an expert in research methodology, offered excellent advice and suggestions that shaped this research.

I want to thank my family for all their love and encouragement. I am forever grateful to my wonderful husband, Shawn, who is always patient with me and did not entertain my quitting thoughts. A special thank you to my parents and siblings for believing in me and always being a source of inspiration.

Table of Contents

Abstract ii

List of Tables v

List of Figures vi

Chapters

1. Introduction 1

Background 1
Problem Statement 2
Dissertation Goals 5
Research Questions 8
Relevance and Significance 9
Barriers and Issues 10
Definitions of Terms 11
Summary 12

2. Review of the Literature 14

Introduction 14
Cybersecurity 14
Risk 21
Social Responsibility 25
Summary of What is Known and Unknown 28

3. Methodology 30

Research Methodology 30
Overview of Research Design 30
Instrument Development 32
Validity and Reliability 36
Sample 37
Data Analysis 38

4. Results

Expert Panel Review – Phase 1 43
Pilot Study – Phase 2 46
Main Data Collection – Phase 3 47

5. Conclusions, Implications, Recommendations and Summary

Overview 75
Conclusion 75
Discussion 75
Implications 77
Recommendations and Future Research 77

Appendices 43

A. Expert Panel Recruitment 43

B. Expert Panel Evaluation 44

C. Cycle 2 with Experts 52

D. Survey Instrument 55

E. Institutional Review Board Approval Letter 61

References 99

List of Tables

1. Data Breaches since 2010 17
2. Summary of Cybersecurity Studies 19
3. Summary of Risk Studies 26
4. Summary of Corporate Social Responsibility Studies 31
5. RDB factors and characteristics 38
6. CySR factors and characteristics 38
7. SME demographics 44
8. Demographics of the Pilot Study Population 46
9. Eigenvalue and Variance for RDB 50
10. RDB Factors resulting from PCA 52
11. List of RDB Items Grouped by Factor 53
12. Total Variance Explained 54
13. CySR Factors resulting from PCA 56
14. List of RDB Items Grouped by Factor 57
15. Demographics of the Study Population 59
16. Descriptive Statistics of RDB and CySR 60
17. Descriptive Statistics of RDB and CySR by Industry 63
18. ANOVA Results of Difference in RDB and CySR Based on Industry 66
19. Descriptive Statistics of RDB and CySR by Use of EMV Chip Technology 67
20. ANOVA Results of Difference in RDB and CySR Based on use of EMV Chip
Technology 69

List of Tables (Cont.)

21. Descriptive Statistics of RDB and CySR by PCI-DSS Compliance 70
22. ANOVA Results of Difference in RDB and CySR Based on PCI-DSS Compliance

List of Figures

1. Cybersecurity Social Risk-Responsibility Taxonomy 8
2. Overview of the Research Design 37
3. RDB Scree Plot 51
4. CySR Scree Plot 55
5. Cybersecurity Risk-Responsibility Taxonomy 61
6. Cybersecurity Risk-Responsibility Taxonomy by Industry (N=105) 64
7. Means and Standard Deviations of RDB by Industry (N=105) 64
8. Means and Standard Deviations of CySR by Industry (N=105) 65
9. Cybersecurity Risk-Responsibility Taxonomy by use of EMV Chip 67
10. Means and Standard Deviations of RDB by use of EMV Chip Technology 68
11. Means and Standard Deviations of CySR by use of EMV Chip Technology 68
12. Cybersecurity Risk-Responsibility Taxonomy by PCI-DSS Compliance 71
13. Means and Standard Deviations of RDB by PCI-DSS Compliance 71
14. Means and Standard Deviations of CySR by PCI-DSS Compliance 72

Chapter 1

Introduction

Background

Organizations are benefitting greatly from the advancement of Information Systems (IS) (Earl & Feeney, 2012). However, this also increases their exposure to data breaches (Gordon et al., 2014; Jang-Jaccard & Nepal, 2014; Shim, 2011).

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' information system (IS) security. The Joint Task Force (JTF) on Cybersecurity Education (2017), defined cybersecurity as "A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems" (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 & Von Solms, 2010; Von Solms & Van Niekerk, 2013). Reports from the Ponemon Institute

showed that over the past 3 years there has been an increase in cyber-attacks on small businesses (Ponemon Institute, 2016, 2017, 2018).

Very Small Enterprises (VSEs) are particularly at risk of data breaches due to the simplicity of their security measures (Berry & Berry, 2018; Harris & Patten, 2014). Straub and Welke (1998) defined a system risk as “the likelihood that a firm’s information systems are insufficiently protected against certain kinds of damage or loss” (p. 441). Risk can also be defined as “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2018, p.46). A cybersecurity risk stems from the interaction of these systems with cyberspace (Von Solms & Van Niekerk, 2013). One challenge faced by VSEs 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 (Plachkinova & Maurer 2018; 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 & 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 VSEs (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 developed a classification methodology and classify VSEs's potential to fall victim to a data breaches based on their cybersecurity social responsibility as well as their risk of data breach.

Problem Statement

The research problem that this study addressed is the failure to prevent data breaches, particularly in VSEs (Bhattacharya, 2011; Hovav & Gray, 2014; Shim, 2011). According to Berry & Berry (2018), VSEs lack information technology (IT) resources and knowledge and, as a result, are at great risk for having their systems.

In the United States (U.S.) there is no standard definition of a VSE or Small Enterprises. The U.S. Small Business Administration (SBA) offered different classifications to determine eligibility for SBA assistance and financing. According to the SBA (2014), a Small Enterprises 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, which appears to be very large when it comes to cybersecurity related issues. Thus, this study adopted 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 (~ \$11.8 million) (Commission, 2016).

Data breaches are not limited to large organizations, however, there is a void on IS security research on cybersecurity in VSEs (Groner & Brune, 2012; Gupta &

Hammond, 2005; O'Rourke, 2019). This may result from an evolution in cybercrime, where in prior years cybercriminals targeted larger organizations. As these organizations heightened their cybersecurity measures, cyber-attacks shifted to smaller companies (Bhattacharya, 2011). VSEs are especially exposed to data breaches because they tend to be less equipped to handle complex security issues due to a smaller structure and limited IS expertise (Cragg et al., 2011; Harris & Patten, 2014). VSEs tend to have limited resources, unqualified personnel and, a thorough understanding of the risk of a data breach (ENISA, 2016). In the event of a data breach, VSEs can face exorbitant costs that put them at risk of going out of business. A cyber-attack in 2014 cost t-shirt manufacturer 80stees.com over \$200,000 to resolve the issue (Berr, 2014).

Lorenzo-Molo and Udani (2013) defined responsibility as “the condition of being responsible or accountable” (p. 124). The corporate social responsibility (CSR) theory implies that organizations are not only responsible to immediate stakeholders, but instead to the wider society (Carroll & Shabana, 2010). While companies strive for economic gains, they also have a duty to balance social and economic responsibility (Hovav & Gray, 2014). Many definitions of CSR have surfaced over the years, however, one definition by Carroll (1979), has been widely used in research for the last three decades. Carroll (1979) defined CSR as “the social responsibility of a business encompasses the economic, legal, ethical, and discretionary expectations that society has of organizations at a given point in time” (p. 500).

Following credit card data breaches such as the Target Corporation, data breach in 2013, corporations are being motivated to implement the Europay, Mastercard, and Visa (EMV) standard for authenticating debit and credit card transactions (Gray & Ladig,

2015). The EMV technology uses a chip to securely store cardholders' data, however, variants of these hybrid credit and debit cards are still susceptible to data breaches because they possess both the magnetic stripe as well as EMV chip technology (Ogundele et al., 2012). The Payment Card Industry (PCI) Data Security Standard (DSS) exists to guide retailers in safeguarding against data breaches, however, without legal enforcement, they are not always utilized (Hovav & Gray, 2014; Morse & Raval, 2008). Park (2019), suggests that information security law is necessary, however, there are challenges such as effectively assessing damages or proving that an organization that was subject to a data breach took the necessary precautions. Moreover, in general, the risk involved in such breaches is normally transferred to the consumer, credit card issuer, or processor. According to Hovav and Gray (2014), even though the merchant may be the source of the breach; the consumer, or credit card issuer tend to experience the brunt of the punitive and financial damages, with fines being imposed on the processors and not the merchants. While the standards imposed by credit card companies may facilitate secure financial transactions, the implementation of these standards is not government mandated (Morse & Raval, 2008; Park, 2019). As such, it is unclear how VSEs are encouraged to invest in cybersecurity preventative measures and/or comply with PCI-DSS standards, thus, warranting additional research on the role of VSE's responsibility in the context of cybersecurity as well as the VSEs' RDB.

Relevance and Significance

The increasing use of computing technology and their interconnectivity with the Internet places organizations who store or transmit sensitive information at risk to data

breaches (Gordon et al., 2014; Jang-Jaccard & Nepal, 2014; Shim, 2011). This study is relevant, as VSEs play an important role in the U.S. economy and supply chain (SBA.gov). VSEs often they perceive themselves to be exempt from cyber-attacks, however, they are particularly at risk of data breaches due to the sensitive information they store and transmit, while having limited investment in cybersecurity countermeasures (Bhattacharya, 2011; Harris & Patten, 2014). In the event of a data breach, these VSEs can face financial costs, tarnished reputation, or loss of customers (Gordon & Loeb, 2002; Kauffman et al., 2011; Son, 2011).

A great number of IS cybersecurity research studies focus on large organizations with few studies being conducted on cybersecurity in smaller organizations (Gafni & Pavel, 2019). Therefore, the significance of this study is that it adds to the body of knowledge regarding social responsibility and the role it plays in preventing data breach in VSEs.

Dissertation Goals

The main goal of this research was to develop and validate a cybersecurity risk-responsibility taxonomy for VSEs' owners' perceived cybersecurity social responsibility (CySR) and risk of data breach (RDB) in order to classify their business level of exposure to a data breach. This dissertation developed on previous research by Hovav and Gray (2014), who studied the T.J. Maxx breach of 2006, and suggested that VSEs have an ethical responsibility to safeguard private information through CSR. According to Perrini et al. (2011), the rejection of CSR can limit an VSE's understanding of their surrounding environment and consequently result in a loss of business opportunities. According to the

Financial Crisis Inquiry Commission (2011), a break down in the standards of responsibility, as well as ethics, caused a financial crisis resulting in loss of trust in the financial system by investors, businesses, and the general public. In the finance sector after the Enron scandal and subsequent recession, CSR became recognized as a necessity to support sustainable business by promoting socially responsible business practices as well as ethical management practices (Holzer & Junglas, 2013). CSR research tends to focus on large organizations, however, it appears that there is a void in CSR research on VSEs (Fassin et al., 2011). As a result, the focus of this study was on cybersecurity social responsibility in VSEs.

This dissertation extends beyond identifying technological solutions for mitigating IS security risks to investigate the role of VSEs' owner's perceived CySR and RDB. According to Spears and Barki (2010), the existing efforts to understand and manage IS security risks tend to focus on technological areas rather than non-technical sources such as personnel, policies, processes, as well as culture. In addition, Soomro et al. (2016), suggest that a more holistic approach involving managers and human contribution in general can impact organizational performance. IS security can be deemed as a technical or behavioral organizational issue, however, technical efforts alone are unable to identify the behavioral causes of a data breach. As such, studies that support the framework outside of the IS discipline are necessary to understand the impact of behavior on IS security (Choo, 2011; Julisch, 2013; Kaur, 2016; Posey et al., 2014).

This study was built on four specific goals. The first specific goal of this research used a team of Subject Matter Experts (SMEs) using the Delphi methodology in order to identify key characteristics for VSEs' owners' perceived RDB, and separately, to identify

key characteristics for CySR. To measure CSR, other researchers have used the Kinder, Lydenberg, and Domini (KLD) ratings, while others have developed survey instruments (Carroll & Shabana, 2010). Given that CSR measure in cybersecurity does not appear to exist in literature, this study used the Delphi method with the team of SMEs to design a survey instrument for measuring CSR (Ramim & Lichvar, 2014). The second goal of this research was to identify the factors for VSEs RDB and CySR. Doing so, allowed the development of the grouping of categories (i.e. factors) of the key characteristics for each of the constructs (RDB & CySR) in order to develop the aggregated scores for classification of the level of exposure to a data breach. The third goal of this research was to collect data from 100 VSEs and plot the aggregated scores of VSEs' owner's perceived CySR and RDB on the cybersecurity risk-responsibility taxonomy (Figure 1). The fourth goal was to assess whether significant differences exist in VSEs' owners' perceived CySR and RDB based on type of industry, implementation of EMV chip technology, and compliance with PCI-DSS using the cybersecurity risk-responsibility taxonomy.

Figure 1

Cybersecurity Risk-Responsibility Taxonomy for Classifying VSE's Level of Exposure to a Data Breach

Cybersecurity Social Responsibility (CySR) Concern for Society Concern for Economic Performance	[C1] Lax	[C3] Engaged	[C5] Accountable
	[C2] Relaxed	[C4] Liable	[C6] Dependable
	Low	Medium	High

**VSE's Owners Perceived Risk
of Data Breach
(RDB)**

Research Questions

The main research question this study addressed was: what characteristics SMEs consider important for developing the measures of CySR and RDB, along with how are VSEs classified in the cybersecurity risk-responsibility taxonomy? The specific research questions for this study are:

RQ1a What specific characteristics will be identified by SMEs as being important for VSEs owners' perceived RDB?

RQ1b What specific characteristics will be identified by SMEs as being important for VSEs owners' perceived CySR?

RQ2a What will be the significant factors for VSEs owners' perceived RDB?

RQ2b What will be the significant factors for VSEs owners' perceived CySR?

- RQ3 How will the aggregated scores of 100 VSEs for the measures CySR and RDB be positioned on the cybersecurity risk-responsibility taxonomy?
- RQ4a Will significant differences exist in VSEs owners' perceived RDB based on three demographics: (1) type of industry, (2) implementation of EMV chip technology, (3) compliance with PCI-DSS?
- RQ4b Will significant differences exist in VSEs owners' perceived CySR based on three demographics: (1) type of industry, (2) implementation of EMV chip technology, (3) compliance with PCI DSS?

Barriers and Issues

This research study was faced with barriers and issues. One issue of concern is that some members of the chosen expert review panel did not provide helpful or constructive responses. They were provided with open-ended questions on the survey instrument and encouraged elaborate further on their quantitative selections. Another issue was that the overall views of the experts was limited to the panel members that are selected. Therefore, using the Delphi technique, literature review, and pilot study alleviated this issue.

The survey instrument itself was also a possible barrier, in that, it may be viewed as long and drawn out, which could result in fewer responses than desired. To combat this, face to face and phone interviews were conducted whenever possible.

Definitions of terms

The following represent terms and definitions.

Corporate Social Responsibility – “The social responsibility of a business encompasses the economic, legal, ethical, and discretionary expectations that society has of organizations at a given point in time” (Carroll, 1979, p. 500).

Cyber-attack – “An attack, via cyberspace, that targets an enterprise’s use of cyberspace for the purpose of disrupting, destroying, or maliciously controlling a computer environment/infrastructure; destroying the integrity of the data; or stealing controlled information” (NIST, 2012, pp. B-3).

Cybersecurity – “A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems” (Joint Task Force on Cybersecurity Education, 2017 p. 16). Or “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” (DOD, 2017, p. 58).

Cyberspace – “A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers” (DOD, 2017, p. 58).

Data Breach – the compromise of electronic data by way of the Internet that results in unauthorized access to personal identifiable information (Whitehouse.gov, 2015).

Personal Identifiable Information – Any information about an individual that can be used to distinguish or trace an individual's identify and any other information that is linked or linkable to an individual (NIST, 2018, p. 1).

Risk – “A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (NIST, 2018, p. 46). Or “Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is “risk” (ISO, 2018).

Systems Risk – “the likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss” (Straub & Welke, 1998, p. 144)

Threat – “A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service” (NIST, 2012, p. B-3).

Vulnerability – “A weakness in a system that can be exploited to violate the system’s intended behavior relative to safety, security, reliability, availability, and integrity or to obtain access to some asset” (Andrews & Whittaker, 2004, p. 70).

Summary

Chapter One described the research problem, research goals, relevance and significance, as well as barriers and issues of this research study. The research problem

that this study addressed is the failure to prevent data breaches, particularly in VSEs. Literature outlining the problem and justifying the need for this study was presented.

The main goal of this research was to develop and validate a cybersecurity risk-responsibility taxonomy using VSEs owners' perceived CySR and RDB for classification of the VSEs base on their level of exposure to data breach. A definition of the research questions was presented in this chapter. The main research question: what characteristics SMEs consider important for developing the measures of CySR and RDB, along with how are VSEs classified in the cybersecurity risk-responsibility taxonomy? The relevance and significance of the study as well as barriers and issues were also discussed. Finally, a list of definitions of terms to be used throughout the study was presented.

Chapter 2

Review of the Literature

The following is a literature review derived from relevant research studies appropriate to cybersecurity, risk of data breach, corporate social responsibility, data breaches, and risk mitigation in small enterprises.

