2022

Impact of Internal Control, Cybersecurity Risk, and Competitive Advantage on Retail Cybersecurity Budget

Samuel William Pfanstiel
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral dissertation by

Samuel Pfanstiel

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Holly Rick, Committee Chairperson, Management Faculty
Dr. Robert Kilmer, Committee Member, Management Faculty
Dr. Aridaman Jain, University Reviewer, Management Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2022

Abstract

Impact of Internal Control, Cybersecurity Risk, and Competitive Advantage on Retail Cybersecurity Budget

by

Samuel Pfanstiel

MBA, University of Phoenix, 2004

BS, Oral Roberts University, 1998

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2022

Abstract

Retail organizations are driven to improve security posture for many reasons, including meeting financial regulation requirements, mitigating threats of data breach, and differentiating themselves within markets affected by customer perception. The problem was that little was known about how these drivers of internal control, cybersecurity risk, and competitive advantage impact retail cybersecurity budgets within the retail sector. The purpose of this quantitative nonexperimental correlational study was to describe the relationship between cybersecurity budget and drivers of internal control, cybersecurity risk, and competitive advantage among U.S.-based retail merchant organizations. Real options theory provided a foundation for explaining this decision-making process. Data were collected from a web-based survey of 66 U.S. retail merchants. Results from multiple linear regression analysis indicated a positive predictive relationship between the driver of internal control and cybersecurity budget (F = 10.369, p = .002). Analysis also resulted in a regression formula by which assessment of this predictive organizational trait may be used to forecast or benchmark expected cybersecurity budget. Retail organizations may evaluate these factors to learn how they may be contributing to inefficient cybersecurity investment strategies, and security firms and regulators may develop improved tools and education initiatives by which to address drivers of underinvestment. With this information, leaders may effect social change by optimizing security investments that lead to lower prices, improved consumer privacy, and a more stable retail economy.

Impact of Internal Control, Cybersecurity Risk, and Competitive Advantage on Retail Cybersecurity Budget

by

Samuel Pfanstiel

MBA, University of Phoenix, 2004

BS, Oral Roberts University, 1998

Dissertation Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy

Management

Walden University

May 2022

Dedication

When I first made the decision to pursue my doctorate, my children were young, and I did not fully grasp how much time and energy this journey would require. As our life journey traversed three states, four houses, three graduations, and a pandemic, one thing was always constant: “Sorry, Daddy’s got to work on school!” Although I don’t regret this choice, and I always made time for the most important moments, I was often distant, distracted, or sleep deprived, and for that I owe my loving family a debt of gratitude. This dissertation is dedicated to them:

To Caleb, my diligent and conscientious professional: You seem intent to ignore my warnings and follow your father into cybersecurity! Your keen insight and kind heart will undoubtedly lead you to success here or wherever your path may lead. Although my studies may have stolen me away from a few of your soccer games, I will always be your biggest fan, and I look forward to my front-row seat for the amazing things you will accomplish!

To Emily, my talented artist and my joy: The beauty of your art is matched only by the beauty of your heart. You aspire to see the treasure and meaning in our earth and in those with whom we share it. You are loving, resilient, and passionate, and you inspire me to seek out those traits in myself and others: to always show compassion, to chance vulnerability, to prioritize self-care—but to never take myself too seriously!

To Judah, my musician, warrior, and philosopher: most of your life has been spent watching your father struggle toward this academic goal, and perhaps mine has been a poor example to the value of this pursuit. However, I believe you have learned its most important lessons: to exercise your mind, consider your weaknesses, respect the wisdom of experts, and leave this world better than you found it. I am immeasurably proud of your staunch resolve, strong will, and sharp wit. Set forth on your path with compassion and strength, and you will change this world for the better.

Most of all, to the love of my life, Melinda: For nearly 30 years you have been my personal source of unflickering light, unfathomable love, and unflinching belief. You have always given your full support to my harebrained ideas and ambitious goals, and backed it up with patience, peace, and prayer. I cannot begin to express just how grateful I am to have you by my side on this journey, as well as through all of life’s challenges. Now that our nest is emptying and school is ending, I’m eager to discover that next challenge together! It may sound trite, but I literally could not have done this without you—nor would I have wanted to. I love you with every bit of my heart.

Acknowledgements

First, I would like to thank Lawrence Gordon, Martin Loeb, William Lucyshyn, and Lei Zhou for their gracious permission to use their survey instrument and build upon their research with the addition of this humble study. I have learned so much from your contributions in our field.

Many thanks to Robert Kilmer and Aridaman Jain, whose wise methodology and research contributions exponentially increased the chances that this capstone work will withstand the rigors of time, review, and—with any luck—real-world application.

Finally, I wish to give my heartfelt thanks to my longsuffering dissertation committee chair, Holly Rick, who took in turn the unenviable roles of cheerleader, counselor, cat herder, and chief cajoler—wearing whatever hat was necessary to ensure we reached the finish line together. Without your insight, encouragement, and patience, I would still be obsessing over some minutia, and losing sight of the big picture. Thank you for helping me achieve my dream!

Table of Contents

List of Tables v

List of Figures vi

Chapter 1: Introduction to the Study 1

Background of the Study 2

Problem Statement 4

Purpose of the Study 4

Research Questions and Hypotheses 5

Omnibus Research Question and Hypotheses 5

Hypotheses 6

Theoretical Foundation 7

Nature of the Study 8

Definitions 9

Assumptions 11

Scope and Delimitations 12

Limitations 13

Significance of the Study 15

Significance to Theory 17

Significance to Practice 17

Significance to Social Change 18

Summary and Transition 18

Chapter 2: Literature Review 20

Literature Search Strategy.....21

Theoretical Foundation.....22

Decision Theory.....22

Real Options Theory.....26

Literature Review.....31

Risk Management.....31

Retail Cybersecurity.....36

Modeling Security Cost Drivers.....44

Independent and Dependent Variables.....47

Internal Control.....47

Cybersecurity Risk.....48

Competitive Advantage.....50

Cybersecurity Budget.....51

Research Question.....52

Summary and Conclusion.....53

Chapter 3: Research Method.....54

Research Design and Rationale.....55

Methodology.....58

Population.....58

Sampling and Sampling Procedure.....59

Procedures for Recruitment, Participation, and Data Collection (Primary Data).....64

Instrumentation and Operationalization of Constructs 69
Operationalization of Variables 70
Data Analysis Plan 73
Threats to Validity 77
External Validity 77
Internal Validity 78
Construct Validity 79
Ethical Procedures 79
Summary 81
Chapter 4: Results 82
Data Collection 83
Study Results 84
Descriptive Statistics 84
Statistical Assumptions 90
Hypothesis Testing 96
Summary 101
Chapter 5: Discussion, Conclusions, and Recommendations 102
Interpretation of Findings 102
Limitations of the Study 108
Statistical Strength 108
Assumptions 109
Model Limitations 111