Cybersecurity

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 & Von Solms, 2010; Von Solms & Van Niekerk, 2013). According to Chopra and Chaudhary (2020), the securing of personal information stored by individuals as well as organizations is important especially in the banking transactions where the use of debit and credit cards are prevalent. The overall intent of cybersecurity is to safeguard the Confidentiality, Integrity, and Availability (CIA) of information systems on the Internet (Von Solms & Van Niekerk, 2013). The term cybersecurity is frequently used in academic and business literature, as well as, the news media. However, many definitions for cybersecurity exist, therefore, a concise definition capturing the multidimensional nature of cybersecurity is necessary (Craig et al., 2014). Early definitions for cybersecurity focused on primarily securing computers and computer networks, particularly from a defense viewpoint while more recent definitions include human interactions, policies, training, risk management and, awareness. The Joint Task Force (JTF) on Cybersecurity Education (2017), defined cybersecurity as “A computing-based

discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems” (p. 16). Craigen et al. (2014), used a shortlist of nine definitions found in literature to identify dominant themes in cybersecurity to define cybersecurity as “the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights”. Jang-Jaccard and Nepal (2014) described cybersecurity as being “concerned with the understanding of surrounding issues of diverse cyber-attacks and devising defense strategies (i.e., countermeasures) that preserve confidentiality, integrity, and availability of any digital and information technologies” (p.974). Von Solms and Van Niekerk (2013) distinguished between cybersecurity and information security. According to von Solms and van Niekerk (2013), “cybersecurity goes beyond the boundaries of traditional information security to include not only the protection of information resources, but also that of other assets, including the person him/herself” (p. 97). As seen with the definitions of cybersecurity, research studies also show that technological solutions for cybersecurity by themselves are not entirely effective in engaging cybersecurity, as such, policies and laws for software development and practices are necessary (Kosseff, 2018).

Cybersecurity Threats & Cyber-Attacks

A cybersecurity threat is frequently the result of Internet-based activities and may affect those technologies connected directly or indirectly to computers and networks. The use of popular software products over the Internet creates opportunities for attack on information systems and assets that results in enterprises suffering from financial losses

and other negative consequences (Galbreth & Shor, 2010). The Internet provides numerous benefits for nations who openly engage with each other by means of Information and Communication Technologies (ICT), however, this creates a prime opportunity for cyber-attacks. A cyber-attack is an attack carried out in cyberspace and, “targets an enterprise’s use of cyberspace for the purpose of disrupting, destroying, or maliciously controlling a computer environment/infrastructure; destroying the integrity of the data; or stealing controlled information” (NIST, 2012, pp. B-3). With cyberspace comes no geographical borders and, in turn, extends the field for criminals to carry out cyber-attacks (Choo, 2011; Jang-Jaccard & Nepal, 2014). In addition, 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 & Gray, 2014).

According to Hui, et al. (2017), attackers are motivated by incentives and are strategic in choosing who to attack. As a result, very small enterprises have been the prime targets. In 2015 cyber-attacks on both large and small enterprises cost the global economy \$575 billion, with malware being the most popular attack tool with 430 million new and unique malware pieces (Symantec, 2016). In 2018 the most popular attack tool was formjacking which saw cyber criminals targeting payment card data on ecommerce sites. Broadcom (2019), reported 4,818 different websites were compromised with formjacking each month in 2018. The Attacks on information systems have been the subject of research for some time. Loch, et al., (1992) reported that companies who used telecommunications to share information and other resources understood the threat of a security breach, however, they believed that the potential of an attack was low. Studies

on cyber threats and attacks focus on deterrence as a means of preventing them.

Organizations may face different types of threats are direct or indirect in nature, which poses a challenge to identify and prepare for possible indirect threats (Ilvonen & Virtanen, 2013).

Data Breach

A data breach may occur as a result of personally identifiable confidential information such as names, social security numbers, date of birth, telephone numbers, vehicle information, IP addresses, and credit card information being acquired through unauthorized access via theft or accident. The effect of a data breach is felt by organizations and individuals. According to Sen and Borle (2015), in the U.S. a single data breach can cost organizations as much as \$5.9 million. The privacy rights clearinghouse has been reporting on data breaches affecting consumers in the U.S. dating back to 2005. Since 2005, 9,016 data breach incidents have been reported in the U.S. (Privacy Rights Clearinghouse, 2019). In the year 2019, there were 3,950 confirmed data breaches across 81 (Verizon, 2020). 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 that included the largest breach ever to be publicly reported by a U.S. healthcare provider Anthem, which had 78 million patient records stolen. 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 & Dorantes, 2006; Ponemon, 2020). These breaches result in the merchant, consumer or financial institutions facing undesirable consequences (Gordon et al., 2014; Son, 2011). According to Sinanaj and Zafar (2016), reputation is significantly impacted by data breach

announcements. Reports show businesses such as Target, and Home Depot, Capital One, being the victims of such incidents (Banjo, 2014; Barrett, 2019; Zioboro, 2014). As such, organizations are faced with the task of employing countermeasures aimed at preventing data breaches.

Table 1*Data Breaches reported since 2010*

Year of Breach	Total number of Data Breaches
2010	140,937,393
2011	447,901,379
2012	298,766,833
2013	158,789,584
2014	1,313,623,927
2015	318,837,458
2016	4,815,012,420
2017	2,051,817,513
2018	1,370,710,973

Countermeasures

The ability to prevent or protect themselves from cyber-attacks and data breaches is one of the biggest issues organizations are faced with (Baskerville et al. 2018; Gupta & Hammond, 2005; Jang-Jaccard & Nepal, 2014). Countermeasures help to lessen the impact of such data breaches (Sawik, 2013; Viduto et al., 2012). Technical and operational countermeasures prevent physical access, as well as, those that block virtual access to networks and computers (Rees et al., 2011). Technical countermeasures include those controls that are built into hardware, software, and firmware. These technical countermeasures may include 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 & Gallagher, 2012). Research shows that data breach laws can have an impact on data breach depending on the level and region. According to Sen and Borle (2015), the strictness of state-level data breach security laws is correlated with reduced RDB. Data breach disclosure laws reduce identity theft, however, there is no significant relationship between the strictness of laws on identity theft, nor in regions of higher population (Romanosky et al., 2011).

Cybersecurity standards and guidelines are meant to enhance cybersecurity. Standards are fundamental in safeguarding an organization's information assets from the threat of a data (Silva et al., 2016). According to Smith et al. (2010), the use of a standard as the basis for securing information systems against unwarranted attacks that can compromise their operation, is fundamental to the process of implementing and accrediting organizations' security. Srinivas et al. (2018), also argue that standards play a critical role in information security and recommend that decision makers encourage the use of standards in both public and private sectors.

Siponen and Willison (2009) also highlighted the need to understand information security standards, stating that, while guidelines are good, it is important to encourage compliance through standards. There are numerous standards aimed at specifying or recommending control measures, including ISO/IEC 27000 family, 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 (Hui et al., 2012; Rees et al., 2011). However, standards by themselves have not proven to be sufficient, nor applicable for VSEs (Fenz et al., 2011; Rees et al., 2011; Silva &

Backhouse, 2003). Therefore, it is recommended that organizations include risk management as a method to warrant information systems security, especially for small and VSEs (Webb et al., 2014).

Table 2

Summary of Cybersecurity Studies

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Baskerville et al., 2018	Survey/Empirical analysis	9721 French firms	System integration and spend for cybersecurity countermeasures	There is a positive correlation between IS integration and the spend for security countermeasures
Choo, 2011	Literature Review			It is essential for governments, businesses and research institutions to quickly invest and create strategies and solutions for cybersecurity
Craigen et al., 2014	Literature review and expert analysis	None	Cybersecurity definitions	A concise definition of cybersecurity
Galbreth & Shor, 2010	Conceptual	Two companies	Market share and the likelihood of an attack	Popular software products offer more potential for attacks

Table 2*Summary of Cybersecurity Studies (Cont)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gordon et al., 2014	Empirical analysis	None	Level of cybersecurity activity expenditures and the probability of a cybersecurity breach	Cybersecurity underinvestment poses a serious threat to the national security and to the economic prosperity of a nation
Gupta & Hammond, 2005	Survey	138 small businesses	Written security policy, security breach experience, concern about virus-related problems	Small business owners may have procedures in place to counteract an information security threat, however, their effectiveness is uncertain
Hovav & Gray, 2014	Case Study/Analysis	One case	TJX security breach	Cyber-attacks go beyond the attacked organization to the society
Ilvonen & Virtanen, 2013	Literature review and scenario analysis	Three cyber threat scenarios	Types of challenges posed on information security challenges and preparation techniques	The formulation of policies from a threat/scenario perspective could effectively manage information security within a company

Table 2*Summary of Cybersecurity Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Jang-Jaccard & Nepal, 2014	Discussion		Cybersecurity vulnerabilities and emerging threats	Emerging technologies present new opportunities for data breaches
Ko & Dorantes, 2006	Comparative	19 firms that had security breaches related to confidential data	Financial performance, total assets, annual sales, and number of employees	Information security breaches have minimal long-term economic impact
Levy et al., 2013	Survey/Empirical Analysis	519 university business students	Attacks on the server, email interception, unauthorized file sharing, unauthorized access, and spoofing attacks	The majority of participants thought the ethical severity of e-learning security attacks were unethical or very unethical. A small percentage found them to be ethical or somewhat ethical

Table 2*Summary of Cybersecurity Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Jang-Jaccard & Nepal, 2014	Discussion		Cybersecurity vulnerabilities and emerging threats	Emerging technologies present new opportunities for data breaches
Ko & Dorantes, 2006	Comparative	19 firms that had security breaches related to confidential data	Financial performance, total assets, annual sales, and number of employees	Information security breaches have minimal long-term economic impact
Romanosky et al., 2011	Empirical analysis via secondary data	Identity theft reports between 2002 and 2009	Log of identity thefts, disclosure laws, adoption of laws	Data breach disclosure laws reduce identity theft, however, there is no significant relationship between the strictness of laws on identity theft, nor in regions of higher population

Table 2*Summary of Cybersecurity Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Sawik, 2013	Scenario based		Threat, countermeasure, attack scenario, countermeasure implementation level	The selection of countermeasures is based on their effectiveness of blocking different threats, implementation costs and probability of potential attack scenarios
Sen & Borle, 2015	Empirical study	Information on data breach incidents in the U.S. between 2005 and 2012	Opportunity theory of crime, the institutional anomie theory	The strictness of state-level data breach security laws is correlated with reduced risk of data breach
Sinanaj & Zafar, 2016	Comparative			Reputation is significantly impacted by data breach announcements

Table 2*Summary of Cybersecurity Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Son, 2011	Survey	602 employees in the United States	Perceived legitimacy, value congruence, perceived deterrent certainty, perceived deterrent severity and, employees' ISSP compliance	Variables rooted in the intrinsic motivation model contributed significantly more to the explained variance of employees' compliance than did those rooted in the extrinsic motivation model
Srinivas et al., 2018	Discussion	Existing literature		Standards play a critical role in information security and, as such, decision makers are encouraged to implement standards in both public and private sectors.
Van Nierkirk & Von Solms, 2010	Exploratory Study	Existing literature	Corporate culture, information security culture	Presented a conceptual model which could assist in improving the understanding of an information security culture

Table 2*Summary of Cybersecurity Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Von Solms & Van Nierkirk, 2013	Exploratory Study		Scenarios and examples	Highlights the difference between cybersecurity and information security

Risk

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 National Institute of Standards and Technology NIST (2012) defined risk as “a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence” (p. 12).

Risk Management

The process of identifying risks and applying the appropriate countermeasures is known as Risk Management (Spears & Barki, 2010). According to Spears and Barki (2010) greater awareness of security risks and controls contributes to improvements in design and implementation as well as performance. 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 security risks (Straub & Welke, 1998). In

addition, managers are often times not committed to IS security (Hu, et al., 2012; Puhakainen & 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 data breaches and in turn help to manage information security (Dhillon & Backhouse, 2001).

Information Systems Security Risk

Straub and Welke (1998) defined an IS security risk as “the likelihood that a firm's information systems are insufficiently protected against certain kinds of damage or loss” (p. 441). In differentiating between a threat and a risk, Schneier (2006) identified a threat as “a potential way an attacker can attack a system” (p. 20), while a risk takes “into consideration both the likelihood of the threat and the seriousness of a successful attack” (p. 20). According to Straub and Welke (1998), risk in the IS field is “the uncertainty inherent in doing business; technically it is the probability associated with losses (or failure), multiplied by the dollar loss of the risk if realized” (p. 442). Research shows that the existing efforts to understand and manage IS security risks tend to focus on technological areas rather than non-technical sources such as personnel, policies, processes, as well as culture (Spears & Barki, 2010; Cram et al., 2019). Studies on cybersecurity risks focus on risk management by identifying countermeasures to safeguard against risks from cyber-attacks (Mukhopadhyay et al., 2013; Rees et al., 2011; Sawik, 2013). Other studies explore quantitative and qualitative risk analysis methods as the basis for assessing IS security risks (Lee, 2014).

Risk of Data Breach

Companies become exposed to data breaches either as they engage in ecommerce

activities or, with physical POS transaction and system 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 & Van Niekerk, 2013) and, the likelihood that these systems are insufficiently protected against damage or loss (Straub & Welke, 1998). A data breach can result in the organization, consumer, or financial institutions facing undesirable consequences (Gordon et al., 2014; Son, 2011). Therefore, many organizations are placing the security of their ISs as a top priority, however, VSEs aren't (Webb et al., 2014).

Despite local state and federal laws regarding data breach notification and such, incidents of data breaches continue to happen in the U.S. 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 & Williams, 2009). According to Culnan and Williams (2009), incorporating moral responsibility in an organization's culture can minimize the effects of a data breach.

Table 3*Summary of Risk Studies*

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Culnan & Williams, 2009	Discussion	ChoicePoint and TJX data breaches		Incorporating moral responsibility in an organization's culture can minimize the effects of a data breach
Dhillon & Backhouse, 2001	Discussion/Review of literature			Information systems security research is moving away from technical viewpoint to a more socio-organizational perspective
Fenz et al., 2011	Case study	Two small to medium European enterprises	Control evaluation, risk determination, threat probability determination, inventory, and business process importance determination	Presented a model for supporting the risk management process. A subsequent case study proved this methodology to be beneficial when compared to previous methodologies

Table 3*Summary of Risk Studies(Cont)*

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Gordon et al., 2014	Empirical analysis	GL model	Level of cybersecurity activity expenditures and the probability of a cybersecurity breach	Cybersecurity underinvestment poses a serious threat to the national security and to the economic prosperity of a nation
Hu et al., 2012	Survey	75 university students enrolled in MIS courses	Behavioral intention, attitudes towards behaviors, subjective norm, perceived behavioral control, perceived goal orientation, perceived top management participation	Top management participation in information security can influence employee compliance
Mukhopadhyay et al., 2013	Literature review and analysis		Business loss, security failure reporting, security element failure, organizational issues	The advocating of cyber-insurance as a way of minimizing the financial impact of financial losses from a data breach

Table 3*Summary of Risk Studies (Cont)*

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Hu et al., 2012	Survey	75 university students enrolled in MIS courses	Behavioral intention, attitudes towards behaviors, subjective form, perceived behavioral control, perceived goal orientation, perceived top management participation	Top management participation in information security can influence employee compliance
Mukhopadhyay et al., 2013	Literature review and analysis		Business loss, security failure reporting, security element failure, organizational issues	The advocating of cyber-insurance as a way of minimizing the financial impact of financial losses from a data breach
Puhakeinen & Siponen, 2010	Empirical – action research	16 employees and IS security managers from an electronic information application development company	Users attitude toward IS security issues	Compliance training coupled with communication is useful in employee compliance. In addition, IS security supported by top management is necessary to support compliance

Table 3*Summary of Risk Studies (Cont)*

Study	Methodology	Sample	Instrument or Construct	Main Findings or Contribution
Smith et al., 2010	Canonical action research	16 senior information systems security managers	Episodic power relations, rules of practice, and domination	There needs to be sufficient financial and managerial resources to effectively implement information security standards
Spears & Barki, 2010	Exploratory and Survey	Nine Interviewees and 228 members of ISACA	User participation, organizational awareness, business-aligned SRM, control development, and control performance	Greater awareness of security risks and controls contributes to improvements in design and implementation as well as performance

Social Responsibility

Corporate Social Responsibility (CSR)

Corporate Social Responsibility (CSR) has been a topic of concern for a number of 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. Bowen (1953) noted that CSR “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 the years, mainly from different areas of study deriving different meanings (Geva, 2003). 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 et al., 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). CSR studies have been conducted in different types of organizations to examine the relationship between CSR and financial performance of an organization. Aras et al. (2010) found that while there is no significant relationship between CSR and financial performance there was a relationship between firm size and CSR.