Recommendations....111

Implications....115

Conclusions....117

References....119

Appendix A: Management Journals Searched....148

Appendix B: Technology Journals Searched....160

Appendix C: Approval to Use Instrument....162

Appendix D: Survey Instrument....168

List of Tables

Table 1. Variables 56

Table 2. Descriptive Statistics for Model Variables 86

Table 3. Recruitment Method 87

Table 4. Participant Roles 88

Table 5. Employee Count 89

Table 6. Gross Annual Revenue 89

Table 7. Descriptive Statistics for Normality 93

Table 8. Coefficient Correlations 95

Table 9. Correlation and Collinearity Indices 95

Table 10. ANOVA 96

Table 11. Omnibus Model Summary 97

Table 12. Omnibus Model Coefficients 98

Table 13. Univariate ANOVA 100

Table 14. Univariate Model Summary 100

Table 15. Univariate Final Model Coefficients 100

List of Figures

Figure 1. Modeled Relationship Between Variables 56

Figure 2. Comparison of Population and Sample - Revenue.. 85

Figure 3. Comparison of Population and Sample - Employees.. 85

Figure 4. Histogram of Standardized Residuals Used to Visualize Outliers 91

Figure 5. Scatterplot of Residuals and Predicted Values to Identify Outliers and
Visualizing Assumption of Homoscedasticity. 92

Figure 6. Testing Assumption of Normality With P-P Plot.. 94

Figure C1. Approval From Martin Loeb.. 162

Figure C2. Approval From Lawrence Gordon.. 163

Figure C3. Approval From William Lucyshyn... 165

Figure C4. Approval From Lei Zhou.. 166

Chapter 1: Introduction to the Study

Retail businesses face the threat of an impending cybersecurity incident, and management must balance financial priorities with the investments necessary to mitigate these risks. When these cybersecurity risks are realized, associated costs commonly lead to price increases and violations to individual privacy, ultimately harming consumers (Hemphill & Longstreet, 2016; Martin et al., 2017). Erosion of consumer confidence from these events also impacts buying behaviors (Janakiraman et al., 2018), adversely affecting entities throughout the retail vertical (Nagurney et al., 2017). These outcomes within the organization, the retail sector, and society at large compel business leaders to recognize risks and prioritize investments in services, systems, and processes to prevent such attacks.

Existing research supported the opportunity for significant contribution on this topic. Cisco (2019) reported that only 47% of security officers allocate resources based on perceived threats. For organizational leadership, this problem translates into competing budgets and risk uncertainty (Raghavan et al., 2017). Chronopoulos et al. (2018) described the challenge of making capital investment decisions related to data breach prevention with incomplete information because the savings from such treatments are unknown. The dynamic nature of cyberattacks and this research gap warranted an improved understanding of how certain organizational traits affect cybersecurity budgets, thereby justifying the increased vigilance needed to reduce their impact on society and industry.

In this chapter, I discuss the theoretical and practical background from which the research problem, purpose of the study, and research questions were derived. An overview of the theoretical foundation and research methodology is also provided. This chapter also contains definitions, assumptions, and research scope delimiters that constrained the study, followed by a description of this study's significance.

Background of the Study

Organization management, managerial accounting, and cybersecurity researchers have sought to answer the question of optimal cybersecurity investment in an effort to aid practitioners seeking to identify which investments are well suited to address associated risk. These approaches include maximizing the efficiency of decision making for capital budgeting and investment in ways that maximize profits and minimize risks for investment in long-term assets (Gordon & Pinches, 1984). Efforts have included those by Gordon and Loeb (2006a) and Sonnenreich et al. (2006), whose submissions on calculating return on security investment offered models that incorporated risk exposure, impact analysis, and investment cost to determine optimal security investment.

However, these models failed to account for the need to address all identified drivers associated with cybersecurity underinvestment. For instance, retail organizations under increasing regulation rely on cybersecurity control systems to provide critical internal control over financial systems (Chang et al., 2019; Flamholtz et al., 1985). Investments in security technologies and processes are crucial to avoid financial losses associated with cybersecurity risks (Romanosky, 2016; von Solms & von Solms, 2018). In addition, market perceptions associated with security also drive success in the marketplace as a function of an organization’s competitive advantage (Kosutic & Pigni, 2020). Recent works have explored the challenge of underinvestment in cybersecurity across various industries. These efforts have resulted in reliable survey instrumentation for measuring internal and external cybersecurity budget drivers (Gordon et al., 2015a), modeling a firm’s optimal investment (Gordon et al., 2015b), and exploring effects of regulation to increase investment (Gordon et al., 2015c).

Real options theory describes how organizations make decisions for investments when future outcomes are uncertain (S. C. Myers, 1977), and provides a framework for explaining why minimized information technology (IT) security investments (to cover identified costs) can yield while incorporating assessments of uncertain outcomes based on net present values can be an efficient and agile investment strategy (Fichman, 2004). Real options theory informs the way subconscious decisions are made to minimize investment based on perceived risk (Benaroch, 2018), and describes the relationship between anticipated cost and cybersecurity return (Martakis, 2015), but does not factor nonfinancial decisions and their impact on determining security budget. Informed by real options theory and its use of multiple decision-influencing factors for investment, Gordon et al. (2015a) measured the influence of certain organizational traits on enterprise cybersecurity investment. However, no known confirmatory analysis has been performed, and these individual attributes have not been modeled as drivers of cybersecurity budget among U.S. retail merchants, an industry impacted by cybersecurity threats such as exfiltration of cardholder data, transaction fraud, and threats to consumer privacy.

Problem Statement

Cybersecurity investment constitutes a significant portion of capital and operational expense for connected retail enterprises; however, allocating budget to predict and prevent cybersecurity attacks can be a significant social and business challenge. The general management problem was that when these budget decisions fail to address security risk, the retail industry may experience continued loss due to regulatory fines, data breach costs, and diminished consumer goodwill (IBM, 2021). These impacts may lead to price increases and threats to individual privacy, which inflict measurable harm on consumers (Hemphill & Longstreet, 2016; Martin et al., 2017). Erosion of consumer confidence from these events also impacts buying behaviors (Janakiraman et al., 2018), adversely affecting entities throughout this vertical (Nagurney et al., 2017). These outcomes within the organization, the retail sector, and society at large compel business leaders to prioritize investments that mitigate the risk of such attacks (Gordon et al., 2018). The research problem was that little was known about how organizational drivers of internal control, cybersecurity risk, and competitive advantage inform U.S. retail management decisions about cybersecurity budget.

Purpose of the Study

The purpose of this nonexperimental quantitative correlational study was to describe the relationships between the dependent variable of cybersecurity budget and three drivers, the independent variables of internal control, cybersecurity risk, and competitive advantage, within U.S.-based retail merchant organizations. Internal control related to the degree that an organization considers cybersecurity part of its approach for protecting the integrity of financial systems. Cybersecurity risk was related to the threat of substantial loss either directly (private cost) or to the retail industry as a whole (externalities). Competitive advantage was derived from its chosen security posture, and information security investment was defined as the percentage of IT budget devoted to cybersecurity. The design of the research included a quantitative evaluation approach to validate the applicability of the real options theory explanatory model proposed by Gordon et al. (2015b, 2018) for understanding and predicting cybersecurity budget drivers among U.S. retail merchants. I leveraged an existing validated instrument (Gordon et al., 2015a) to collect primary data from this population of U.S. retail merchants to measure the strength of these hypothesized relationships.

Research Questions and Hypotheses

The goal of this quantitative study was to obtain a better understanding of how cybersecurity budget may be impacted by an organization’s internal control, cybersecurity risk, and competitive advantage by answering the following research question and addressing the omnibus and individual null hypotheses and alternative hypotheses:

Omnibus Research Question and Hypotheses

RQ: What relationships exist between internal control, cybersecurity risk, competitive advantage, and cybersecurity budgets among U.S. retail merchants?