Cybersecurity Social Responsibility (CySR)

Cybersecurity Social Responsibility (CySR) is derived from the CSR theory, which implies that organizations are not only responsible to its direct stakeholders when it

comes to protecting there is assets, but also to the wider society (Carlton & Levy, 2017; Carroll & Shabana, 2010). 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 CySR (Hovav & Gray, 2014). Culnan and Williams (2009) also believed that it is the moral responsibility of the organizations to ensure that necessary precautions are in place to prevent data breach 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. According to Matwyshyn (2009), legal compliance does not equate to social responsibility, companies have an ethical obligation to offer information security as a moral duty. However, it appears that very little attention has been given in literature to the aspect of CySR, let alone how to measure or quantify it, which is one of the key goals of this study.

Table 4*Summary of Corporate Social Responsibility Studies*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Aras et al., 2010	Content analysis	Annual reports of 40 companies	CSR disclosure reports	While there is no significant relationship between CSR and financial performance there was a relationship between firm size and CSR
Aupperle et al., 1985	Empirical survey	Corporate CEOs	Economic, legal, ethical and, discretionary responsibilities	Contributes an empirical research to test CSR definitions
Carlton & Levy, 2017	Discussion			Cybersecurity skills are necessary for dealing with Advanced Persistence Threats and other cyber threat mitigation
Carroll, 2004	Analysis			Proposed a pyramid for global CSR implying that practice of CSR influences performance

Table 4*Summary of Corporate Social Responsibility Studies (Cont.)*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Geva, 2003	Comparative	Three CSR models		Social responsibility varies in different means, depending on the CSR model being explored
Hovav & Gray, 2014	Case Study/Analysis	One case	TJX security breach	Cyber-attacks go beyond the attacked organization to the society
Matwyshyn, 2010	Analysis		The relationship between law and business ethics	Legal compliance does not equate to social responsibility. Companies have an ethical obligation to offer information security as a moral duty

Summary of What is Known and Unknown

The interaction with cyberspace puts organizations at risk to cyber threats and attacks. These attacks vary in nature and span geographical boundaries thereby posing varying challenges for organizations (Jang-Jaccard & Nepal, 2014; Hovav & Gray, 2014). A review of literature was conducted to examine the existing research on cybersecurity, data breaches, risk management and, corporate social responsibility.

While technical and operational countermeasures will lessen the impact of a data breach, information security standards and laws are also needed to encourage strictness and foster compliance (Kosseff, 2018; Silva et al., 2016). Risk management identifies and implements the appropriate countermeasures. However, much of the existing risk management techniques tend to focus on the technological areas rather than non-technical (Spears & Barki, 2010; Cram et al., 2019).

It is a common misconception 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 cybercriminals (Gupta & Hammond, 2005). According to the Verizon 2017 Data Breach Investigation Security Report, small enterprises were the primary victims of data breaches.

VSEs are recognizing that they are at risk to cyber-attacks because hackers will attack any susceptible target. However, while numerous VSEs acknowledge the necessity of cybersecurity, they do not engage in preventative measures against cyber-attacks (Berry & Berry, 2018). According to Raghavan et al. (2017), one of the reasons VSEs fail to invest in cybersecurity is because they do not understand the associated costs as being essential and necessary to keep their businesses operational. They also do not have the IT expertise to implement the necessary countermeasures (Raghavan et al., 2017).

While small and medium size organizations outnumber their larger counterparts globally, Cybersecurity and CSR research studies tend to focus on large organizations (Gafni & Pavel, 2019). In addition, the role of responsibility in the IS research, in particular, security related research studies have not been thoroughly explored.

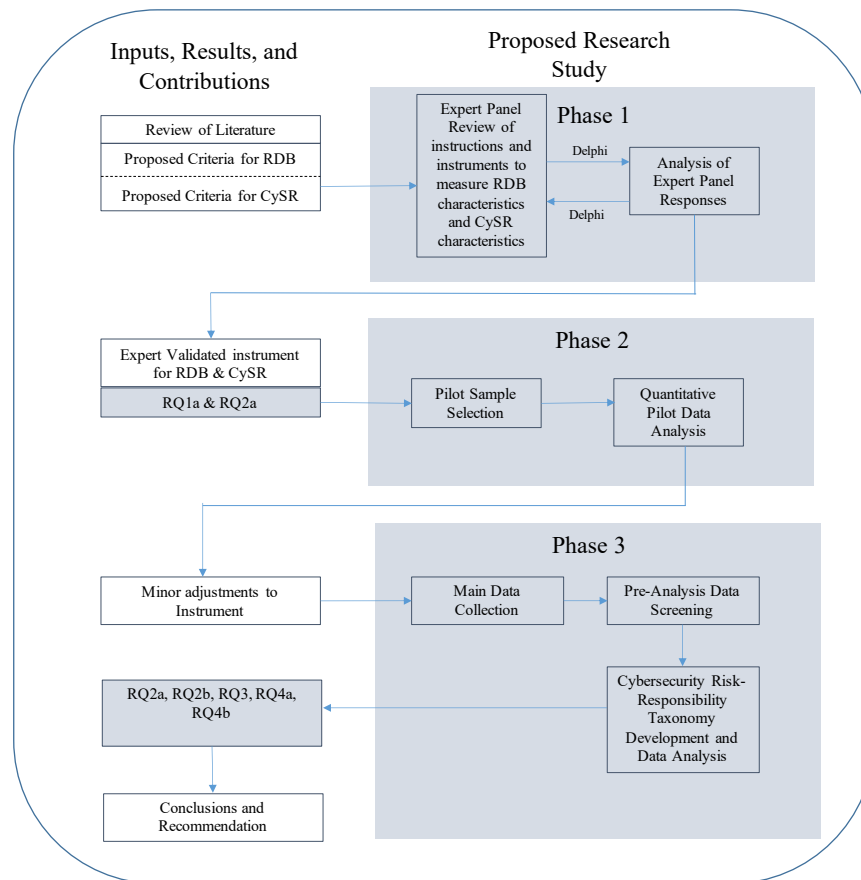
Furthermore, much of the research studies in the IS field around computer security and not much on cybersecurity.

Chapter 3

Methodology

Overview of Research Design

This study employed a quantitative approach for data collection and analysis. Figure 2 depicts the research overview of the research design. Phase 1 of this research study used Subject Matter Experts (SMEs) panel review process via the Delphi method to review the initial characteristics of RDB and CySR from literature to provide their qualitative feedback on the lists. The Delphi method is used to conduct complex research studies where there isn't sufficient understanding of a phenomenon using qualitative (for list completeness) and quantitative approach (for criteria rankings) (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 utilized the SMEs validated criteria and rankings from the previous stage to conduct a pilot test to further validate the instruments. Even skilled researchers are encouraged to conduct pilot tests to avoid unexpected problems (Boudreau et al., 2001). The main goal of this research was to develop and validate a cybersecurity risk-responsibility taxonomy for VSEs owners' perceived CySR and RDB. Therefore, the final quantitative phase of this research study (Phase 3) conducted data analysis and taxonomy development.

Figure 2:*Overview of the Research Design***Instrument Development**

The first step in developing the instruments for this study was to develop a thorough list of initial characteristics and factors for RDB and CySR. As shown in Table 5, a review of the current literature on risk and data breaches was used to establish the characteristics and factors of RDB. Similarly, as shown in Table 6, the characteristics and factors of CySR were drawn from current literature.

SMEs were asked to evaluate the list of characteristics for each construct and provide feedback on removal, adjustments, and additions. Following the SME evaluation, the original list of characteristics were finalized using the feedback from the SMEs.

Table 5*RDB factors and characteristics.*

Risk of Data Breach (RDB) Factors	Risk of Data Breach (RDB) Characteristics
External Risk from Cybercriminals	<ul style="list-style-type: none"> ✓ Lack of firewall software ✓ Lack of intrusion detection systems ✓ Lack of a password strength policy ✓ Unencrypted transmission of cardholder data ✓ Lack of security awareness to social engineering and phishing ✓ Lack of malware protection
Internal Risk from Users (Insider's Threat such as disgruntled employees or human error/mistake)	<ul style="list-style-type: none"> ✓ Lack of user knowledge and training ✓ Improper access permission (e.g. employees having unnecessary privilege) ✓ Improper access to software ✓ Lack of separation duties ✓ Weak encryption or poor key-management practices
Risk of Physical Intruder/Thief	<ul style="list-style-type: none"> ✓ Lack of physical monitoring ✓ Insecure handling of payment terminals ✓ Disposal of storage media with data ✓ Unsupervised visitors such as vendors

Table 6*CySR factors and characteristics.*

Cybersecurity Social Responsibility (CySR) Factors	Cybersecurity Social Responsibility (CySR) Characteristics
Economic CySR	<ul style="list-style-type: none"> ✓ The organization is successful at maximizing profits ✓ The organization strives to lower operating costs ✓ Owners/managers try to establish long-term strategies for the organization
Legal CySR	<ul style="list-style-type: none"> ✓ Owners/managers are aware of cybersecurity laws ✓ Software products meet legal standards ✓ Owners/managers try to comply with the law

Table 6*CySR factors and characteristics (Cont.).*

Cybersecurity Social Responsibility (CySR) Factors	Cybersecurity Social Responsibility (CySR) Characteristics
Ethical CySR	<ul style="list-style-type: none"> ✓ The organization has a comprehensive information security policy ✓ The organization follows information security standards ✓ The organization is recognized as a trustworthy company ✓ A procedure is in place for employees to report misconduct or misuse of information systems
Discretionary CySR	<ul style="list-style-type: none"> ✓ The organization tries to improve its corporate image ✓ The organization tries to improve the perception of how it conducts business ✓ The organization contributes to the bettering of the local community

Validity and Reliability

The reliability and validity of a measurement instrument are vital and is the first line of defense against inaccurate conclusions (Salkind, 2009). According to Creswell (2002), reliability and validity of an instrument should provide “an accurate assessment of the variable and enable the researcher to draw inferences to a sample or population” (p. 180). There are two constructs in this study, CySR and, RDB, both are measured from the perspective of the business owner or managers. The measurement instrument was validated to ensure they measure what they intend to measure. According to Terrell (2016), “a well-developed test must consistently measure what it’s intended to measure” (p. 82). A panel of SMEs were used to ensure the validity of the proposed instruments that were derived from previous research studies. The SMEs were requested to provide feedback on the proposed instrument (Appendix B). According to McFadzean et al.

(2011), the Delphi technique “ensures that the data collection process is both reliable and valid because it exposes the investigation to differing, and often divergent, opinions and seeks convergence through structured feedback” (p. 108). Therefore, in order to ensure validity and reliability, this study will gather feedback from the SMEs to verify that the proposed measures are appropriate to assess CySR and RDB. A pilot study was also conducted using a sample of 20 VSEs to further verify the validity of the proposed instrument.

Internal Validity

Salkind (2009) described internal validity as “the quality of an experimental design such that the results obtained are attributed to the manipulation of the independent variable” (p.231). Salkind (2006) stated that instrumentation is a possible threat because “when the scoring of an instrument itself is affected, any change in the scores might be caused by the scoring procedure, rather than the effects of the treatment” (p. 224). The use of the expert panel via the Delphi method will ensure initial internal validity.

External Validity

According to Creswell (2002), “External validity threats arise when experimenters draw incorrect inferences from the sample data to other persons, other settings, and past and future situations” (p. 176). Prior to the main data collection, this study was conducted with a small pilot group of the sample population. Additionally, the main data collection was done amongst different groups with different demographical markers including the type of industry, implementation of EMV chip technology, compliance with PCI-DSS.

Sample

The unit of analysis for this research study is the assessment of results from VSEs who utilize POS systems. About 400 companies were invited to participate in the study from a list of small companies that conduct credit card transactions. With an anticipated response rate of about 25%, a total of 100 participants were expected to take part in this study.

Data Analysis

The responses were analyzed to detect accuracy, response set, missing data, and outliers. This study addressed RQ1a and RQ1b via the Delphi methodology to identify the instrument to measure RDB & CySR.

The aggregated scores for RDB and CySR were based on the Equations 1 and 2.

$$\text{Eq. 1:} \quad \text{RDB} = (1/C1) * (w_{A1} * A1 + w_{A2} * A2 \dots + w_{Ax} * Ax)$$

RDB has a range of 0-100, where x is the final number of item for the RDB construct, the w_s are the weights assigned to the items from the SMEs, as are the items for RDB construct (See Appendix B), C1 is a constant coefficient to normalize the aggregated score for RDB from 0 to 100.

$$\text{Eq. 2:} \quad \text{CySR} = (1/C2) * (w_{B1} * B1 + w_{B2} * B2 \dots + w_{By} * By)$$

CySR has a range of 0-100, where y is the final number of item for the CySR construct, w_s are the weights assigned to the items from the SMEs, B_s are the items for RDB construct (See Appendix B), C2 is a constant coefficient to normalize the aggregated score for CySR from 0 to 100.

Resources

This research study involved human subjects, therefore, the Institutional Review Board (IRB) approval was needed to carry out this study. The Delphi technique expert panel review process required access to cybersecurity professionals. In addition to the above-mentioned resources, a computer, Internet access, Microsoft Word[®], Microsoft Excel[®], Microsoft PowerPoint[®], SPSS[®], post office box, and email accounts was required to carry out the study.

Summary

Chapter three provided the methodology overview that was used in this research study. This study employed a sequential-exploratory mixed methods design using qualitative phase followed by a quantitative data collection and analysis. This study was conducted in three phases to ensure reliability and validity of the results. Phase 1 of the study used SMEs to identify the characteristics for RDB and CySR via the Delphi method. Phase 2 involved a pilot test with a small sample of the population. The final phase 3 involved the data analysis and taxonomy development.

Chapter 4

Results

This chapter outlines the results of the data collection and data analysis for this research study. The results for this study were completed in three phases. Phase 1 entailed the data collection from the expert panel using the Delphi technique to review the initial characteristics of RDB and CySR and to provide their qualitative feedback on the lists.

Phase 2 of this study utilized the SMEs validated criteria and rankings from the previous stage to conduct a pilot test to further validate the instruments. Phase 3, the final stage of this research study developed and validated a cybersecurity risk-responsibility taxonomy for VSEs owners' perceived CySR and RDB.

Data Analysis and Results

Expert Panel Review - Phase 1

The first step in developing the instruments for this study was to develop a thorough list of initial characteristics for RDB and CySR. A review of the current literature on IS risk and data breaches and cybersecurity social responsibility was used to establish the characteristics and factors of RDB and CySR. SMEs were asked to evaluate the list of characteristics for each construct and provide feedback on removal, adjustments, and additions using google forms (See Appendix B). This phase of the study took place between March and May 2019. A panel of 26 experts was targeted with 13 responding, representing 50% response rate. The agreement percentages ranged from

69% to 100% for the questions that were presented to the SMEs. Following the SME evaluation, the original list of characteristics was finalized using the feedback from the SMEs. Table 7 represents the descriptive statistics of the expert panel members.

Table 7

SME Demographics (N=13)

Demographic Item	Frequency	Approximate Percentage
Age:		
25-29	1	7.7%
30-34	1	7.7%
40-44	2	15.4%
45-49	4	30.8%
50-54	4	30.8%
55-59	1	7.7%
Industry:		
Academic	5	38.5%
Government/Military	4	30.8%
Private Organization	4	30.8%
Years of cybersecurity experience:		
Less than 1 year	0	0%
2-5 years	3	23.1%
5-10 years	3	23.1%
10-15 years	4	30.8%
15-20 years	0	0.0%
Over 20 years	3	23.1%
Formal cybersecurity training or certification:		
Training only	5	38.5%
Certification only	0	0.0%
Training and certification	8	61.5%
No training or certification	0	0.0%

The ages of the SMEs ranged from 25 to 59 years old, with the majority of SMEs

aged 45 to 49 years old (4; 30.8%) and 50 to 54 years old (4; 30.8%). For type of industry, SMEs 5 (38.5%) were in academia, 4 (30.8%) were government or military and, 4 (30.8%) identified as private organization. The majority of SMEs had 10-15 years of cybersecurity experience (4; 30.8%) while 3 (23.1%) had over 20 years experience. For cybersecurity training and certification, 8 (61.5%) achieved both training and certification while the remaining 5 (38.5%) obtained training only.

Risk of Data Breach

SMEs were asked to provide a recommendation for keeping, adjusting, or removing each of the proposed characteristics. SMEs were also encouraged to provide an explanation for their recommendation if it involved removing or adjusting as well as suggest additional characteristics to be included. The overall response from the SMEs was that the characteristics remain as proposed. The consensus percentages for RDB characteristics ranged from 85% to 100% with the exception of “Unencrypted transmission of cardholder data” which had a 69% consensus. As a result, the characteristic was changed to read “Unencrypted transmission of sensitive data”, as was suggested.

Cybersecurity Social Responsibility

SMEs were asked to provide a recommendation for keeping, adjusting, or removing each of the proposed characteristics. SMEs were also encouraged to provide an explanation for their recommendation if it involved removing or adjusting as well as suggest additional characteristics to be included. The overall consensus percentages for RDB characteristics ranged from 85% to 100%. The SMEs who suggested adjusting as their response provided no explanation of their recommendation, as a result no changes

were made to the proposed characteristics.