H_0: There is no relationship between the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = \beta_2 = \beta_3 = 0$.

H_a: At least one of the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) are useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants (DV): At least one of these inequalities is true $\beta_1 \neq 0$, $\beta_2 \neq 0$, $\beta_3 \neq 0$.

Hypotheses

$H_0$1: There is no relationship between the independent variable of internal control (IV_1) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = 0$.

H_a1: The independent variable of internal control (IV_1) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_1 \neq 0$.

$H_0$2: There is no relationship between the independent variable of cybersecurity risk (IV_2) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_2 = 0$.

H_a2: The independent variable of cybersecurity risk (IV_2) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_2 \neq 0$.

$H_0$3: There is no relationship between the independent variable of competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_3 = 0$.

H_a3: The independent variable of competitive advantage (IV_3) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_3 \neq 0$.

Theoretical Foundation

The challenge of understanding the reasons for underinvestment in cybersecurity across various industries necessitates a reliable survey instrument for modeling a firm’s optimal investment (Gordon et al., 2015b) and exploring effects of financial and security regulation on such increases in security budgets (Gordon et al., 2015c). Recent research has also shown that causal drivers of investment may be best understood in light of real option theory, where these organizational traits influence security budget decisions and explain how organizations make decisions for investments in light of uncertain outcomes (S. C. Myers, 1977). Originally used in decisionmaking for investments in petroleum exploration, real options theory has also been used in minimizing IT security investments to cover identified costs by incorporating quantitative assessments of uncertain outcomes (Fichman, 2004). Real options theory helps explain subconscious decisions to minimize investment based on perceived risk (Benaroch, 2018) and describes the relationship between anticipated cost and cybersecurity return (Martakis, 2015).

Real options theory is also useful for explaining the relationships between internal control, cybersecurity risk, competitive advantage, and the resulting cybersecurity budget decisions as retailers seek to maximize the outcomes of their capital investments to prevent data breach (Gordon et al., 2015a). Fichman (2004) proposed a similar theoretical integration of real options theory with IT platform investment, identifying 12 factors that may be used to determine option value and aid in operationalizing influences on cybersecurity within the paradigm of real options theory. Benaroch (2018) and Chronopoulos et al. (2018) also proposed a quantitative model for applying real options theory to cybersecurity investment, allowing for approaches such as progressive application of mitigation and monitoring, and optimizing investment timing to minimize losses. These applications of real options theory that leverage determinants to understand budgetary decisions empower management with more granular understanding of applying security treatments with an eye toward optimized outcomes.

This understanding from real options theory of how individual drivers influence decisions to commit or defer investments in cybersecurity informed the analytical technique in the current study. This research design relied on measurement of respondent organizations' allocation of information technology budget for cybersecurity investment, and management's perceptions about organizational benefits driven by cybersecurity investments in these three areas. Correlational analysis techniques were used to assess each driver's explanatory power over management's decision to allocate budget to cybersecurity investments. Finally, these techniques supported the testing of the hypotheses, which suggested that these determinants predict or explain the corresponding cybersecurity budget decisions based on the value of the respective options. In this manner real options theory informed the relationship between the analytical technique, the hypotheses, and their role in answering the research question regarding relationships that may exist between the drivers and the decision to invest.

Nature of the Study

This nonexperimental quantitative correlational study included an email recruitment data collection approach to enlist survey respondents from a randomized sample of management contacts from U.S. retail merchants. Survey response data included responses to demographic and psychographic questions administered via an internet survey using a validated instrument and were analyzed using multiple regression statistical analysis. The goal of this analysis was to confirm a positive predictive model that explains the relationship between each of the three independent variables—internal control, cybersecurity risk, and competitive advantage—and the dependent variable of cybersecurity budget. This study also included descriptive statistics to provide useful benchmarking and industry insights to clarify the role each of these attributes may play in influencing cybersecurity investments among the target population. The selection of a quantitative nonexperimental design to model determinants of management investment decision making was common within the body of decision-theory research (Dixit et al., 1994; Economides, 1999; Pindyck, 1991; Simon, 1960). The current study expanded the collective works that have contributed to the formation and revisions of the Gordon-Loeb model (Gordon & Loeb, 2002, 2006b), the Department of Homeland Security (DHS) Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector survey instrument (Gordon et al., 2015a), and analysis of the variables included within the posited model (Gordon et al., 2018).

Definitions

Competitive advantage: The degree to which an organization receives benefits from the market based on its perceived cybersecurity posture (Gordon et al., 2015a).

Cybersecurity budget: The annual budget of an organization allocated to cybersecurity capital investment and operational expenditures as a function of overall information technology budget (Gordon et al., 2015a).

Cybersecurity risk: Identified impacts of a significant data security incident calculated based on financial losses including both private costs and externality costs (Gordon et al., 2015a).

Externality cost: Indirect spillover costs incurred due to cybersecurity breaches that occur to other entities within the industry, geographic region, country, or other association (Gordon et al., 2015a).

Internal control: The need for reliable financial reports driven by the need for cybersecurity controls around an organization’s financial accounting systems, whether by strong internal management or in response to regulatory requirements (Gordon et al., 2015a).

Merchant: The industry definition of merchant is used in alignment with the definition provided by the Payment Card Industry Security Standards Council (PCI SSC) as “any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services” (PCI Security Standards Council, 2016, p. 11).

Private costs: Direct costs associated with potential cybersecurity breach (Gordon et al., 2015a).

Retail: The industry classification “retail trade” was used to create a sampling frame from the population of retail organizations within the identified geography and is defined by NAICS as the “sector [which] comprises establishments engaged in retailing merchandise, generally without transformation, and rendering services incidental to the sale of merchandise” (NAICS Association, 2022, para. 2). The preliminary identification was based on available NAICS codes assigned to the organization beginning with "44." This was further confirmed based on self-identification by acknowledgement of employment in a "U.S.-based retail compan[y]" and/or response to the survey question: "Which of the below categories describes your organization's principal operations (circle the correct answer/s): Consulting, Defense, Education, Energy, Financial, Services, Health Care, Information Technology, Law Enforcement, Legal Manufacturing, Retail, Telecommunications, Transportation, Utilities, Other (please specify)?" (Gordon et al., 2015a, p. 119).

Assumptions

The use of email as a recruiting method was necessary to obtain sufficient responses. I assumed that entities within the target population used email, did not have overly restrictive antispam methods in place to block receipt of the recruitment emails and other correspondence, and would respond to unsolicited inquiries. Previous studies of adoption of email technologies by businesses showed a growth of email adoption from 23.9% to 90% from 1998 (Sillince et al., 1998) to 2003 (M. Levy & Powell, 2003). My experience and this identified adoption curve confirmed that sufficient retail businesses use email to render this assumption of minimal impact to the external validity of the study.

The validity and reliability of the existing instrument created by Gordon et al. (2015a) facilitated ease of data collection and limited potential threats to internal validity due to the previous testing performed by these researchers. During their initial study and subsequent use, Gordon et al. (2018) the researchers identified measures taken to perform pilot study and field testing of the published instrument to confirm reliability and internal validity for measuring these variables within a similar model to that posited in the current study. However, reliability and validity coefficients were not provided; therefore, assumptions were made as to the construct validity of the instrument and its suitability for measurement of the variables.

Additionally, I assumed the respondents in positions of retail management would recognize the role and degree of influence of the determinants of internal control, cybersecurity risk, and competitive advantage in decisions related to cybersecurity budget allocation. Appropriate measures were taken to ensure recruitment of contacts with the necessary level of insight, but I assumed that management perceptions of the influence of these traits may be impacted by position, assigned responsibilities, and ability to discern the influences of these factors on budgetary decisions. I chose wording for the informed consent acknowledgement that identified the purpose of the study and types of questions that the respondent would be expected to address.

Scope and Delimitations

The scope of this study was constrained to the population of retail merchant businesses with headquarters located within the boundaries of the United States. This delimitation was intended to control for effects of cultural, legal, language, economic, or geographic confounding influences on the posited relationships. Results were generalizable to all types of retailers within this region. However, this scope reduced generalizability of findings to other countries, industries, or markets.

The research problem focused on three organizational drivers about which little was known within this population, and which were measurable by demographic and psychographic responses within the published Department of Homeland Security (DHS) Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector instrument (see Gordon et al., 2015a). These drivers were selected for research due to their perceived impact on cybersecurity investment and the availability of the validated instrument by which to measure them. The scope, however, was not extended to identification of other potential confounding variables, such as gross revenue, respondent role, or cybersecurity awareness. Discussion of other traits is included in recommendations for future research in Chapter 5; however, analysis of their role was excluded from this study as a means of answering the research question.

Limitations

The first identified set of limitations was the constraints that resulted from the use of email-based recruitment methodology. Email solicitation using a third-party data source presented a challenge in obtaining a sufficient sample representative of the population and free from self-selection bias. This may be due to risk-aware information technology and information security management being naturally suspicious of unsolicited emails, untrusting of the source (despite reasonable efforts to provide reassurance), or otherwise too busy to respond. Furthermore, the outcome of this study was limited in its generalizability outside of the sampled industry (retail) and region (United States) due to data set limitations. However, these restrictions also created opportunities for future studies by modeling an effective research methodology that may be used to measure these relationships in other target populations.

Second, the research methodology analyzed a proposed predictive relationship between the independent variables, measured by respondents' perceptions, to the dependent variable, measured in budget ranges. This expected correlation of the subjective perception to empirical data constituted a limitation of the study. Although the results supported the hypothesized relationships, the granularity of impact was also limited. This data collection approach allowed room for future researchers to hone the survey instrument and model to operationalize these independent and dependent variables using measurable data thereby providing improved resolution of each variable's unique contribution.

The model included three possible variables that may impact the dependent variable but did not measure the presence of possible confounding variables such as additional risks or infrastructure that may increase security budgets, or previous security investments or financial constraints that may limit the entity's ability to invest at the time of the survey. The overall impact of these variables was controlled through random sampling. I measured only the impacts of the identified explanatory variables; however, the impact of these confounding variables could have threatened the internal validity of the resulting relationship.

Finally, as a security practitioner and retail compliance auditor, I was conscious of my biases that could have impacted the outcomes of the study. These biases may have been exhibited in the form of a natural proclivity toward internal control or cybersecurity risk as carrying greater weight in security investment decisions, or my use of specialized terminology that may be unfamiliar to the target population. Researcher bias was addressed by use of an impersonal data collection methodology, objective quantitative statistical analysis, and conscious review of solicitation emails and instructions (as well as reliance on instrument language that had undergone pilot testing).

Significance of the Study

Through an improved understanding of the drivers that influence budget decisions among U.S. retailers, stakeholders such as card brands, acquiring banks, regulatory agencies, and policymakers may be better able to implement educational programs, increase knowledge sharing, and address prevalent attitudes that may be leading to inadequate cybersecurity investment. Through this study, I have reported empirical response data used to confirm this explanatory model for drivers of cybersecurity investment, providing a retail benchmark for perceived impacts by which decision makers may measure their expectations and cybersecurity investments against those of peers within the industry (see Eilts & Y. Levy, 2018). These survey outcomes may be valuable for retail payments organizations evaluating their cybersecurity investment strategy in security optimization technologies, which may aid in improving retail efficiency, mitigating fraud, and strengthening data security posture.

Beyond the benefits to the organization, retailers are bound by corporate social responsibility to protect their consumers and other entities from the spillover effects of poor security management (Shackelford, 2017). The current study added to a growing body of knowledge to reduce the negative social impacts that occur from increasing security threats by reminding organizational leadership of their role to protect the integrity of sensitive consumer data and contribute to the stability of the retail economy at large. By quantifying the degree to which organizational response to externalities affects cybersecurity investment, this work shed light on the shared responsibility of retailers to decrease spillover costs that result from cybersecurity attacks. These externalities from vulnerable infrastructure may include attacks launched against other entities, threats to individual consumer privacy, disrupted access to critical (even lifesaving) supplies, and general loss of market confidence (Gordon et al., 2015b). The unique contribution of these three drivers for investment—internal control, cybersecurity risk, and competitive advantage—may help raise awareness of corporate responsibility and its role in reducing the occurrence of society-affecting outcomes resulting from inadequate security investment.

This study also added to the work of Gordon et al. (2018), in which senior executives from 1,600 private firms in various sectors (predominantly critical infrastructure) were surveyed to determine how internal control, cybersecurity risk, and competitive advantage influenced overall cybersecurity spending as a percentage of revenue. Gordon et al. leveraged a validated and published survey instrument they introduced three years prior (2015a) and analyzed the resulting data using logistic regression analysis to quantify the associations between these organizational attributes and corresponding budget allocation. The current study served as both confirmatory analysis of these observed relationships, as well as an extension of the analysis performed by introducing multiple linear regression as an alternate analytical technique (given the normal distribution of the outcome variable) for purposes of explaining the linear influence of these predictors and supporting regression-based benchmarking techniques.

Significance to Theory

The use of real options theory to provide explanatory power to the expected observations supported other researchers who also wish to explore this decision support system within this model or other models related to cybersecurity budget decisions. In Chapter 5, I provide discussion related to these traits and their impact on current or deferred actions related to capital investment decisions as operationalized through the organization’s cybersecurity budget, adding to the body of knowledge related to real options theory for cybersecurity investment.

Significance to Practice

Practical use of the Gordon-Loeb model for determining optimal investment was an important application of this study because it lent support to this informative model as a useful tool for security and management practitioners seeking to optimize their cybersecurity budget. When organizations do not match the optimal investment as described by this model, this may be due to the strategic priorities and cultural norms identified within the current study, such as influence of internal control, identified cybersecurity risk, or strategic competitive advantage. Confirming the roles these attributes play in bringing parity to cybersecurity budgeting and actual risk may provide useful focus for educators when communicating the importance of culture as a predictor for mitigating cyber risk, or regulators seeking to create incentives that influence the prioritization of cybersecurity investments.

Significance to Social Change

The goal of this work was to influence the U.S. retail industry to better prepare for cyber incidents and prioritize optimal investment to limit the social costs that harm consumers and reduce confidence in retail markets. As researchers and security practitioners better understand the drivers for investment, events associated with loss of consumer information, credit card data breaches, and fraud occurrences may be reduced, thereby creating positive social change for consumers on whose shoulders (and pocketbooks) these events fall. Reduction of retail fraud may impact merchant discount rates and, in turn, consumer pricing. Furthermore, mitigation of security events that compromise customer information may improve confidence in retail shopping experiences, thereby reducing indirect harm incurred by consumers who depend on secure local and online retail as a reliable means of access to necessities.