Pilot Study – Phase 2

A total of 20 organizations participated in the pilot study for this research project. The purpose of this pilot study was to further validate the instrument and detect problems that could arise in the main study. The pilot study was conducted between June and September 2019 via email solicitation, telephone, and face to face interviews using the proposed survey instrument of the main study (see Appendix C). The pilot study population included 20 organizations with number of employees ranging from less than five to 50 total employees across seven different industries. The overall feedback from the pilot study did not warrant major changes to the survey instrument. However, during the interviews some organizations did not know how to respond to the question about obtaining PCI-DSS and, as a result, a new option for “uncertain” was added to the responses, as well as, an explanation of PCI-DSS.

Table 8

Demographics of the Pilot Study Population (N=20)

Demographic Item	Frequency	Percentage
Number of employees:		
Less than 5 employees	4	20.0%
6 to10 employees	6	30.0%
11 to 20 employees	6	30.0%
21 to 30 employees	2	10.0%
31 to 50 employees	2	10.0%
51 or more employees	0	0.0%

Table 8*Demographics of the Pilot Study Population (N=20) (Cont)*

Demographic Item	Frequency	Percentage
Industry:		
Business Services	1	5.0%
Food and Restaurant	4	20.0%
General Retail	2	10.0%
Health, Beauty and Fitness	4	20.0%
Automotive Repair	6	30.0%
Healthcare	2	10.0%
Other	1	5.0%
Credit Cards accepted:		
Yes	20	100%
No	0	0.0%
Use of chip reader:		
Yes	11	55.0%
No	9	45.0%
PCI-DSS compliant:		
Yes	9	45.0%
No	11	55.0%

Main Data Collection – Phase 3

During this phase the modified survey instrument from the pilot study was used to collect data from a larger set of organizations. Data collection took place between September and December 2019. Approximately 400 organizations were selected and contacted via email to participate in the study. 105 surveys were completed over the four-month period, constituting a response rate of 26%. Participation in the survey was anonymous and participants were given the option of exploring cybersecurity resources for small business on the Small Business Administration and the National Cybersecurity Alliance’s website upon completion.

Pre-Analysis Data Screening

This process was necessary to identify anomalies within the data collection and, to ensure that the data is accurate and reliable (Levy, 2006). The responses for the main data collection were gathered using Google Forms designed to eliminate errors and missed questions during the process. The collected data was transferred to excel worksheets and assigned a CaseID then visually inspected for incomplete or missed responses. Following the initial data screening, 105 responses were deemed usable and was loaded into SPSS for further pre-analysis data screening. Outlier detection was done using Mahalanobis distance box plot and no extreme multivariate outliers were identified.

Exploratory Factor Analysis

To address RQ2a (What will be the significant factors for VSEs owners' perceived RDB?) and, RQ2b (What will be the significant factors for VSEs owners' perceived CySR?) the main data was subjected to EFA using PCA using varimax rotation to extract factors of eigenvalue greater than one.

RDB Factor Analysis

The review of literature identified three factors for RDB; External Risk from Cybercriminals (ERCC), Internal Risk from users (IRU) and, External Risk of Physical Intruder/Thief (PIT). Exploratory factory analysis using PCA was conducted to identify as many factors as suggested by the data. Three factors were produced which were evaluated using eigenvalue, variance and, scree plot. The eigenvalue for the first factor was 7.8, the second factor was 1.5 and the third factor three 1.0 indicating that all three factors could be retained. After the varimax rotation, the first factor accounted for 52.4% of the loading while the second factor accounted for 10% and the third factor accounted

for 6.8% making the total variance 69.2% which was slightly lower than the recommended 70% of total variability. Table 9 shows the eigenvalue and variance of each factor.

Table 9

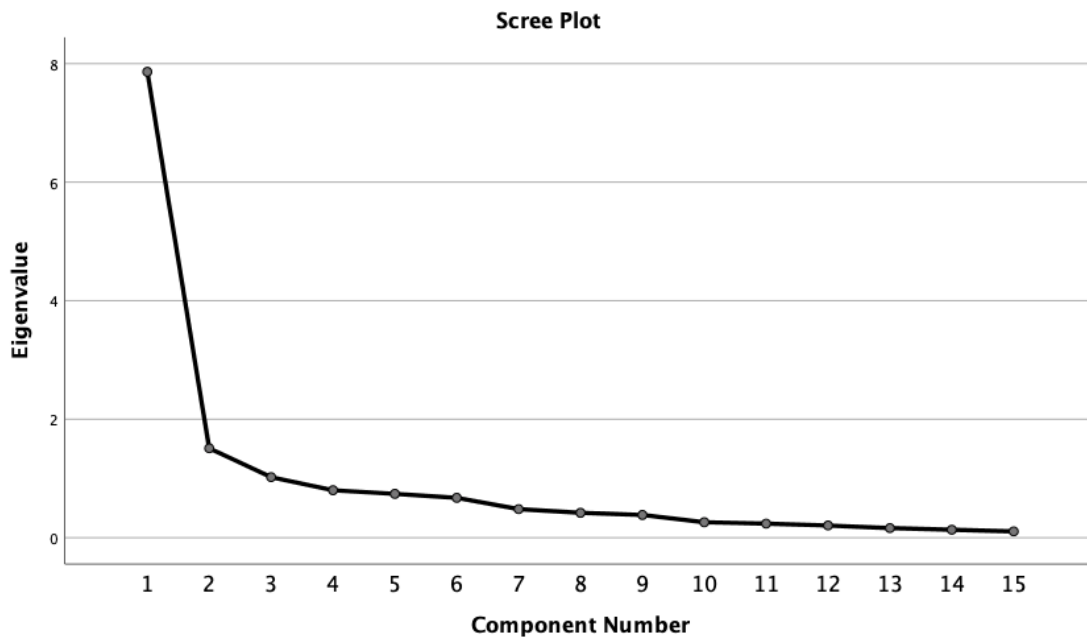
Eigenvalue and Variance for RDB

Factor	Total	% of Variance	Cumulative %
1	7.862	52.415	52.415
2	1.509	10.059	62.475
3	1.022	6.813	69.287
4	0.801	5.341	74.629
5	0.74	4.933	79.561
6	0.673	4.488	84.049
7	0.482	3.215	87.264
8	0.42	2.799	90.063
9	0.384	2.559	92.622
10	0.261	1.74	94.362
11	0.238	1.584	95.946
12	0.206	1.373	97.318
13	0.162	1.079	98.397
14	0.134	0.894	99.291
15	0.106	0.709	100

The scree plot (Figure 3) shows the plot leveling off after the third factor which suggested that the first three factors could be retained. Cronbach's Alpha reliability test was done to further test the reliability of each factor.

Figure 3

RDB Scree Plot



The Cronbach's Alpha for each factor was 0.701 or higher, which indicates reliability. The Cronbach's Alpha for each factor was: External Risk from Cybercriminals -0.898, Internal Risk from Users - 0.897, and Physical Risk from Outsiders - 0.701. The Cronbach's Alpha "if item is deleted" was calculated to further test the reliability of each item. The results indicate minimal change to Cronbach's Alpha of the second factor (IRU) if item PIT_A15 (Unsupervised visitors such as vendors) was deleted, however, based on literature and the expert panel review it was retained in the study. Table 10 represents the factor loadings and Cronbach's Alpha for RDB.

Table 10*RDB Factors resulting from PCA*

RDB Factor Name	Item	1	2	3	Cronbach's Alpha if Item Deleted
External Risk from Cybercriminals	ERCC_A5	0.811	0.030	0.270	0.881
	ERCC_A1	0.752	0.346	0.072	0.874
	ERCC_A3	0.742	0.435	0.050	0.871
	ERCC_A4	0.728	0.211	0.104	0.890
	ERCC_A2	0.723	0.458	0.004	0.877
	ERCC_A6	0.678	0.215	0.456	0.885
Internal Risk from Users	IRU_A10	0.242	0.822	0.208	0.869
	IRU_A9	0.254	0.721	0.307	0.874
	IRU_A8	0.409	0.720	0.270	0.864
	IRU_A7	0.532	0.710	0.022	0.872
	PIT_A12	0.266	0.672	0.244	0.896
	IRU_A11	0.496	0.651	0.244	0.868
	PIT_A15	-0.109	0.502	0.465	0.911
Physical Risk from Outsiders	PIT_A13	0.112	0.188	0.794	
	PIT_A14	0.316	0.287	0.735	
Factor Cronbach's Alpha →		0.898	0.897	0.701	

Upon completion of the data analysis for RDB, three factors comprised of 15 items were retained. The results of this analysis provided an answer to RQ2a: What will be the significant factors for VSEs owners' perceived RDB? Table 11 provides the final list of RDB items aligned with their associated RDB factors and definitions.

Table 11*List of RDB Items Grouped by Factor*

Item	RDB Factor	Owners Perceived RDB Characteristics
ERCC_A5	External Risk from Cybercriminals	Lack of security awareness to social engineering and phishing
ERCC_A1		Lack of firewall software
ERCC_A3		Lack of a password strength policy
ERCC_A4		Unencrypted transmission of cardholder data
ERCC_A2		Lack of intrusion detection systems
ERCC_A6		Lack of malware protection
IRU_A10	Internal Risk from Users	Lack of separation of duties
IRU_A9		Improper access to software
IRU_A8		Improper access permission (e.g. employees having unnecessary privilege)
IRU_A7		Lack of user knowledge or training
PIT_A12		Lack of physical monitoring
IRU_A11		Weak encryption or poor key-management practices
PIT_A15	Physical Risk from Outsider	Unsupervised visitors such as vendors
PIT_A13		Insecure handling of payment terminals
PIT_A14		Disposal of storage media with data

CySR Factor Analysis. Four factors were identified in the review of literature for CySR; Economic CySR (EcCySR), Legal CySR (LCySR), Ehtical CySR (ECySR) and, Discretionary CySR (DCySR), Exploratory factory analysis using PCA was conducted to identify as many factors as suggested by the data. Initial factor analysis was conducted

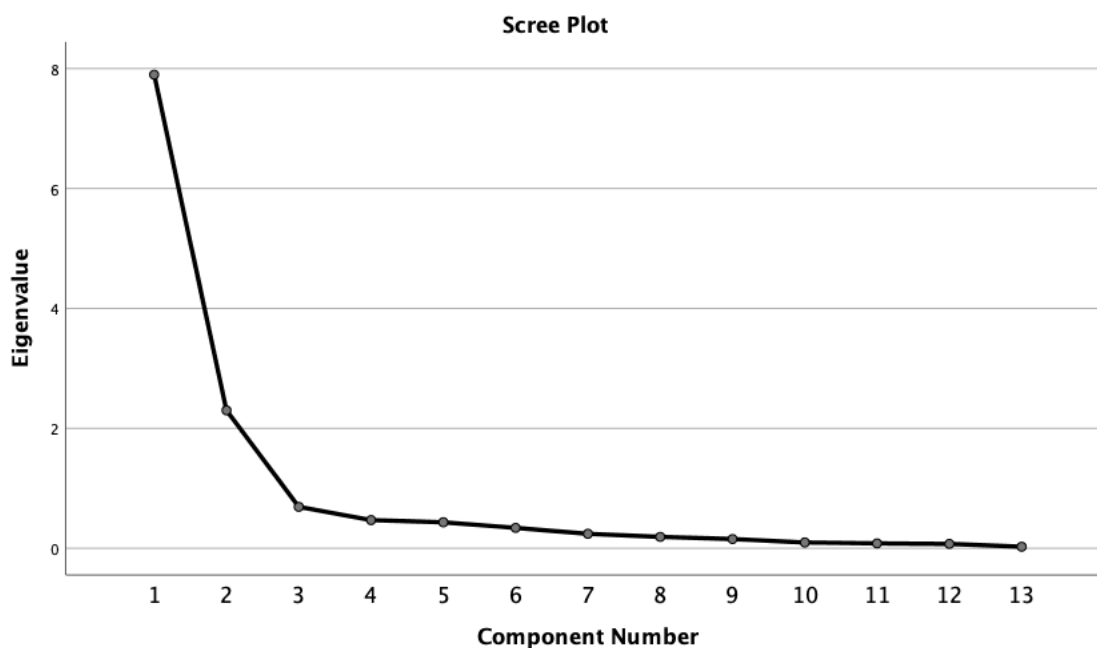
for four factors, then three factors, however, the eigenvalue suggested two factors with values greater than one. A final analysis was conducted on two factors using eigenvalue, variance and, scree plot. The eigenvalue for the first factor was 7.897 and the second factor was 2.301, both meeting the eigenvalue criteria. After the varimax rotation, the first factor accounted for 60.7% of the loading while the second factor accounted for 17.7% making the total variance 78.4% which was satisfies the criteria for at least 70% of total variability. Table 12 shows the eigenvalue and total variance for the factors.

Table 12

Total Variance Explained

Factor	Eigenvalue	% of Variance	Cumulative %
1	7.897	60.748	60.748
2	2.301	17.697	78.444
3	0.691	5.317	83.761
4	0.47	3.616	87.377
5	0.433	3.334	90.711
6	0.341	2.621	93.332
7	0.242	1.861	95.193
8	0.191	1.468	96.662
9	0.154	1.188	97.849
10	0.097	0.748	98.598
11	0.082	0.634	99.231
12	0.073	0.562	99.794
13	0.027	0.206	100

The scree plot (Figure 4) shows a steep descent for the first two factors, then the plot leveling off after the second factor which suggested that the first two factors could be retained.

Figure 4*CySR Scree Plot*

Cronbach's Alpha reliability test was done to further test the reliability of each factor. The Cronbach's Alpha for each factor was 0.942 or higher, which indicates reliability. The Cronbach's Alpha for each factor was: Ethical Responsibility -0.942, and, Legal Responsibility -0.944. The Cronbach's Alpha "if item is deleted" was calculated to further test the reliability of each item. Items ECySR_B1 and ECySR_B10 showed a slight increase if deleted, however, based on literature and the expert panel recommendation they were retained. Table 13 shows the factor loadings and Cronbach Alpha for CySR.

Table 13*CySR Factors resulting from PCA*

CySR Factor Name	Item	1	2	Cronbach's Alpha if Item Deleted
Business Responsibility	DCySR_B12	0.911	0.271	0.924
	DCySR_B11	0.905	0.245	0.925
	DCySR_B13	0.893	0.225	0.928
	ECySR_B9	0.840	0.192	0.933
	EcCySR_B3	0.821	0.255	0.934
	EcCySR_B2	0.805	0.257	0.934
	EcCySR_B1	0.559	0.516	0.950
Legal Responsibility	ECySR_B7	0.189	0.914	0.926
	ECySR_B8	0.228	0.899	0.926
	LCySR_B4	0.168	0.891	0.933
	LCySR_B6	0.320	0.869	0.928
	LCySR_B5	0.335	0.855	0.930
	ECySR_B10	0.247	0.692	0.955
Factor Cronbach's Alpha →		0.942	0.944	

Upon completion of the data analysis for CySR, two factors comprised of 13 items were retained. The results of this analysis provided an answer to RQ2b: What will be the significant factors for VSEs owners' perceived CySR? Table 14 provides the final list of RDB items aligned with their associated CySR factors and definitions.

Table 14*List of RDB Items Grouped by Factor*

Item	CySR Factor	CySR Characteristics
DCySR_B12	Business Responsibility	The organization tries to improve the perception of how it conducts business
DCySR_B11		The organization tries to improve its corporate image
DCySR_B13		The organization contributes to the bettering of the local community
ECySR_B9		The organization is recognized as a trustworthy company
EcCySR_B3		Owners/managers try to establish long-term strategies for the organization
EcCySR_B2		The organization strives to lower operating costs
EcCySR_B1		The organization is successful at maximizing profits
ECySR_B7	Legal Responsibility	The organization has a comprehensive information security policy
ECySR_B8		The organization follows information security standards
LCySR_B4		Owners/managers are aware of cybersecurity laws
LCySR_B6		Owners/Managers try to comply with the law
LCySR_B5		Software products meet legal standards
ECySR_B10		A procedure is in place for employees to report misconduct or misuse of information systems

Demographic Analysis

Following the pre-analysis data screening, the demographics of the participants of the study were analyzed. The participants of the study were VSEs throughout the United States of America. The participants varied across four demographics; number of employees, industry, size, use of chip card readers and, PCI-DSS compliance. The analysis of the number of employees within each organization showed that of the 105 participants, the majority (39 or 37.1%) employed between six and 10 employees, 27 VSEs or 25.7% employed 11 to 20 employees, 20 VSEs or 20%, 10 VSEs or 9.5% employed between 31 to 50 employees), while eight VSEs or 7.7% employed between 31 and 50 employees. The participants of the study represented 11 different businesses industries with the majority (16 or 15.2%) representing the automotive repair industry and 12.4% identifying as “other”. 60 VSEs or 57.1% had terminals that could read credit cards with EMV chip, while 45 or 42.9% did not have EMV chip technology. The data also showed that 46 participants or 43.8% had not obtained PCI-DSS compliance, while 37 VSEs or 39.2% had obtained PCI-DSS compliance and, the remaining 22 or 21% was uncertain about their PCI-DSS compliance status. The demographics of the population are presented in Table 15.