Summary and Transition

Decisions made about cybersecurity investment by retail organizations have significant impact on results of omnipresent security threats and the impacts these events have on society at large. In this chapter, I described the purpose of this study to examine organizational determinants that lead to such investments, provided a background of research related to the decision theories that support this research, and examined drivers for security budget decisions. I also described the research question and hypotheses that I sought to address related to three traits that previous research suggested have predictive power on these decisions: internal control, cybersecurity risk, and competitive advantage. These variables were the predictors for this study, and the outcome variable was cybersecurity budget. I provided an overview of the quantitative research methodology, data collection approach, assumptions, and scope to support the academic rigor by which this study was performed. Finally, I reviewed the research, practical, and social significance of the study, which indicated the importance of this work. In the following chapter, I review the research foundation in greater detail.

Chapter 2: Literature Review

The research problem for this study was that little was known about how organizational drivers of internal control, cybersecurity risk, and competitive advantage impact U.S. retail management decisions about cybersecurity budget. U.S. retailers often do not allocate sufficient budget to mitigate risks of cybersecurity breach (Cisco, 2019; IBM, 2021; Verizon, 2019a). Security events incur significant costs both to the organization and to the industry, which lead to price increases and threats to individual privacy, inflicting measurable harm on consumers and society at large (Hemphill & Longstreet, 2016; Martin et al., 2017). To better understand the role of these characteristics and to address this problem of underinvestment, I sought to explain the how three measurable attributes among U.S.-based retail organizations (internal control, cybersecurity risk, and competitive advantage) influence cybersecurity budgets.

In this chapter, I provide an in-depth analysis of the current and historical literature that informed this study. This review includes the origin, evolution, application, and use of real options theory, which formed the theoretical foundation for this study and drove the research question. Furthermore, I describe the concepts and models found in the literature that were commonly used to understand and identify drivers for cybersecurity budgets and explain this observed phenomenon of underinvestment in cybersecurity. In addition, I review the body of research from which the independent and dependent variables within this study were derived: internal control, cybersecurity risk, cybersecurity competitive advantage, and cybersecurity budget. Finally, I show how other researchers employed methods to answer similar questions within the U.S. retail industry and other industries, and explore research trends and gaps that justified the need for the current study and informed my research design.

Literature Search Strategy

I used the following search methods to access relevant academic articles and industry publications related to the theories, models, variables, and design of this study. I accessed the Walden University online library, powered by EBSCO Discovery Service, and conducted broad and targeted searches among the catalog of journals identified within the business and management disciplines and targeted peer-reviewed journals classified as management, decision theory, and business (general). This approach resulted in a number of journals being queried, which are listed in Appendix A. Additional searches within management-related journals related to technical topics were focused on journals related to telecommunications, computer science, and technology matters, including those listed in Appendix B. I also performed searches using Google Scholar and accessed published articles from ResearchGate and other original publication sources based on references found in other articles. In each case, I applied the appropriate year of publication filter to ensure particular focus was placed on articles published in the past 5 years, although in some cases this filter was removed to identify articles that provided historical context to important topics.

The search terms I employed to find applicable articles included multiple combinations of the following search words and phrases: *cybersecurity*, *security*, *information security*, *compliance*, *information technology*, *cost*, *budget*, *cybersecurity budget*, *cybersecurity investment*, *framework*, *model*, *retail*, *decision theory*, *real options* *theory*, *Gordon-Loeb model*, *internal control*, *risk*, *cybersecurity risk*, *externality*, *spill-over cost*, *spillover cost*, *competitive advantage*, *benchmarking*, *multiple regression analysis*, and *logistic regression analysis*.

Theoretical Foundation

This research may aid the retail industry in better understanding optimal cybersecurity budget in light of uncertain data security risks informed by organizational drivers that influence these budgeting decisions. Due to this complexity of drivers and optimized investment, a theoretical foundation addressed both the innate mechanisms that drive human risk evaluation and the quantitative approach for selecting investment projects and allocating budget. The design of this study, including the predictive model, data collection methodology, and analysis approach, was grounded in real options theory, which had its origins in managerial decision theory.

Decision Theory

When considering how individuals and organizations select activities that will be planned and controlled, decision theory provides a valuable framework for understanding human behavior related to making decisions by identifying objectives, measuring relative success, and using analysis models to identify choices that meet these established criteria (Bellman, 1954). This area of behavioral decision theory commonly includes quantitative statistical analysis and probabilities to model how decisions are made and relative correctness of decisions related to one or more identified outcomes (Edwards, 1961). This family of explanatory models and theories can help explain and inform choices by aiding in judgment and inference aided by mathematical models and quantitative analysis techniques (Raiffa & Schlaifer, 1961; Slovic et al., 1977). These techniques are suitable for understanding human behavior in a variety of fields—medicine, economics, education, political science, psychology—but due to the informative nature for guiding both ad hoc and procedural tasks to increase organizational value, the application of decision theory for use in management is apparent (Simon, 1960).

Decision Theory in Management

Organizations, industries, and agencies rely on management decision making related to resource investment, and the drivers behind such decisions can be complex. Management decision theory focuses on the elements of decision theory related to minimizing risk and maximizing calculated value of the evaluated outcomes and builds on this foundation to guide organizational decisions by informing judgment for investment decisions. The manner in which decision theory researchers describe an individual's arrival at a particular judgment has included evaluating biases (Tversky & Kahneman, 1973), subconscious weighting of information (Wallsten, 1971), and sequential processing limitations (M. D. Cohen et al., 1972). Support for objective correctness of decisions independent of the biases and inclinations of management decision makers was endorsed by Blau (1968), placing managers in a position of responsibility to ascertain the best option as agents for these decisions.

This use of contemporary quantitative analytical means to determine optimal decision paths thus originated from positivist organizational ideals promoted by researchers of the late 20th century and supported by the existence of decision science systems, accessible programming, and database systems by which these decisions may be optimized (Tversky & Kahneman, 1973). Irrespective of the inputs studied or models utilized, outcomes in decision management were measured using quantitative statistical analyses techniques (Pindyck, 1991). Adoption of descriptive correlations, financial analysis of predicted outcomes, weighted averages, and decision trees evidence the positivist pedigree of the decision sciences (Donaldson, 2003). This positivist-functionalist underpinning of modern decision theory drives analysis across multiple domains based on quantitative analysis rather than intuition.

Decision Theory in Budgeting

Gordon and Pinches (1984) explored decision support systems for capital budgeting throughout the lifecycle of the decision process, beginning with identifying the problem, developing a number of alternative responses, selecting the optimal investment, and evaluating its performance over time. Gordon et al. (1975) noted that these responses can be operational, administrative, or strategic decisions characterized by whether they are selected frequently by lower level managers, occur semifrequently by middle management, or are implemented less frequently by senior management; the drivers may depend on internal and external environment, risk, business strategy, and goals.