Table 15*Demographics of the Study Population (N=105)*

Demographic Item	Frequency	Percentage
Number of employees:		
Less than 5 employees	20	20.0%
6 to10 employees	39	37.1%
11 to 20 employees	27	25.7%
21 to 30 employees	10	9.5%
31 to 50 employees	8	7.7%
51 or more employees	0	0.0%
Industry:		
Business Services	11	10.5%
Food and Restaurant	9	8.6%
General Retail	14	13.3%
Health, Beauty and Fitness	14	13.3%
Automotive Repair	16	15.2%
Technology	6	5.7%
Transportation	2	1.9%
Construction	5	4.8%
Manufacturing	5	4.8%
Healthcare	10	9.5%
Other	13	12.4%
Credit Cards accepted:		
Yes	104	99.0%
No	1	1.0%
Use of chip reader:		
Yes	60	57.1%
No	45	42.9%
PCI-DSS compliant:		
Yes	37	35.2%
No	46	43.8%
Uncertain	22	21.0%

Data analysis was conducted on the sample of 105 VSEs. Table 16 provides the descriptive statistics of the RDB and CySR variables. For RDB, the mean score was 0.74 and standard deviation 0.17 which indicated that the samples of VSEs have low overall

owners perceived RDB. For CySR the mean score was 0.76 and standard deviation 0.13 which indicated that the overall CySR was low.

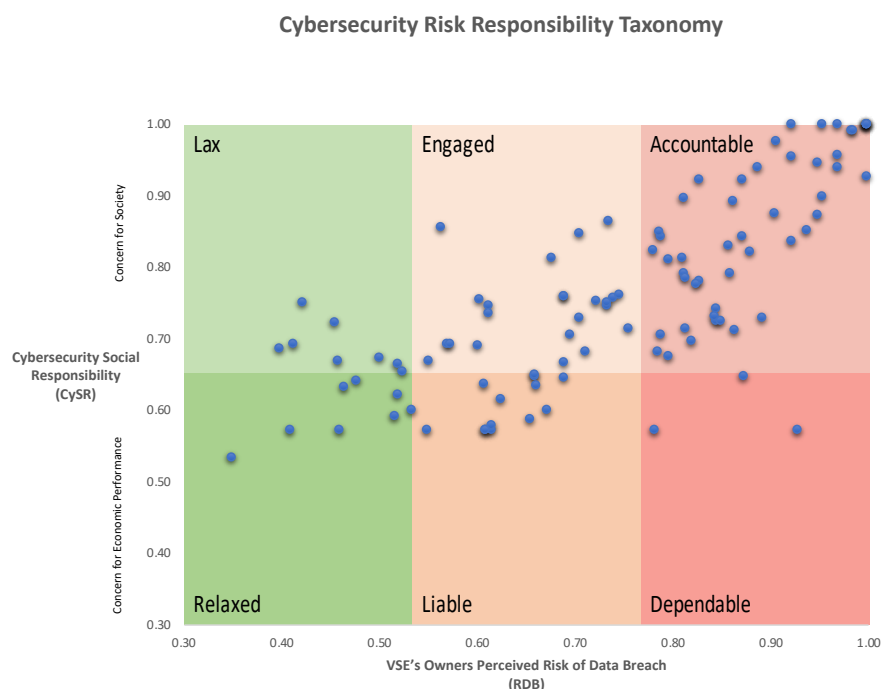
Table 16

Descriptive Statistics of RDB and CySR (N=105)

Variable	Minimum	Maximum	Mean	Std. Deviation
RDB	0.35	0.99	0.74	0.17
CySR	0.53	1.00	0.76	0.13

For RQ3, the aggregated scores of 105 VSEs for the measures CySR and RDB were positioned on the cybersecurity risk-responsibility taxonomy. Figure 5 shows the sample of VSEs positioned on the taxonomy with VSE's owners perceived RDB on the horizontal axis and CySR on the vertical axis.

Demographic data was collected on the VSEs to address RQ4a and RQ4b. The data was evaluated to determine if significant differences exist in VSEs owners' perceived RDB (RQ4a) and, CySR (RQ4b) based on three demographics: (1) type of industry, (2) implementation of EMV chip technology, (3) compliance with PCI-DSS? One-way ANOVA was used to address RQ4.

Figure 5*Cybersecurity Risk-Responsibility Taxonomy**Industry*

The descriptive statistics for RDB and CySR based on the type of industry is shown in Table 17 with the respective means and standard deviations. The top three highest VSE's owners perceived RDB were healthcare (Mean = 0.92, Standard Deviation 0.06); technology (Mean = 0.85, Standard Deviation 0.17); and transportation (Mean = 0.82, Standard Deviation = 0.05). Construction (Mean = 0.66, Standard Deviation = 0.12); food and restaurant industry (Mean = 0.69, Standard Deviation = 0.16); and those industries identifying as "other" (Mean = 0.67, Standard Deviation = 0.20) were the lowest VSEs owner's perceived RDB. For CySR the healthcare (mean = 0.92, Standard Deviation = 0.09); technology (Mean = 0.82 Standard Deviation = 0.18); and transportation (Mean = 0.79, Standard Deviation = 0.15) were the three highest for CySR,

while manufacturing (Mean = 0.70, Standard Deviation = 0.11); “other” (Mean = 0.70 Standard Deviation = 0.11); and construction (0.65, Standard Deviation = 0.06) were the industries with the lowest CySR. Figure 6 shows the cybersecurity risk-responsibility taxonomy by industry.

Table 17

Descriptive Statistics of RDB and CySR by Industry (N=105)

Industry	N	RDB		CySR	
		Mean	Std. Deviation	Mean	Std. Deviation
1. The Business Services Industry	11	0.75	0.14	0.78	0.15
2. The Food and Restaurant Industry	9	0.69	0.16	0.72	0.11
3. The General Retail Industry	14	0.72	0.20	0.77	0.12
4. The Health, Beauty and Fitness Industry	14	0.71	0.16	0.75	0.12
5. The Automotive Repair Industry	16	0.71	0.17	0.77	0.10
6. The Technology Industry	6	0.85	0.17	0.82	0.18
7. The Transportation industry	2	0.82	0.05	0.79	0.15
8. The Construction industry	5	0.66	0.12	0.65	0.06
9. The Manufacturing industry	5	0.77	0.11	0.70	0.11
10. The Healthcare industry	10	0.92	0.06	0.92	0.09
11. Other	13	0.67	0.20	0.70	0.13
Total	105	0.74	0.17	0.76	0.13

Figure 6

Cybersecurity Risk-Responsibility Taxonomy by Industry (N=105)

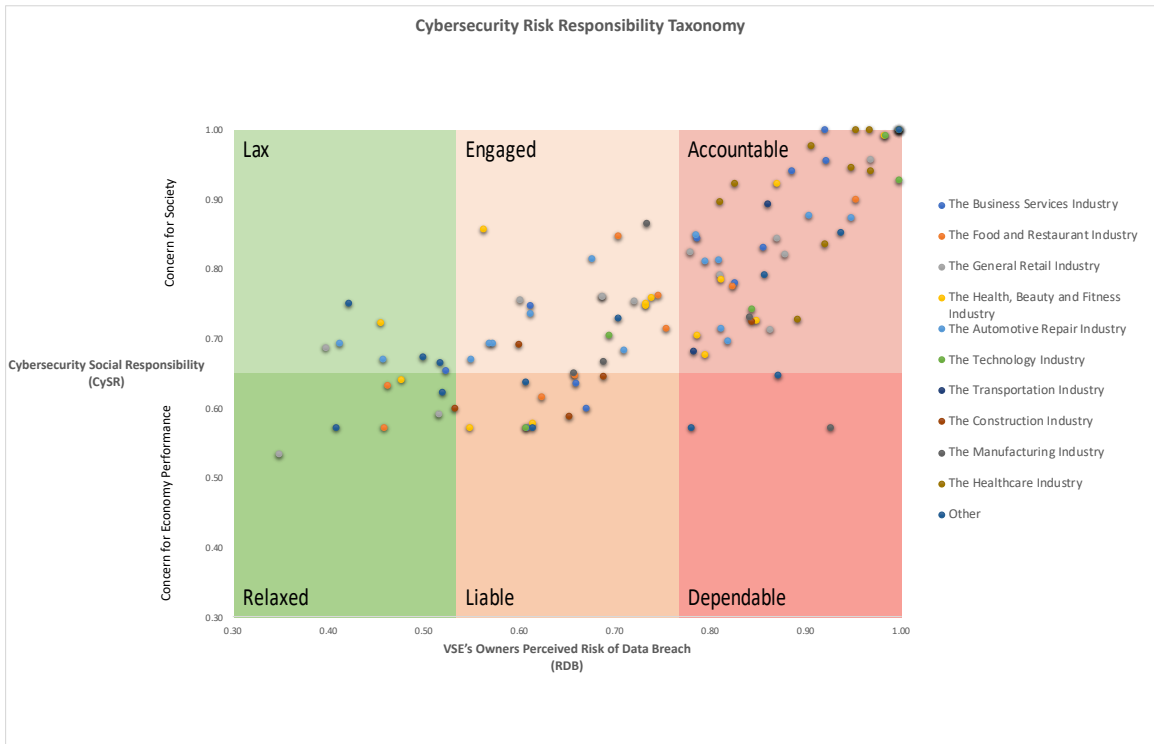


Figure 7

Means and Standard Deviations of RDB by Industry (N=105)

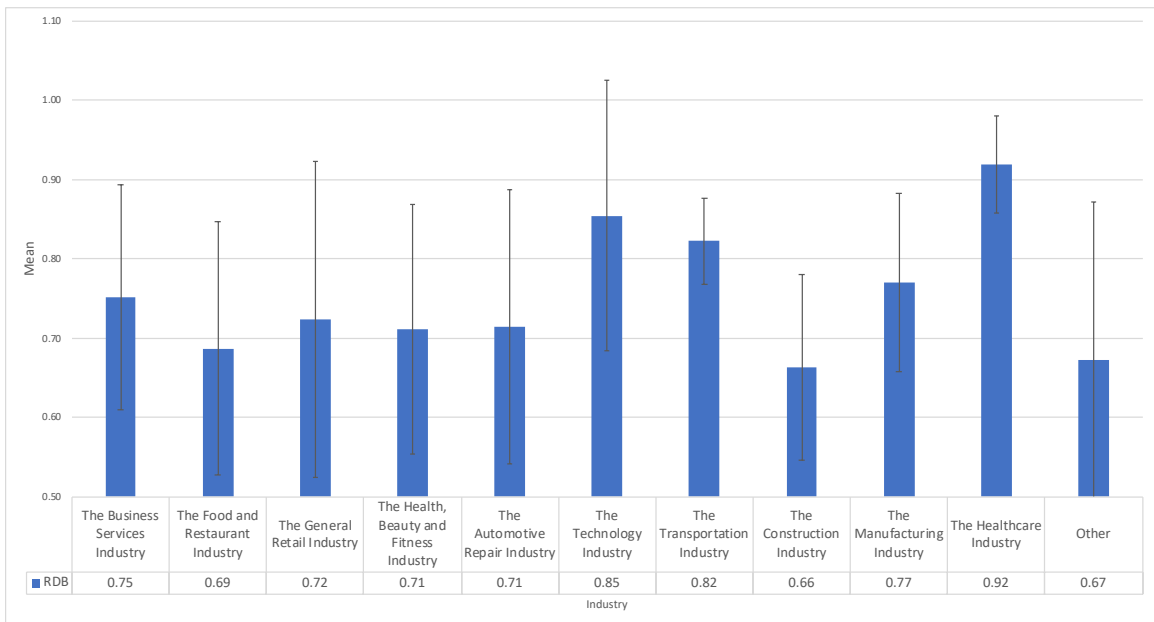
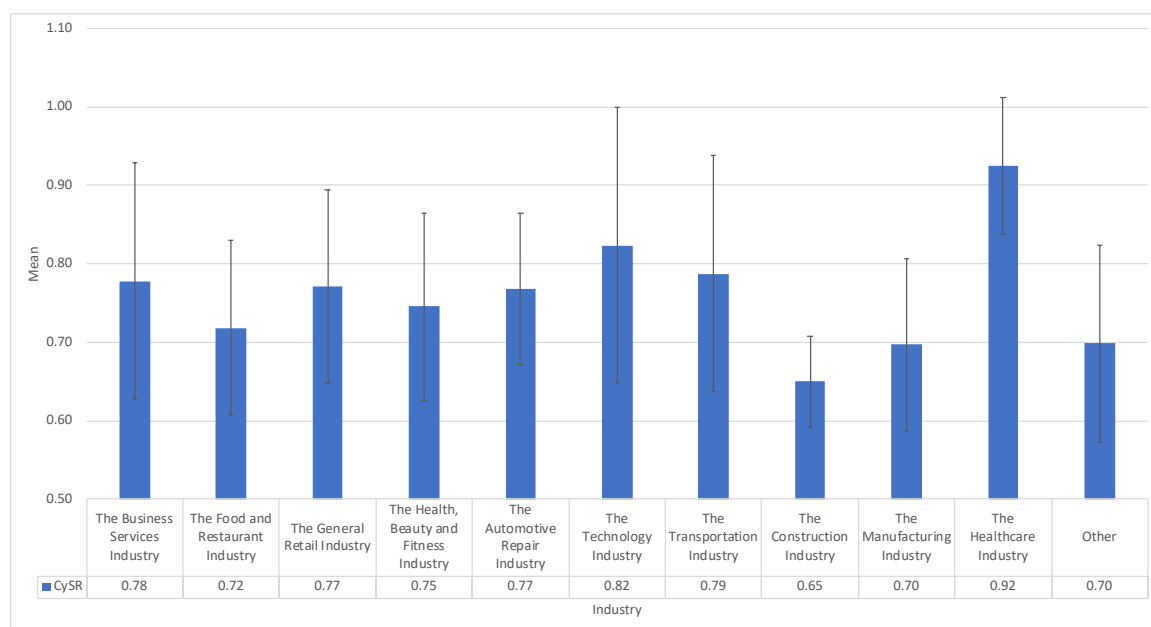


Figure 8

Means and Standard Deviations of CySR by Industry (N=105)



One-way ANOVA was used to determine whether there were significant differences between VSEs owners' perceived RDB and CySR based on their industry. Table 18 summarizes the results of the one-way ANOVA. For RDB the value of F is 2.13, which reaches significance with a p -value of 0.03 which is less than the 0.05 alpha level: $(F(10, 94) = 2.13, p = 0.03)$ and for CySR the value of F is 3.15, which reaches significance with a p -value < 0.001 which is less than the 0.05 alpha level: $(F(10, 94) = 3.15, p < 0.001)$. Figure 8 shows a graphical representation of the means and standard deviations of RDB and CySR by industry. There were significant differences in the one-way ANOVA for both VSEs owners' perceived RDB and CySR because the p -value of the F test were less than the 0.05 alpha level.

Table 18*ANOVA Results of Difference in RDB and CySR Based on Industry*

		Sum of Squares	df	Mean Square	F	Sig.
RDB	Between Groups	0.56	10	0.06	2.13	0.030*
	Within Groups	2.46	94	0.03		
	Total	3.02	104			
CySR	Between Groups	0.45	10	0.05	3.15	0.000***
	Within Groups	1.35	94	0.01		
	Total	1.80	104			

* $p < 0.05$; *** $p < 0.001$ *Use of EMV Chip Technology*

The descriptive statistics for RDB and CySR based on the use of EMV chip technology. The descriptive statistics for RDB and CySR based on the type of industry (Table 19) shows the use of EMV chip technology with the respective means and standard deviations. For RDB, VSEs who used EMV chip technology (Mean = 0.78, Standard Deviation = 0.17) while VSEs that did not use EMV chip technology (Mean = 0.71, Standard Deviation 0.16). For CySR, VSEs who used EMV chip technology (Mean = 0.79, Standard Deviation = 0.13) while VSEs that did not use EMV chip technology (Mean = 0.74, Standard Deviation 0.12). Figure 9 shows the cybersecurity risk-responsibility taxonomy by use of EMV chip technology. Figure 10 shows a graphical representation of the means and standard deviations for RDB while Figure 11 shows a graphical representation of the means and standard deviations for CySR by use of EMV chip technology.

Table 19

Descriptive Statistics of RDB and CySR by Use of EMV Chip Technology (N=105)

Use of EMV Chip Technology	N	RDB		CySR	
		Mean	Std. Deviation	Mean	Std. Deviation
1. Yes = Uses EMV Chip	45	0.78	0.17	0.79	0.13
2. No = Does not use EMV Chip	60	0.71	0.16	0.74	0.12
Total	105	0.74	0.17	0.76	0.13

Figure 9

Cybersecurity Risk-Responsibility Taxonomy by use of EMV Chip Technology (N=105)

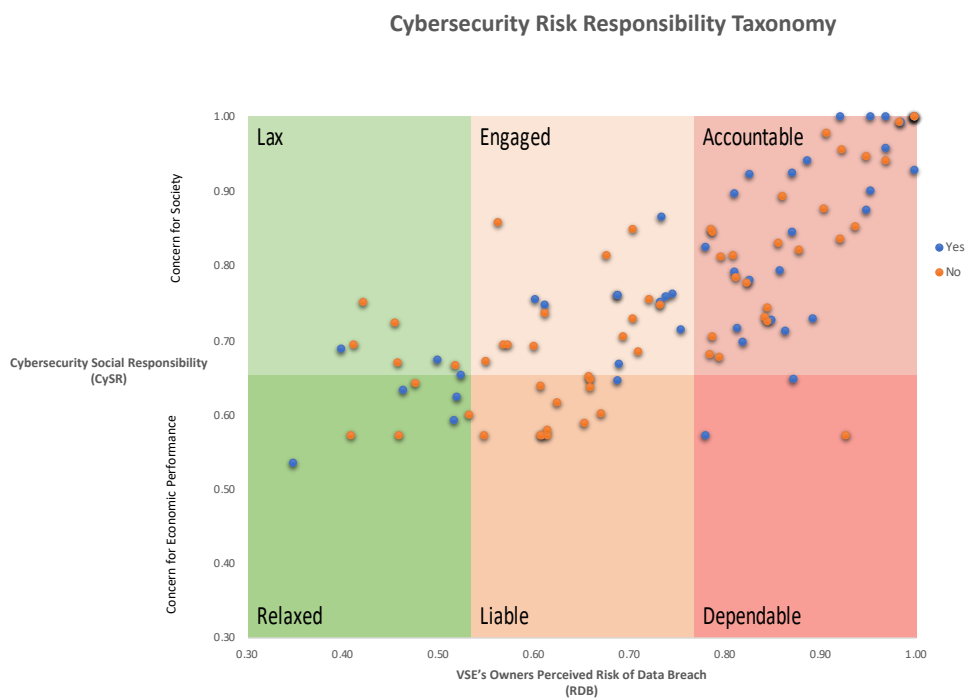
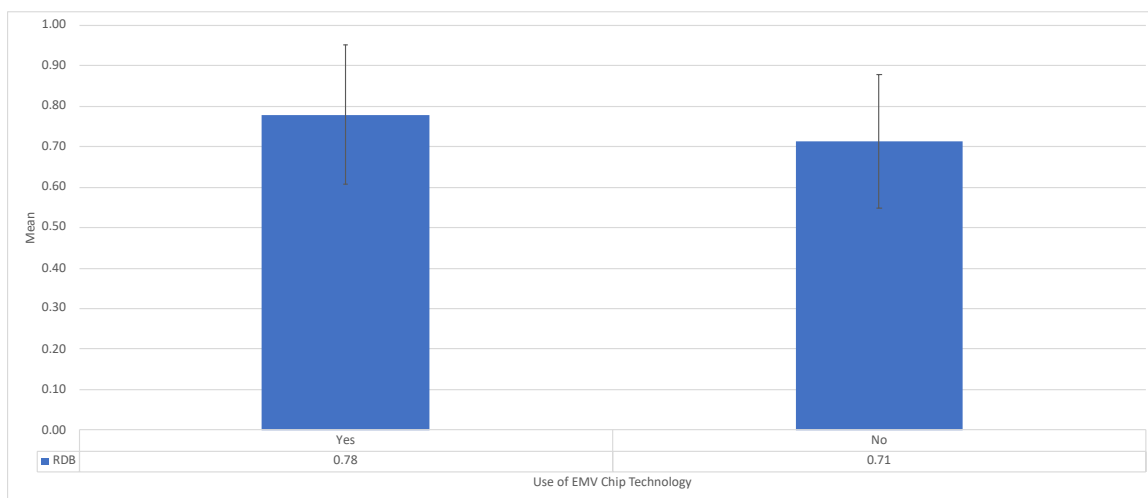
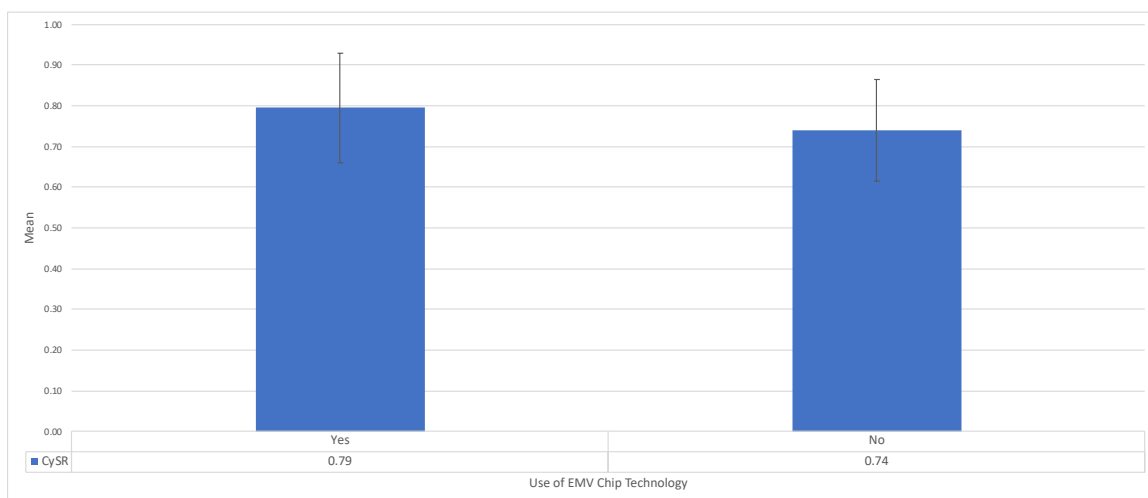


Figure 10

Means and Standard Deviations of RDB by use of EMV Chip Technology (N=105)

**Figure 11**

Means and Standard Deviations of CySR by use of EMV Chip Technology (N=105)



One-way ANOVA was used to determine whether there were significant differences between VSEs owners' perceived RDB and CySR based on their use of EMV chip technology. Table 20 summarizes the results of the one-way ANOVA. For RDB the value of F is 3.94, which reaches significance with a p -value of 0.05 which is equal to the 0.05 alpha level: $(F(1, 103) = 3.94, p = 0.03)$ and for CySR the value of F is 4.62, which

reaches significance with a p -value of 0.03 which is less than the 0.05 alpha level: ($F(1, 103) = 4.62, p = 0.03$). There were significant differences in the one-way ANOVA for both VSEs owners perceived RDB and CySR because the p -value of the F test were less than the or equal to 0.05 alpha level.

Table 20

ANOVA Results of Difference in RDB and CySR Based on use of EMV Chip Technology (N=105)

		Sum of Squares	df	Mean Square	F	Sig.
RDB	Between Groups	0.11	1	0.11	3.94	0.05
	Within Groups	2.91	103	0.03		
	Total	3.02	104			
CySR	Between Groups	0.08	1	0.08	4.62	0.03*
	Within Groups	1.72	103	0.02		
	Total	1.80	104			

* $p < 0.05$

PCI DSS Compliance

The descriptive statistics for RDB and CySR based on the PCI-DSS Compliance. The descriptive statistics for RDB and CySR (Table 21), shows the PCI-DSS compliance status of the VSEs with the respective means and standard deviations. For RDB, VSEs who obtained PCI-DSS compliance (Mean = 0.85, Standard Deviation = 0.14) while VSEs who did not obtain PCI-DSS compliance (Mean = 0.68, Standard Deviation 0.15) and, VSEs were uncertain of their PCI-DSS status (Mean = 0.69, Standard Deviation = 0.17). For CySR, VSEs who PCI-DSS compliant (Mean = 0.85, Standard Deviation = 0.13) while VSEs that did not use obtain PCI-DSS compliance (Mean = 0.71, Standard

Deviation 0.09) and, VSEs were uncertain of their PCI-DSS status (Mean = 0.73, Standard Deviation = 0.12). Figure 12 shows the cybersecurity risk-responsibility taxonomy by PCI-DSS compliance. Figure 13 shows a graphical representation of the means and standard deviations for RDB while figure 14 shows a graphical representation of the means and standard deviations for CySR by use PCI-DSS compliance.

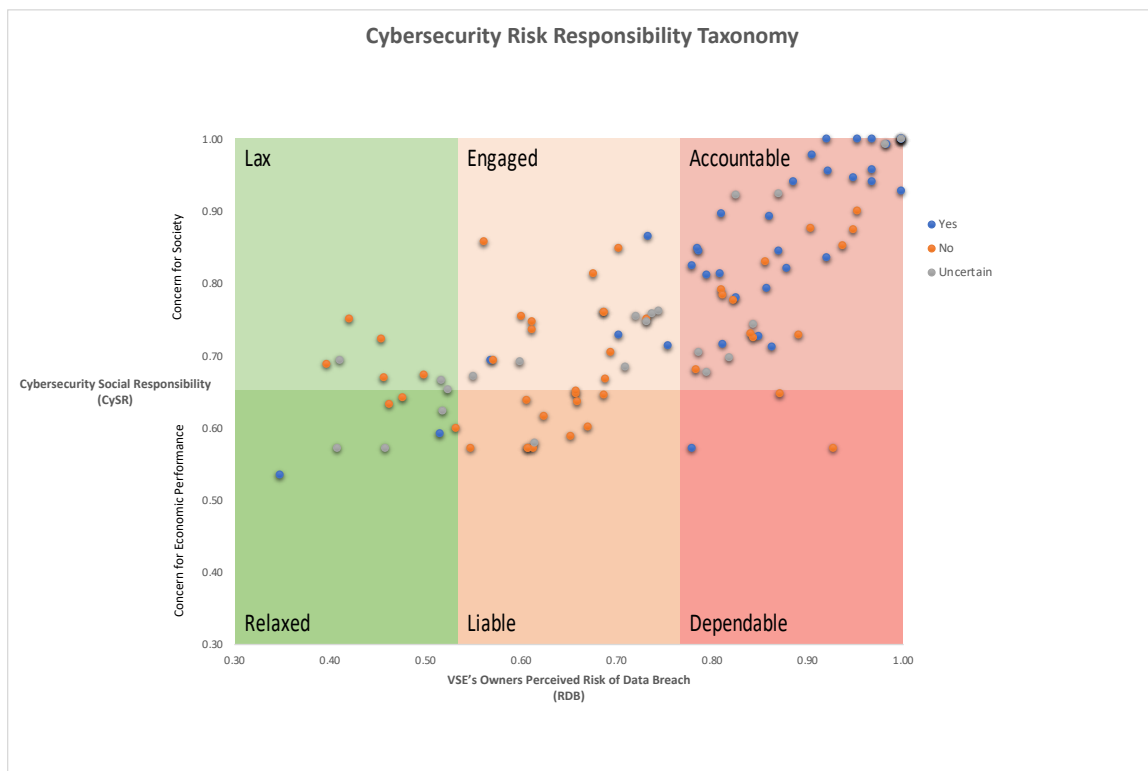
Table 21

Descriptive Statistics of RDB and CySR by PCI-DSS Compliance (N=105)

PCI-DSS Compliance	N	RDB		CySR	
		Mean	Std. Deviation	Mean	Std. Deviation
1. Yes	37	0.85	0.14	0.85	0.13
2. No	46	0.68	0.15	0.71	0.09
3. Uncertain	22	0.69	0.17	0.73	0.12
Total	105	0.74	0.17	0.76	0.13

Figure 12

Cybersecurity Risk-Responsibility Taxonomy by PCI-DSS Compliance

**Figure 13**

Means and Standard Deviations of RDB by PCI-DSS Compliance (N=105)

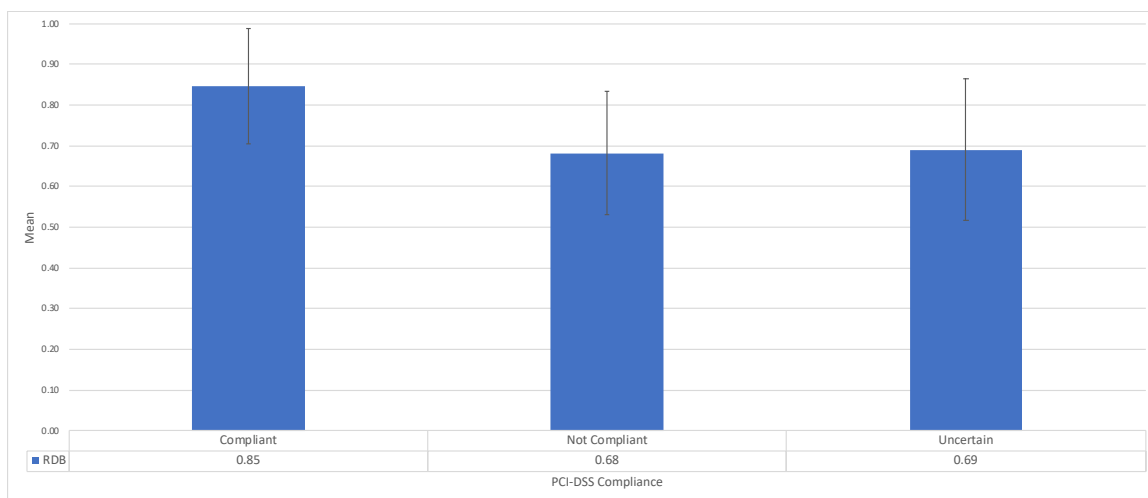
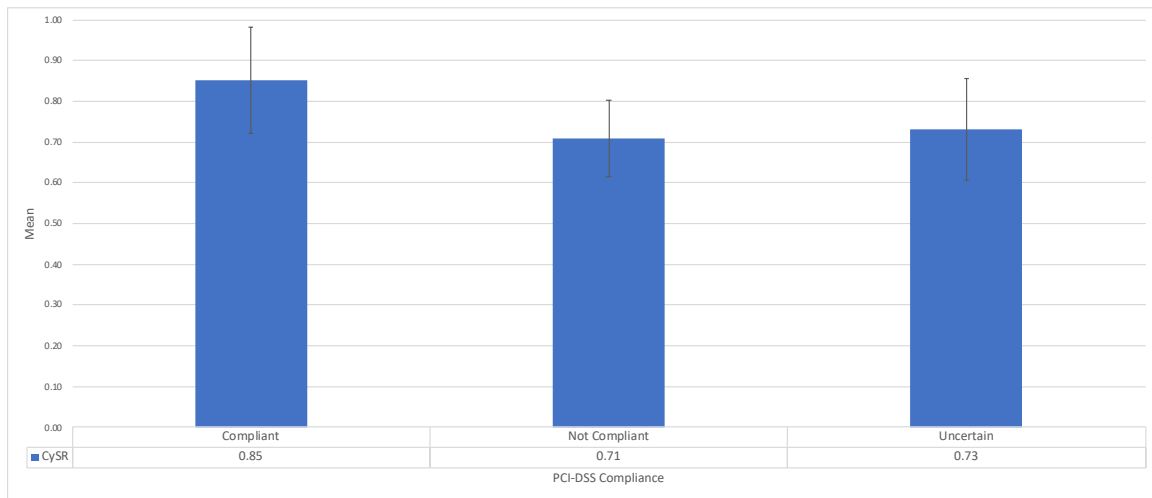


Figure 14

Means and Standard Deviations of CySR by PCI-DSS Compliance (N=105)



One-way ANOVA was used to determine whether there were significant differences between VSEs owners' perceived RDB and CySR based on their PCI-DSS compliance status. Table 20 summarizes the results of the one-way ANOVA. For RDB the value of F is 13.57, which reaches significance with a p -value < 0.001 which is less than the 0.05 alpha level: $(F(2, 102) = 13.57, p < 0.001)$ and for CySR the value of F is 17.23, which reaches significance with a p -value < 0.001 which is less than the 0.05 alpha level: $(F(2, 102) = 17.23, p < 0.001)$. There were significant differences in the one-way ANOVA for both VSEs owners perceived RDB and CySR because the p -value of the F test were less than the 0.05 alpha level.

Table 22*ANOVA Results of Difference in RDB and CySR Based on PCI-DSS Compliance**(N=105)*

		Sum of Squares	df	Mean Square	F	Sig.
RDB	Between Groups	0.63	2	0.32	13.57	0.000***
	Within Groups	2.38	102	0.02		
	Total	3.02	104			
CySR	Between Groups	0.45	2	0.23	17.23	0.000***
	Within Groups	1.34	102	0.01		
	Total	1.80	104			

*** $p < 0.001$ **Summary**

This chapter presented the results of this research study. Phase 1 of this study used SMEs to evaluate the characteristics for RDB and CySR. The original list of characteristics was finalized using the feedback from the SMEs. The SME validated instrument was used for the pilot data study (Phase 2), where a sample of 20 VSEs was used to further validate the survey instrument of the main study. The overall feedback from the pilot study did not warrant major changes to the survey instrument.

Phase 3 – the main data collection used the final instrument from the pilot study to collect data from 105 VSEs. Following the data collection, data screening was conducted to ensure accurate and reliable data was being used. The main data was subjected to exploratory factor analysis using principal component analysis to extract significant factors and further test reliability of the items and provide an answer to RQ2a and RQ2b: What will be the significant factors for VSEs owners' perceived RDB and CySR?