According to Gordon (2004), budgeting is accompanied by making strategic decisions and evaluating outcomes against defined objectives using planning and control. These two functions comprise the principal activities of managerial accounting, with budgeting of resources as one of the crucial tasks. Planning begins with setting or identifying organizational objectives that, when considering the priorities facing modern enterprises, may vary significantly. Control, on the other hand, describes a framework of organizational influence over business processes and systems, and can be categorized into three domains: sociological, administrative, and psychological (Flamholtz et al., 1985). Among these mechanisms are contextual contributors to control, such as culture and surrounding industrial factors. Within their model, Flamholtz et al. (1985) described planning as informing and being informed by operational behaviors, which is to say planning exists in an iterative feedback loop with behavior. Deliberate interventions should thus be made to influence this intricate balance to avoid undesired outcomes.

Decision Theory and Cybersecurity Investment

There have been many applications of decision theory for cybersecurity investment. Moore et al. (2015) found that most information security decision makers do not use quantitative metrics but rather rely on security frameworks to support the adequacy of and dictated cost for investment decisions. Rahimian et al. (2016) viewed this challenge and noted that the common compliance checklist approach lacks recognition of the risks associated with each control objective. To address this, Rahimian et al. developed a risk classification model that quantified three levels of financial risk in three independent risk domains: operational, reputational, and legal. Similarly, Dor and Elovici (2016) modeled the influence of various components of security investment decisions, including the stakeholder involved, their role, organizational structure, and industry.

Straub and Welke (1998) further identified the challenge managers face identifying all available options for addressing systems risk and the impact this knowledge gap plays in identifying optimal solutions. To incorporate risk into these models for decision optimization, Srinidhi et al. (2015) developed a model for optimal allocation of resources that took into account breach risk and opportunity cost of underinvestment in productive assets—outlays that improve an organization's ability to weather security threats in the long term. This difficulty stems from the challenge with determining whether any set of investments or controls provided are sufficient to prevent vulnerabilities from leading to loss (Port & Wilf, 2017).

Selection of security controls can also be modeled using algorithms that evaluate possible combinations and weigh the tradeoffs between risk and cost of the corresponding investments (L. P. Rees et al., 2011). One approach offered by Fielder et al. (2016) highlighted the strengths and weaknesses of game theory and combinatorial optimization as decision-making methodologies, taking into account the impact and cost of the investment. Such complexity lends itself to a theoretical model that is designed to acknowledge uncertainty and incorporate variability, such as real options theory.

Real Options Theory

The current study was grounded in real options theory, which explains how organizations make decisions for investments when future outcomes are uncertain (S. C. Myers, 1977). Originally used in decision making for investments in petroleum exploration (S. C. Myers, 1984; Smith & McCardle, 1998) to provide managerial flexibility for real estate investment (Kulatilaka & Marcus, 1988) or corporate finance (Mason & Merton, 1985), real option theory recognizes and supports the stepwise evaluation processes common among management. In real options theory, decisions to invest are weighed against other outcomes, including decreasing or increasing investment, deferring the decision, or discontinuing pursuit of an investment based on new information that becomes available over time (Kulatilaka, 1995). This additional flexibility analysis approach provides a closer fit to real-world scenarios in which decisions are not made within a single point in time and information related to the investment continues to evolve. This approach lends itself to both traditional investments as well as capital expenditures.

In work on real option theory applications for information technology, Pindyck (1991) compared organizational investment decision making with models from option pricing theory due to their intrinsic irreversibility and ability to be deferred. These decisions, Pinkdyck revealed, are dependent on market forces that introduce risk, and evaluating the value of the option as net present value under each current and future investment state increases the decision maker's ability to maximize the value of the uncertain technology investment. In 1994, Dixit et al. expanded this model by addressing the other naturally occurring market fluctuations, such as changing price, uncertainty, probabilities, and timing, thereby laying the groundwork for the use of real options theory in organizational management for the modern era, with increasing dependence on investments in telecommunications and technology.

Real options theory is more informative than traditional discounted cash flows models in uncertain environments (Pivorienė, 2017) and has explanatory power in numerous realms of industry and management. As part of the drive to facilitate seamless integration of real options theory into all areas of modern enterprise management, Fichman (2004) posited that the value of each real option can be considered along multiple axes of innovation (technology strategy, organizational learning, bandwagon, and adaptation) and addressed the difficulty in predicting, valuing, and managing these options effectively. Li and J. D. Johnson (2002) also examined real options theory for information technology investments along two axes: (a) technology switching costs from low to high and (b) the nature of competition and information exchange from shared to proprietary. When applied to information technology, this model provides unique perspective on cybersecurity investment because the mindset of security practitioners is often one of information sharing and collaboration as these reduce the impact of spillover costs within an industry (Gordon et al., 2015d).

Decision models provide the framework for understanding the rationales and procedures by which optimal decisions may be made. Adner and Levinthal (2004) explored the boundaries within which real options theory may be applied in management decision making, such as identifying new uses for technology under consideration and the new options this creates. Adner and Levinthal also noted that the flexibility of real options decision theory is best employed under a certain level of organizational rigidity whereby the models work best when an organization is willing to abandon an investment despite sunk costs as future uncertainties become clearer. This rigidity supports the original intent of real options, as described by Amram and Kulatilaka (1999) who warned that the value of this approach is realized when organizations are flexible enough to start many projects but rigid enough to abandon them as information becomes available. McGrath (1999) also supported this notion by examining biases that resist such abandonment as failure rather than encouraging the entrepreneurial mindset that sees abandonment as a valued entrepreneurial approach that maximizes the value of real options theory.

This theoretical framework supported the deductive approach used in the current study by providing a systemic view of modern management decision making that helped me explain the observed phenomena (see Imenda, 2014) in which decision determinants may be measured and quantitatively observed. The theoretical proposition of real options theory is that although many investment options exist at any given time, they also persist after a decision has been made and may hinge not on one single decision point but rather on innumerable options to act or defer (Economides, 1999). Real options theory was appropriate to examine decisions made in light of an evolving cybersecurity threat landscape.

Real options theory has thus been applied in similar research related to information security management. Gordon et al. (2003) explained that real options theory can be used with deployment of cybersecurity controls by employing a “wait-and-see” approach. Benaroch (2018) expanded on this approach by describing the deployment of security controls in order of highest impact using a “deploy-and-see” partial implementation approach which makes use of prototypes or scaled deployment. Benaroch (2018) and Chronopoulos et al. (2018) proposed quantitative models for applying real options theory to cybersecurity investment, allowing for approaches such as progressive application of mitigation and monitoring and optimizing investment timing to minimize losses. Herath and Herath (2008) observed that management of intrusion detection systems and intrusion prevention systems (IDS/IPS) can involve not only initial capital outlays, but ongoing post-audit activities for configuration and monitoring, and leveraged real options theory to explain these ongoing interventions. Their proposed model distinguished the traditional use of real options analysis for information technology investment decisions from the approach commonly used in cybersecurity decisions, maximizing breach risk reduction by modeling the incremental impacts of subsequent decisions (Herath & Herath, 2008).

Informed by real options theory, the model proposed by Gordon et al. (2015c) supports the use of both linear and logistic regression analysis to measure the influence of organizational attributes on enterprise cybersecurity investment. Their work confirmed that real options theory is useful for explaining the relationships between internal cost, cybersecurity risk, strategic advantage, and the resulting cybersecurity budget decisions as organizations seek to maximize the outcomes of their capital investments to prevent data breach. These interpretations of real options theory empower management with more granular understanding of applying security treatments with an eye for optimized outcomes.

Real options theory is well-suited to inform the theoretical basis for this study as it provides insight into management perceptions and decision-making calculus that account for immediate and long-term investment options and budgeting allocations. In this current study, the use of real options theory informed the processes by which managers arrive at cybersecurity budgets, informed by their own perceptions of internal control, cybersecurity risk, and competitive advantage within their organization (See Gordon et al., 2015c).

Literature Review

Some of the constructs of interest for this study included risk management, cybersecurity, budgeting, retail cybersecurity, credit card fraud, PCI compliance, and security cost modeling, which were explored below in light of seminal and current research into these topics.

Risk Management

Enterprise risk management strives for an integrated view of all business risk within a coordinated, strategic framework (Bromiley et al., 2015; Nocco & Stulz, 2006). Any investment to offset risk should be aligned to strategic management objectives, risk appetite, and compliance requirements (Bromiley et al., 2015). These alignments demonstrate that, although risk management presents a management challenge for prioritization of limited resources, this function also provides an opportunity for an organization to improve its competitive advantage (Nocco & Stulz, 2006), reduce unexpected costs (Bodin et al., 2008), and protect the integrity of financial reporting systems (Kaplan & Mikes, 2016).

Organizations struggle with managing risk, especially where they have insufficient structure and maturity to manage the process effectively. The process of maturing to use quantitative risk models is a challenge, requiring managers to eschew intuition in favor of filtering risk through analysis of probability and a culture of “quantitative enthusiasm” (Kaplan & Mikes, 2016, p. 8). Frameworks and tools for risk management in certain industries, such as those designed for critical infrastructure and finance, may be extended for use in other sectors, but may be too complex or obscure for use outside of these industries (Bromiley et al., 2015; National Institute of Standards and Technology, 2018).

Adopting mature processes and appropriate toolsets for managing risk is difficult, but culture also plays an important role. Companies that employ mature quantitative risk management frameworks may be better at identifying projects with a tolerable risk-reward ratio, however such companies can still face practical implementation challenges if they lack the company culture necessary to empower middle management to act on those findings (Nocco & Stulz, 2006). Risk management that relies on qualitative faculties such as intuition or anecdotes subject an organization to groupthink and political influences that may adversely affect this important risk management process (Kaplan & Mikes, 2016). Changes to technology and errors in implementation drive a bottom-up risk identification approach, which naturally conflicts with top-down approaches driven by external regulations or governance (Rasmussen, 1997). In this way, cultural norms related to how risks are perceived and mitigated can influence the degree to which these actions are ultimately taken.

Cybersecurity

Cybersecurity, also spelled "cyber security," is a term describing the subcomponent of information security related to electronic data and its protection. The concept of cybersecurity originated in the principle of internet security, described by Moore and R. Anderson (2012) as that study within information security related to messages that may be carried over internetworked systems. As the term cybersecurity came into more common use, Craigen et al. (2014) defined it 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" (p. 13). In its simplest sense, C. Anderson et al. (2017) sought to describe cybersecurity as the balance of sharing and protecting information. Von Solms and von Solms (2018) aligned their definition with those provided by ISO and ISACA, that cybersecurity is the component of information security related to digital data, exclusive of paper media or assets that exist solely in the physical realm. Cybersecurity may thus be described, generally, as those efforts taken with the purpose of preventing unauthorized actions which may impact the confidentiality, integrity, availability, or authenticity of electronic data or services (Zdzikot, 2022). These definitions each convey that physical security controls alone cannot provide sufficient protection to electronic assets, nor is it practical to implement every possible mitigation; thus, a risk-informed approach is crucial for implementing practical and sufficient electronic protections.

Within the realm of cybersecurity, risk management takes on the form of the analytical process of identifying these risks; discovery process of determining potential mitigating treatments; evaluative process of selecting one or more courses of action based on economies, probabilities, and willingness to tolerate negative outcomes; and operational process of implementing and monitoring the selected approach (Ruan, 2017). One such analytical process, proposed by Bodin et al. (2008), combined quantitative risk factors into a single metric based on perceived importance of individual risks, demonstrating that a structured approach using risk perceptions is a key to successful cybersecurity risk management. As a set of decisions and activities that directly impact the organization’s exposure to myriad assaults, an organization’s collective risk management processes (irrespective of whether they are being identified as such) is thus directly responsible for the success or failure of its cybersecurity program, and indirectly for the success or failure of businesses of all sizes (Berry & Berry, 2018; Soltanizadeh et al., 2016).

Cybersecurity Budget

Each possible risk treatment carries with it an intrinsic business cost, whether short term financial cost, long-term investment outlay, or opportunity cost, associated with addressing the identified security risks (Romanosky, 2016). In the hierarchy of cybersecurity management activities, Raghavan et al. (2017) contrasted information technology security investment with those operational costs associated with day-to-day enterprise security processes, such as configuration, vulnerability management, and human resource processes including customer trust and employee training. Capital and operational expenses may be budgeted in advance or measured in arears, using analytical techniques which seek to optimize these expenses by measurement of risk or empirical outcomes (Ekelund & Iskoujina, 2019). In each case, cybersecurity budget decisions are driven by both overt and intrinsic calculations, and it is economically advantageous to seek an optimal investment level.

The potential for misalignment of budget with breach cost is the subject of study into theories related to attaining economic equilibrium among investment decisions. Gordon and Loeb (2002, 2006b) posited a budget framework, from which their eponymous model was obtained, for seeking optimal security investment while minimizing security breach. However, the Gordon-Loeb model fails to consider all externalities, and that the failure to secure private consumer data is a failure of social contract incurring a heavy cost on the company, markets, and society (Acquisti et al., 2006). Böhme and Moore (2016) explored their observation that treatment costs may be both non-linear and unrecoverable: that certain higher impact investments defray sizeable costs with a much lower treatment cost, and that these sunk costs must be considered in contrast to doing nothing at all.

Organizations make these budget decisions based on expected need and represent these needs in the form of forecasted costs, but there also remains the challenge of balancing competing budget priorities for cybersecurity projects when compared to other IT functions. Cisco (2019) observed that only 47% of respondents establish their cybersecurity budget based on organization security outcome objectives, but an almost equal number (46%) admitted that their budget was simply based on the previous year's. While perceived risk reduction is often the primary driver for information security investment, general prioritization of those investments may be more commonly driven by industry frameworks, compliance, or history of previous breach than a strict quantitative analysis or cost-value estimations (Moore et al., 2015). Boston Consulting Group (2019) affirmed that this prioritization task is difficult, and although there is no single way to determine order of cybersecurity spending, the process starts with identifying risk appetite and focusing first on maturity rather than panacea solutions. Overcoming misaligned perceptions of risk is therefore crucial to responsible allocation of limited budget resources.

Retail Cybersecurity

For retail organizations, cybersecurity must be considered for its own set of challenges that it brings. Changes in fraud patterns show retail security breaches shifting from point-of-sale-based vectors to e-commerce attacks, adding to a growing list of attack methods that includes ransomware, denial of service, or other abuse of resources (Trustwave, 2019; Verizon, 2019a). Often the retailer isn’t even the final target, as malicious third parties may seek to attack infrastructure to compromise customer privacy (Larsson et al., 2021), or as a vehicle for launching attacks against other targets (Rashmi et al., 2021). These threats are compounded by changes in consumer behaviors and expectations, as customers increasingly shop via mobile device or marketplace, thereby expanding the attack surface which must be protected (Dumanska et al., 2021). In sum, retailers must be conscious of numerous drivers for cybersecurity that include protecting consumer credit card data, protecting other sensitive corporate data, maintaining service availability, preventing fraud, protecting customer privacy, and meeting compliance mandates.