The results of the main data collection were presented to show how the

aggregated scores of the study participants for the measures RDB and CySR were positioned on the cybersecurity social risk-responsibility taxonomy. Further analysis was conducted to determine if industry, use of EMV chip technology and, PCI-DSS compliance resulted in a significant difference in VSEs owners perceived RDB and CySR. The result showed that there was a statistically significant difference in both RDB and CySR for industry, use of EMC Chip and, PCI-DSS compliance.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

This chapter provides the conclusions for the research that were derived from the results of the data analysis. A discussion of the implications, recommendations for future research, as well as limitations and a summary of the research study. Finally, a synopsis of the study is presented with a summary of the study's main goal and, research methodology along with the findings of the study and its contribution to IS systems security.

Conclusions

VSEs are especially exposed to data breaches because they tend to be less equipped to handle complex security issues due to a smaller structure and limited IS expertise (Berry & Berry, 2018; Cragg et al., 2011; Harris & Patten, 2014). While information systems security studies have been done on larger organizations, there is a lack of such research studies on VSEs (Gafni & Pavel, 2019). In addition, the role of responsibility in the IS research, in particular, security related research studies have not been thoroughly explored (Hovav & Gray, 2014). Furthermore, much of the research studies in the IS field center around computer security and not much on cybersecurity (O'Rourke, 2019). Given that cyber-attacks can be detrimental to VSEs, it is important that VSEs understand and address their inability to prevent cyber threats.

This research study was driven by the failure to prevent data breaches in VSEs. This study is built upon prior research on cybersecurity, IS security, IS systems risk and, CSR (Hovav & Gray, 2014). The main goal of this research was to develop and validate a cybersecurity risk-responsibility taxonomy for VSEs' owners' perceived CySR and RDB in order to classify their business level of exposure to a data breach. The goals of this research study were achieved by studying the relationship between CySR and RDB. A three-phased approach was used to achieve the four specific goals of this research study. Because CySR was being developed from the CSR theory, a set of measures for CySR did not exist and had to be developed. Similarly, a set of measures for perceived RDB needed to be developed as the first goal as this study. The items for both constructs were identified from a review of literature and presented to a panel of SMEs for review. The results of the expert panel review solidified the validity of the items that were being used for the survey instrument which was then used to conduct a pilot study for further validation.

The second goal of this research was to identify the factors for VSEs perceived RDB and CySR. The identification of the factors made it possible to determine the main categories for the RDB and CySR constructs in order to develop the aggregated scores for classification of the level of exposure to a data breach. The third goal of this research was to plot the aggregated scores of VSEs' owner's perceived CySR and RDB on the cybersecurity risk-responsibility taxonomy.

The cybersecurity risk-responsibility taxonomy classified VSEs in terms of their owners' perceived CySR, i.e. whether they display concern for society (high CySR) or concern for economic performance (low CySR), and their perceived risk of a potential

data breach (Low, Medium, & High). The overall results show that VSEs have a high CySR, as well as, a high RDB. According to the suggested implications of each cell in the cybersecurity risk-responsibility taxonomy, the first cell C1, consists of a low VSE's owner's perceived RDB and shows a concern for society. This cell is labeled 'lax' suggesting that the VSEs in this cell are oblivious to the potential of an RDB. The second cell C2, consists of a low VSE's owners' perceived RDB and shows concern for economic performance. This cell is labeled 'relaxed', suggesting that the VSEs in this cell are not strict in safeguarding against a data breach. The third cell C3 is labeled 'engaged', with a medium VSE's owners' perceived RDB and shows concern for society. VSEs in this cell participate in activities that put them at medium RDB. The fourth cell C4, consists of a medium VSE's owners' perceived RDB and demonstrates a concern for economic performance. This cell is labeled 'liable', suggesting that there may be a likely RDB. The fifth cell C5, demonstrates a high VSE's owner's perceived RDB demonstrates a concern for society. This cell has been labeled 'accountable', suggesting that VSEs in this cell demonstrate ethical awareness and are considered accountable. The sixth cell C6, represents VSEs that are at high owner's perceived RDB and demonstrates concern for economic performance. This cell is labeled 'dependable', suggesting that while responsibility focus is geared toward economic performance, VSEs in this cell are still aware of the importance of securing against data breaches.

The fourth goal of this study was to assess whether significant differences exist in VSEs' owners' perceived CySR and RDB based on type of industry, implementation of EMV chip technology, and compliance with PCI-DSS. The results of this assessment indicated whether there was a statistically significant difference in both RDB and CySR

for industry, use of EMC Chip and, PCI-DSS compliance. This finding implies a statistical difference in RDB and CySR based on industry. This is most likely due to the nature of the business, the type of data collected and, existing standards and regulations that govern them. For example, the healthcare industry was the highest for RDB. Healthcare providers such as doctors' offices are required by law to protect the storage and transmission of sensitive data. The VSEs identifying as being in the technology industry were also among the highest RDB and CySR. A reasonable assumption is that technology companies have a high perceived RDB and CySR because of the expertise of their staff and the services they provide to their wider community. The lowest RDB were the construction, food and restaurant and companies identifying as "other" industries. Restaurants widely use swipe and signature type terminals which are frequently targeted by cyber criminals.

There was also a difference in RDB and CySR for the use of EMV chip technology and PCI-DSS compliance. The EMV chip technology is considered a more secure way to use credit cards and can help to reduce data breaches. In addition, companies that engage in the use of EMV chip technology see that as a way to prevent such breaches and, though not required to do so, are engaging in civic responsibility showing concern for society. Similarly, PCI-DSS compliance, though not mandated is deemed a way of mitigating these risks, as a result, companies that have obtained this compliance are already taking these risks seriously. The threat of having customers' payment card data stolen is real, but it can be reduced by adhering to PCI-DSS (Raghavan et al. 2017).

Limitations were noted with this study. The first limitation is the method used to

solicit participation in the study. The organizations were sent an email inviting them to participate in the study with a clickable link to the survey. This email could have been viewed by some VSEs owners as spam or phishing. This led to a small number of participants in the study which can impact the generalizability of the findings. Another limitation was the size of the survey instrument and the time it would take to complete the survey. Without prior knowledge of the study, it is unlikely that VSEs owners would willingly participate in a survey which they were unaware of.

Implications

This research study has some implications for the existing body of knowledge in the area of cybersecurity and corporate social responsibility. This study raises awareness of cybersecurity among VSEs. A contribution to practice was the development of the survey instrument which can be used by VSEs to determine their level of preparedness for cybersecurity. Another implication of this study is that the results and conclusions may assist organizations in understanding and mitigating a cybersecurity data breach.

The theoretical implications of this study include the cybersecurity risk-responsibility taxonomy which can be used to further compare and provide insight on VSEs CySR and perceived RDB. This study further contributes to the body of knowledge by introducing CSR to IS studies which further facilitates discussion on the social factors influencing the cybersecurity position of small enterprises.

Recommendations and Future Research

Future studies are necessary to improve the validity of the CySR instrument. First, the number of SMEs who participated in the expert panel review of the study could be increased to include more SMEs outside of government and academia, specifically,

industry experts with insight on small business operations should be targeted for inclusion on the SME panel. Second, an increase in the sample size of the study population to improve both validity and generalizability of the findings. Third, the study could be replicated with additional demographic markers such as, having an online storefront, number of years in business and average age of the business owner. By adding additional demographic markers, further discussion and analysis of factors influencing CySR and RDB for research and practice. Fourth, the validated factors for RDB were consistent with what was proposed, however, CySR had to be modified. This is likely due to CySR being developed from CSR which has had different classifications over the years. Therefore, additional research could be carried out to identify additional factors for CySR.

Summary

This study developed a classification methodology to classify VSEs based on their perceived CySR as well as RDB. Factors for VSEs RDB and CySR were identified in order to obtain the aggregated scores for the cybersecurity risk-responsibility taxonomy. The cybersecurity risk-responsibility taxonomy was developed from a sample of 105 VSEs to classify them in terms of their owners' perceived CySR and perceived RDB.

In order to develop a reliable and valid method of measuring the VSEs owners perceived RDB and CySR, this study was conducted in three phases. Phase 1 of the study used SMEs to identify the characteristics for RDB and CySR via the Delphi method. Thirteen SMEs from academia, government and industry participated in the development

of the RDB and CySR items for the study. This process was necessary because measures didn't exist for RDB and CySR. Phase 2 involved a pilot test with a small sample of the population. A total of 20 VSEs participated in the pilot study which further validated the instrument. The results of the pilot study did not warrant major additional changes to the survey instrument which was used for the main data collection.

The final phase (Phase 3) involved the data analysis, taxonomy development testing of the hypotheses. The collected data was subjected to screening to identify factors for RDB and CySR. Upon completion of the data analysis for RDB, external risk from cyber criminals, internal risk from users and, physical risk from outsiders were the resulting factors. Whereas the data analysis for CySR resulted in two factors; business responsibility and legal responsibility. Data aggregations showed that scores of 105 VSEs were positioned in all 6 cells of the cybersecurity risk-responsibility taxonomy. The majority of the scores were on the high end of VSEs owners perceived CySR which indicated that VSEs in general showed concern for society. For perceived RDB the responses were spread throughout low medium and high, however, the majority of VSEs were in the high range, a moderate amount in the medium range and, a small amount on the low end.

During the study, further analysis was performed to determine if significant differences exist in VSEs owners' perceived RDB and CySR based on three demographics: (1) type of industry, (2) implementation of EMV chip technology, (3) compliance with PCI-DSS. The results of this analysis showed that there were considerable differences in both RDB and CySR for industry, use of EMC Chip and, PCI-DSS compliance.

In summary, this research addressed the failure to prevent data breaches in VSEs who are at risk because they do not understand cybersecurity, or they do not have experts on hand to help safeguard their computer systems. The findings of this research suggest that different business industries have a higher perceived risk of a cybersecurity data breach. In particular, those industries such as healthcare are generally forced to protect the storage and transmission of sensitive data. VSEs in generally demonstrate a high level of cybersecurity social responsibility, showing concern for the society, despite their perception of a risk of a cybersecurity data breach. In conclusion, VSEs need to be more aware of the risks associated with a cybersecurity data breach and, the impact such a risk places on the wider society. Because VSEs demonstrate a concern for society, such awareness would encourage decision makers to utilize the necessary practices to ensure safety of their computer systems and help to mitigate cybersecurity data breaches.

Appendix A

Dear IT/IS Expert,

My name is Keiona Davis and I am a doctoral candidate at the College of Engineering and Computing, Nova Southeastern University (NSU). I am currently working under the supervision of Dr. Yair Levy, Professor of IS and Cybersecurity on a dissertation entitled “Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach.” The main goal of this proposed research is to develop and validate a cybersecurity risk-responsibility taxonomy for VSEs’ cybersecurity social responsibility (CySR) and risk of data breach (RDB).

I would like to request your assistance in providing feedback as a subject matter expert for my upcoming doctoral research study. Please review the preliminary survey instrument attached to this email and complete the quantitative and qualitative evaluation form using the link below. Your input will shape the final instrument for this proposed study.

Best Regards,

Keiona Davis, Ph.D. Candidate

College of Engineering and Computing

Nova Southeastern University

Appendix B

Section 1: Proposed factors and characteristics

The items in Section 1 are related to the proposed factors and characteristics for Risk of Data Breach and Cybersecurity Social Responsibility. Please evaluate and provide feedback on the list of characteristics in the tables below.

Risk of Data Breach Factors and Characteristics

Proposed Risk of Data Breach (RDB) Factors	Proposed Risk of Data Breach (RDB) Characteristics
External Risk from Cybercriminals	<ul style="list-style-type: none"> A1. Lack of firewall software A2. Lack of intrusion detection systems A3. Lack of a password strength policy A4. Unencrypted transmission of cardholder data A5. Lack of security awareness to social engineering and phishing A6. Lack of malware protection
Internal Risk from Users (Such as disgruntled employees or human error/mistake)	<ul style="list-style-type: none"> A7. Lack of user knowledge or training A8. Improper access permission (e.g. employees having unnecessary privilege) A9. Improper access to software A10. Lack of separation of duties A11. Weak encryption or poor key-management practices
Risk of Physical Intruder/Thief	<ul style="list-style-type: none"> A12. Lack of physical monitoring A13. Insecure handling of payment terminals A14. Disposal of storage media with data A15. Unsupervised visitors such as vendors

Cybersecurity Social Responsibility Factors and Characteristics

Proposed Cybersecurity Social Responsibility (CySR) Factors	Proposed Cybersecurity Social Responsibility (CySR) Characteristics
Economic CySR	<p>B1. The organization is successful at maximizing profits</p> <p>B2. The organization strives to lower operating costs</p> <p>B3. Owners/managers try to establish long-term strategies for the organization</p>
Legal CySR	<p>B4. Owners/managers are aware of cybersecurity laws</p> <p>B5. Software products meet legal standards</p> <p>B6. Owners/Managers try to comply with the law</p>
Ethical CySR	<p>B7. The organization has a comprehensive information security policy</p> <p>B8. The organization follows information security standards</p> <p>B9. The organization is recognized as a trustworthy company</p> <p>B10. A procedure is in place for employees to report misconduct or misuse of information systems</p>
Discretionary CySR	<p>B11. The organization tries to improve its corporate image</p> <p>B12. The organization tries to improve the perception of how it conducts business</p> <p>B13. The organization contributes to the bettering of the local community</p>

Expert Panel Evaluation for Risk of Data Breach Characteristics

In the section below, please provide your expert opinion about the list of characteristics for Risk of Data Breach by very small companies. For each of the proposed characteristics below, please select one of the three options:

1. Keep - the proposed characteristic should be included as is.
2. Adjust- the characteristic should be included but with modifications (Please provide your feedback below on the exact modifications at the short text field at the end of the list of characteristics in question A21).
3. Remove - the proposed characteristic should NOT be included (Please recommend reasons below on why not, and propose a replacement if possible at the end of the list of characteristics in question A22)

If you feel there are characteristics not covered here that should be included, please include them in “Additional characteristics to be included” below.

Please provide a recommendation for each of the proposed Risk of Data Breach characteristics (As) below.

	Keep	Adjust	Remove
A1. Lack of firewall software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A2. Lack of intrusion detection systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A3. Lack of a password strength policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A4. Unencrypted transmission of cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A5. Lack of security awareness to social engineering and phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A6. Lack of malware protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A7. Lack of user knowledge or training	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A8. Improper access permission (e.g. employees having unnecessary privilege)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A9. Improper access to software	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A10. Lack of separation of duties	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A11. Weak encryption or poor key-management practices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A12. Lack of physical monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A13. Insecure handling of payment terminals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A14. Disposal of storage media with data

A15. Unsupervised visitors such as vendors

A21. Please provide adjustments that you see fit to the proposed Risk of Data Breach characteristics listed above (A1 to A15):

A22. Please provide additional characteristics that you see fit to be included for Risk of Data Breach beyond those listed above:

Expert Panel Evaluation for Cybersecurity Social Responsibility Characteristics

In the section below, please provide your expert opinion about the list of characteristics for Cybersecurity Social Responsibility by very small companies. For each of the proposed characteristics

below, please select one of the three options:

1. Keep - the proposed characteristic should be included as is.
2. Adjust- the characteristic should be included but with modifications (Please provide your feedback below on the exact modifications at the short text field at the end of the list of characteristics in question B21).
3. Remove - the proposed characteristic should NOT be included (Please recommend reasons below on why not, and propose a replacement if possible at the end of the list of characteristics in question B22)

If you feel there are characteristics not covered here that should be included, please include them in “Additional characteristics to be included” below.

In the section below, please provide your expert opinion about the list of characteristics for Cybersecurity Social Responsibility.

For each of the proposed characteristics below, please select one of the three options:

1. Keep - the proposed characteristic should be included
2. Adjust- the characteristic should be included but with modifications. Please include feedback for any topics under the “Adjustment to proposed characteristics” short text field below.
3. Remove - the proposed characteristic should NOT be included

If you feel there are characteristics not covered here that should be included, please include them in “Additional characteristics to be included” below.

Please provide a recommendation for each of the proposed Cybersecurity Social Responsibility characteristics below.

	Keep	Adjust	Remove
B1. The organization is successful at maximizing profits	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B2. The organization strives to lower operating costs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B3. Owners/managers try to establish long-term strategies for the organization	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B4. Owners/managers are aware of cybersecurity laws	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B5. Software products meet legal standards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B6. Owners/Managers try to comply with the law	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B7. The organization has a comprehensive information security policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B8. The organization follows information security standards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B9. The organization is recognized as a trustworthy company	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B10. A procedure is in place for employees to report misconduct or misuse of information systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B11. The organization tries to improve its corporate image	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B12. The organization tries to improve the perception of how it conducts business	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
B13. The organization contributes to the bettering of the local community	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B21. Please provide adjustments that you see fit to the proposed Risk of Data Breach characteristics listed above (B1 to B13):

B22. Please provide additional characteristics that you see fit to be included for Risk of Data Breach beyond those listed above:

Appendix C

Proposed survey instrument

A. Risk of Data Breach

External Risk from Cybercriminals (ERCC)

Below you will find a set of characteristics related to external risk from cyber criminals at your organization. Please rate each on a scale from 1 to 3.

	No, and not considered (1)	No, but considered (2)	Yes (3)
A1. My organization has firewall software installed on computers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A2. My organization utilizes an intrusion detection system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A3. My organization has a password strength policy	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A4. My organization ensures encrypted transmission of cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A5. My organization is aware of social engineering and phishing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A6. My organization uses malware protection	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Internal risk from users such as disgruntled employees (IRU).

Below you will find a set of characteristics related to internal risk from users at your organization. Please rate each on a scale from 1 to 7.

	Strongly disagree	Disagree	Somewhat disagree	Neither agree or disagree	Somewhat agree	Agree	Strongly agree
	(1)	(2)	(3)	(4)	(5)	(6)	(7)
A7. My organization conducts training on internal cyber risk	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A8. Each employee only has access or permission to computers necessary to carry out his/her work on a need to know basis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A9. Each employee has access only to specific modules or files in the computer system to carry out his/her work	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A10. My organization has a clearly defined separation of duties for each employee	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A11. My organization uses strong password encryption practices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

External risk from a physical intruder or thief (PIT)

Below you will find a set of characteristics related to external risk from a physical

intruder or thief at your organization. Please rate each on a scale from 1 to 3.

	No, and not considered (1)	No, but considered (2)	Yes (3)
A12. My organization has security cameras for physical monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A13. Only employees can access payment terminals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A14. My organization wipes all data from storage media before disposal	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
A15. Visits from vendors are always supervised	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

B12. My organization is
recognized as a trustworthy
company

B13. My organization has a
procedure in place for employees
to report misconduct or misuse
of information systems

Appendix D



MEMORANDUM

To: **Keiona Davis**

From: **Ling Wang, Ph.D.,
Center Representative, Institutional Review Board**

Date: **February 8, 2019**

Re: **IRB #: 2019-84; Title, "Cybersecurity Risk-Responsibility Taxonomy: The Role of
Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

Appendix D

Survey for Participants

Survey - The Role of Cybersecurity Social Responsibility in Small Enterprises on Risk of Data Breach

Dear Business Owner/manager

My name is Keiona Davis and I am a doctoral candidate at the College of Engineering and Computing, Nova Southeastern University (NSU). I am currently working under the supervision of Dr. Yair Levy, Professor of IS and Cybersecurity on a dissertation entitled "Cybersecurity Risk-Responsibility Taxonomy: The Role of Cybersecurity Social Responsibility in Small Enterprises (SEs) on Risk of Data Breach."

Why are you asking me to be in this research study?

You are being asked to take part in this research study because your company has been identified as a small enterprise accepting credit card payments.

Why is this research being done?

The purpose of this study is to develop and validate a cybersecurity risk-responsibility taxonomy for SEs' cybersecurity social responsibility (CySR) and risk of data breach (RDB).

What will I be doing if I agree to be in this research study?

You will be taking a one-time, anonymous survey. The survey will take approximately 10 minutes to complete. This research study involves minimal risk to you.

Are there possible risks and discomforts to me?

To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

Will it cost me anything? Will I get paid for being in the study?

There is no cost for participation in this study. Participation is voluntary and no payment will be provided.

How will you keep my information private?

Your responses are anonymous. Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law. You will not be required to provide any identifiable information about your organization. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any granting agencies (if applicable). All confidential data will be kept securely on google forms. All data will be kept for 36 months from the end of the study and destroyed after that time by deleting all data collected.

Who can I talk to about the study?

If you have questions, you can contact me at 954-990-3830 or my advisor Dr. Levy at levyy@nova.edu. Additionally, if you have read the above information and voluntarily wish to participate in this research study, please click next to continue.

If you have questions about the study but want to talk to someone else who is not a part of the study, you can call the Nova Southeastern University Institutional Review Board (IRB) at (954) 262-5369 or toll free at 1-866-499-0790 or email at IRB@nova.edu.

Do you understand and do you want to be in the study?

You can decide not to participate in this research and it will not be held against you. You can exit the survey at any time.

If you have read the above information and voluntarily wish to participate in this research study, please click NEXT below.

Best Regards,

C. About your organization

Below please answer the following questions about your organization

5. My organization has *

Mark only one oval.

- Less than 5 employees
- 6 to 10 employees
- 11 to 20 employees
- 21 to 30 employees
- 31 to 50 employees
- 51 or more employees

6. My organization is a part of *

Mark only one oval.

- The Business Services Industry
- The Food and Restaurant Industry
- The General Retail Industry
- The Health, Beauty and Fitness Industry
- The Automotive Repair Industry
- The Technology Industry
- The Transportation industry
- The Construction industry
- The Manufacturing industry
- The Healthcare industry
- Other

7. My organization conducts credit cards transactions *

Mark only one oval.

- Yes
- No

8. My organization uses a chip compatible card reader for credit card transactions *

Mark only one oval.

- Yes
- No

9. My organization has obtained PCI-DSS Compliance (PCI-DSS is a set of information security standards merchants must meet in order to allow their customers to make credit card purchases.) *

Mark only one oval.

- Yes
- No
- Uncertain

This content is neither created nor endorsed by Google.

Google Forms

References

- Andrews, M., & Whittaker, J. A. (2004). Computer security. *IEEE Security & Privacy*, 2(5), 68-71.
- Aras, G., Aybars, A., & Kutlu, O. (2010). Managing corporate performance: Investigating the relationship between corporate social responsibility and financial performance in emerging markets. *International Journal of Productivity and Performance management*, 59(3), 229-254.
- Aupperle, K. E., Carroll, A. B., & Hatfield, J. D. (1985). An empirical examination of the relationship between corporate social responsibility and profitability. *Academy of Management Journal*, 28(2), 446-463.
- Axelrod, C. W. (2006). Cyber security and the critical infrastructure. *Information Systems Control Journal*, 3, 24-28.
- Banjo, S. (2014, September 2). Home depot investigating possible payment card data breach. *The Wall Street Journal*. <http://www.online.wsj.com/>
- Barrett, D. (2019, July 29). Capital One says data breach affected 100 million credit card applications. *The Washington Post*. https://www.washingtonpost.com/national-security/capital-one-data-breach-compromises-tens-of-millions-of-credit-card-applications-fbi-says/2019/07/29/72114cc2-b243-11e9-8f6c-7828e68cb15f_story.html
- Baskerville, R., Rowe, F., & Wolff, F. C. (2018). Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 49(1), 33-52.
- Berr, J. (2014). A fast-growing threat to small business: Hackers. *CNBC*. <http://www.cnn.com/2014/09/08/hackers-target-small-biz-are-you-prepared.html>
- Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security*, 19(5), 300-312.
- Blank, R., & Gallagher, P. (2012). NIST-National Institute of Standards and Technology: Guide for Conducting Risk Assessments. *US Department of Commerce*.
- Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: a state-of-the-art assessment. *MIS Quarterly*, 1-16.
- Bowen, H. R. (1953). *Social Responsibility of the Businessman*. Harper and Row.
- Broadcom. (2019). *Internet security threat report*. <https://docs.broadcom.com/doc/istr-23-2018-en>
- Carlton, M., & Levy, Y. (2017). Cybersecurity skills: The cornerstone of advanced

- persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, 5(2), 16-28.
- Carroll, A. B. (1979). A three-dimensional conceptual model of corporate performance. *Academy of management review*, 4(4), 497-505.
- Carroll, A. B. (2004). Managing ethically with global stakeholders: A present and future challenge. *The Academy of Management Executive*, 18(2), 114-120.
- Carroll, A. B., & Shabana, K. M. (2010). The business case for corporate social responsibility: a review of concepts, research and practice. *International Journal of Management Reviews*, 12(1), 85-105.
- Chopra, A., & Chaudhary, M. (2020). The need for information security. *In Implementing an Information Security Management System* (pp. 1-20). Apress, Berkeley, CA. https://doi-org.ezproxylocal.library.nova.edu/10.1007/978-1-4842-5413-4_1
- Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, 30(8), 719-731.
- Choo, K-K. R., & Smith, R. G. (2008). Criminal exploitation of online systems by organized crime groups. *Asian Journal of Criminology*, 3(1), 37-59.
- Clearinghouse, P. R. (2019). *Data breaches*. <https://www.privacyrights.org/data-breaches>.
- Coburn, A. (2010). Fitting PCI DSS within a wider governance framework. *Computer Fraud & Security*, 2010(9), 11-13.
- Commission, E. (2016). User guide to the SME Definition. http://ec.europa.eu/regional_policy/sources/conferences/state-aid/sme/smedefinitionguide_en.pdf
- Conner, C. (2013). Are you prepared? record number of cyber attacks target small business. *Forbes*. <http://www.forbes.com/sites/cherylsnappconner/2013/09/14/are-you-prepared-71-of-cyber-attacks-hit-small-business/2/>
- Cragg, P., Caldeira, M., & Ward, J. (2011). Organizational information systems competences in small and medium-sized enterprises. *Information & Management*, 48(8), 353-363.
- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10), 13-21.
- Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525-554.
- Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating*

quantitative and qualitative research. Prentice Hall.

- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4 ed.). Sage Publications.
- Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the choicepoint and TJX data breaches. *MIS Quarterly*, 33(4), 673-687.
- Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11(2), 127-153.
- DOD. (2017). *DOD dictionary of military and associated terms*. http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.
- Earl, M., & Feeney, D. (2012). How to be a CEO for the information age. *Sloan Management Review*.
- ENISA. (2016). *Guidelines for SMEs on the security of personal data processing*. European Union Agency for Cybersecurity. <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>.
- Fassin, Y., Van Rossem, A., & Buelens, M. (2011). Small-Business owner-managers' perceptions of business ethics and CSR-related concepts. *Journal of Business Ethics*, 98(3), 425-453.
- Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information security risk management: In which security solutions is it worth investing. *Communications of the Association for Information Systems*, 28(1), 329-356.
- Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, 7(1), 14-26.
- Galbreth, M. R., & Shor, M. (2010). The impact of malicious agents on the enterprise software industry. *MIS Quarterly*, 34(3), 595-612.
- Geva, A. (2008). Three models of corporate social responsibility: Interrelationships between theory, research, and practice. *Business and Society Review*, 113(1), 1-41.
- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2014). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, 6(01), 24.

- Gray, D., & Ladig, J. (2015). The implementation of EMV chip card technology to improve cyber security accelerates in the US following target corporation's data breach. *International Journal of Business Administration*, 6(2), p60.
- Groner, R., & Brune, P. (2012). Towards an empirical examination of IT security infrastructures in SME *Secure IT Systems* (pp. 73-88): Springer.
- Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, 13(4), 297-310.
- Harris, M. A., & Patten, K. P. (2014). Mobile device security considerations for small- and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97-114.
- Holzer, A., & Junglas, I. (2013). Toward JUSTIS - a research program aimed at fostering business ethics by empowering stakeholders through information systems. *Communications of the Association for Information Systems*, 33(24), 407-422.
- Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Association for Information Systems*, 34(50), 893-912.
- Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615-660.
- Hui, K.-L., Hui, W., & Yue, W. T. (2012). Information security outsourcing with system interdependency and mandatory security requirement. *Journal of Management Information Systems*, 29(3), 117-156.
- Ilvonen, I., & Virtanen, P. (2013). *Preparing for cyber threats in companies with information security policies. Proceedings of the European Conference on Information Warfare and Security*.
- ISO. (2009). Risk management — Principles and guidelines. <https://www.iso.org/obp/ui/-iso:std:iso:31000:ed-1:v1:en>
- Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.
- Julisch, K. (2013). Understanding and overcoming cyber security anti-patterns. *Computer Networks*, 57(10), 2206-2211.
- Kauffman, R. J., Lee, Y. J., Prosch, M., & Steinbart, P. J. (2011). A survey of consumer information privacy from the accounting information systems perspective. *Journal of Information Systems*, 25(2), 47-79.

- Kaur, K. (2016). Information Security Management of an organization with a focus on Human perspective. *International Journal of Computer Techniques*, 3(2), 201-204.
- Ko, M., & Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management*, 17(2), 13-22.
- Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review*, 103(3).
- Lee, M.-C. (2014). Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method. *International Journal of Computer Science & Information Technology*, 6(1), 29-45.
- Levy, Y. (2006). *Assessing the value of e-learning systems*. Idea Group Publishing.
- Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173-186.
- Lorenzo-Molo, C. F., & Udani, Z. A. S. (2013). Bringing back the essence of the “S” and “R” to CSR: Understanding the limitations of the merchant trade and the white man’s burden. *Journal of Business Ethics*, 117(1), 123-136.
- Matwyshyn, A. M. (2009). CSR and the corporate cyborg: Ethical corporate information security practices. *Journal of Business Ethics*, 88(4), 579-594.
- Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. *Computer Law & Security Review*, 24(6), 540-554.
- Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, 56, 11-26.
- NIST. (2012). *Guide for conducting risk assessments.*: National Institute of Standards and Technology. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>
- NIST. (2018). *Vetting the security of mobile applications.*: NIST Special Publication 800-163. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf>
- Ogundele, O., Zavorsky, P., Ruhl, R., & Lindskog, D. (2012). The implementation of a full EMV smartcard for a point-of-sale transaction and its impact on the PCI DSS. *Proceedings of the 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Conference on Social Computing (SocialCom)*.
- O'Rourke, M. (2019). The small business cybersecurity knowledge gap. *Risk Management*, 66(8), 36-36.

- Park, S. (2019). Why information security law has been ineffective in addressing security vulnerabilities: Evidence from California data breach notifications and relevant court and government records. *International Review of Law and Economics*, 58, 132-145.
- Perrini, F., Russo, A., Tencati, A., & Vurro, C. (2011). Deconstructing the relationship between corporate social and financial performance. *Journal of Business Ethics*, 102(1), 59-76.
- Ponemon Institute. (2016). *2016 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf
- Ponemon Institute. (2017). *2017 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from <https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html>
- Ponemon Institute. (2018). *2018 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/Keeper_2018-Ponemon-Report.pdf
- Ponemon Institute. (2020). *The economic value of prevention in the cybersecurity lifecycle*. Retrieved from <https://info.deepinstinct.com/value-of-prevention>
- Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5), 551-567.
- Pragati, V. (2015, June 11). Is your small business a perfect target for hackers? *Forbes*.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 34(4), 757-778.
- Raghavan, K., Desai, M. S., & Rajkumar, P. (2017). Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence*, 2(1), 9-15.
- Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management*, 2(1), 122-136.
- Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems*, 51(3), 493-505.
- Salkind, N. J. (2009). *Exploring research*. Pearson Education.

- Sawik, T. (2013). Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems, 55*(1), 156-164.
- Schneier, B. (2006). *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media.
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341.
- Shim, W. (2011). *Interdependent risk and cyber security: An analysis of security investment and cyber insurance*. ProQuest Dissertations and Theses Database (UMI No. 3432938).
- Sidel, R. (2014, August 15). Supervalu reports data breach. *The Wall Street Journal*.
- Silva, L., & Backhouse, J. (2003). The circuits-of-power framework for studying power in institutionalization of information systems. *Journal of the Association for Information Systems, 4*(1), Paper 14.
- Silva, L., Hsu, C., Backhouse, J., & McDonnell, A. (2016). Resistance and power in a security certification scheme: The case of c: Cure. *Decision Support Systems*.
- Sinanaj, G., & Zafar, H. (2016). Who wins in a data breach? A comparative study on the intangible costs of data breach incidents. *Proceedings of the Pacific Asia Conference on Information Systems*.
- Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*(1), 2.
- Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of power: A study of mandated compliance to an information systems security de jure standard in a government organization. *MIS Quarterly, 34*(3), 463-486.
- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225.
- Son, J. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48*(7), 296-302.
- Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly, 34*(3), 503-522.
- Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly, 147-169*.
- Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning

- models for management decision making. *MIS Quarterly*, 441-469.
- Strauss, K. (2015, August 6). How small businesses can improve their cyber security. *Forbes*.
- Symantec. (2016). *Internet security threat report*. <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>
- Terrell, S. R. (2016). *Writing a proposal for your dissertation*. Guilford.
- The Joint Task Force on Cybersecurity Education (2017). *Curriculum guidelines for post-secondary degree programs in cybersecurity*. <https://cybered.acm.org/>
- Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), 476-486.
- Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37(1), 21-54.
- Verizon Enterprise. (2017). Verizon 2017 data breach investigations report (DBIR). Retrieved from www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf
- Verizon Enterprise. (2020). Verizon 2018 data breach investigations report (DBIR). Retrieved from <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>
- Viduto, V., Maple, C., Huang, W., & López-Peréz, D. (2012). A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem. *Decision Support Systems*, 53(3), 599-610.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102.
- Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security*, 44, 1-15.
- Whitehouse.gov. (2015). *The personal data notification & protection act*. <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf>.
- Zioboro, P., Yadro, D. (2014, January 10). Target now says 70 million people hit in data breach. *The Wall Street Journal*.