Among these, the protections of consumer credit card data and the accompanying compliance mandates often take a central focus. Retail operations rely heavily on electronic monetary transactions, and its primary form is credit card processing, which introduces sensitive data that must be protected. To perform credit card transactions, certain critical data must be exchanged between the customer and the merchant, and between the merchant and the credit card processing network. The number embossed or printed on the credit card itself (called the primary account number, or PAN) is the central data element in this exchange, although others must be protected including expiration date, cardholder name, and service code (collectively called “cardholder data”). Other important data include magnetic track data, personal identification number (PIN), PIN block, or card security code (collectively called “sensitive authentication data”). Together these account data support the authorization of the transaction, as well as the process of clearing and funds settlement, but in the wrong hands could allow unauthorized individuals to conduct fraudulent transactions (PCI Security Standards Council, 2016).

Since the inception of credit card processing, authorizations have been performed using imprint readers, telephone authorizations, and mail-in remittance slips, depending on the payment channel in use. In-person payments (referred to as “card present” because the credit card is physically available to the merchant at the time of authorization) could make use of a magnetic stripe reader or integrated chip card reader to obtain authentication data from the magnetic track or chip. In addition, some card present transactions allowed for the cardholder to enter a PIN or sign their name, demonstrating that an authenticated cardholder performed the transaction. For payments conducted by mail order/telephone order (referred to as “card-not-present”), the transaction could be verified using different authentication data printed (but not embossed) on the front or back of the card (card security code). In this manner card present and card-not-present transactions rely on sensitive authentication data to reliably verify the authenticity of the card and cardholder, thereby reducing fraud (Willey & B. J. White, 2013).

At present, with e-commerce, internetworked systems, mobile devices, the Internet-of-things (IoT), and computerized merchant environments, systems now encounter and transmit credit card account data via innumerable ways, increasing the possibility of access by unauthorized individuals at any number of vulnerable touch points. In addition, both cardholder data and sensitive authentication data can be extracted from the memory of compromised systems even if it is never stored (Verizon, 2019b), rendering reliance on knowledge of card and cardholder authentication values less effective at detecting fraudulent transactions. It is for these reasons and others that credit card fraud continues to rise (PCI Security Standards Council, 2018; Willey & B. J. White, 2013).

Credit Card Fraud

According to Prabowo (2011), common approaches to fighting credit card fraud fall into six categories: understanding, policy, awareness, technology, identity, and legal. Implementing controls in each of these areas requires commitment from all parties to the transaction, and innovative approaches that cannot be easily defeated or bypassed by the fraudster. Researchers agree that fraud should be a priority for all members of the transaction chain; by the consumer, the banking institutions, the card network, and the industry as a whole (Prabowo, 2011; Wilson, 2012).

Theft of credit card data continues to be the most prominent threat to retailers. Segal et al. (2011) and Moore and R. Anderson (2012) both suggested that the fundamental reason for increasing fraud is not due to technology limitations, but due to reduced economic incentives on banks and card networks to do their part to implement fraud control measures. Over the past decade, rashes of retail credit card data breaches have underscored this critical importance of data security. In November and December 2013, hackers were able to extract account data from 40 million payment cards using malware on Target Brands' computer systems; the following year similar attacks compromised 56 million payment cards from retailer Home Depot, as well as other major retailers including Nieman Marcus, Michaels, Goodwill Industries, SuperValu, and Staples (Simpson, 2016). In addition to retail, other sectors have reported high incidents of card breach, including the restaurant, hotel, service, finance, health care, and technology industries (Walters, 2014).

Advancements in credit card fraud detection, such as logistic regression techniques (Hussein et al., 2021), Bayesian analysis (Buonaguidi et al., 2021), and machine learning (Al Rubaie, 2021; Parashar & Bhati, 2020; Seera et al., 2021) improve chances of detecting these activities once the card data is lost; however, these measures are not yet sufficient to discourage credit card data thieves or ameliorate the corresponding cost to retailers. Data breach costs have increased steadily 10% year over year, and continue to carry significant direct and indirect costs, resulting in an average cost to retailers of $3.27 million per breach, or as much as $180 per record lost (IBM, 2021).

In addition to their costs, data breaches violate consumer trust, making customer acquisition and retention even more difficult. For instance, in 2014 Target Corporation reported a 2.5% loss of sales and $248 million in costs directly attributed to its 2013 data breach (Weiss & R. S. Miller, 2015). Other costs from compromised card data can include business disruption, productivity loss, non-compliance fines, incident response, forensic investigation, remediation, notification of affected parties, costs to reissue credit cards, credit monitoring for consumers, reputational damage, lost business, negative impact to share prices, and potential civil litigation (IBM, 2021; Simpson, 2016; Verizon, 2019b). The fraud impact to the industry because of these compromised records is estimated to be as high as $2.2 billion (Weiss & R. S. Miller, 2015).

In response to this recent rash of retail hacks, much of the U.S. retail industry has turned to chip card technology produced by Europay, Mastercard, and Visa, eponymously branded EMV (Gray & Ladig, 2015). Although the chip card performs cryptographic functions to authenticate the card used in the transaction, it does not encrypt all account data. Clear-text data transmission originating from a chip card transaction may still contain cardholder data such as PAN, cardholder name, and expiration date, and these data may still be used to perform fraudulent online transactions (El Madhoun et al., 2018). This trend is evidenced by the growth of e-commerce fraud in regions where EMV has been implemented. In the 8 years following the implementation of EMV in the UK in 2005, counterfeit and stolen card fraud dropped by half, while CNP fraud nearly doubled in size (Conroy, 2014). Following its adoption of EMV in 2015, the U.S. has reflected similar trends, with fraud comprising 19.66% of e-commerce transactions during the 2021 holiday shopping season (TransUnion, 2021).

PCI Compliance

Maintaining security over the transaction process is the most effective approach to mitigate risk, deter attackers, and reduce the prevalence of data breach (Cheney et al., 2012). Every day, retail merchants accepting credit cards must pass their customers' account information through their systems and on to the processor in order to conduct business. Other entities such as gateways, POS systems, e-commerce platforms, and processors may also depend upon this information, which allows them to execute the payment transactions. Today, a treasure trove of credit card information passes through these systems and networks and, if not secured, hackers may be able to obtain these data and perform fraudulent transactions. Therefore, preventing threat actors from accessing account data is the first step in preventing fraud. The Payment Card Industry Data Security Standard (PCI DSS) is the compliance framework that focuses on securing these data.

This standard was an outgrowth of the Visa Cardholder Information Security Program (CISP) released in 2004 as a joint effort by the five major card brands, Visa, Mastercard, Discover, American Express, and JCB, to enforce card security best practices throughout the retail industry (Clutterbuck, 2010). Today, merchants who accept credit cards from any of these brands are required to be compliant with PCI DSS (commonly referred to as being "PCI compliant"). To do so, merchants may employ the use of compliant third-party service providers to address certain controls on their behalf, or to provide software or systems that are already validated as compliant (PCI Security Standards Council, 2018).

To ensure security across the credit card ecosystem, the card brands require their acquirers to monitor and enforce their merchants are PCI compliant, who in turn may levy fees on non-compliant merchants to induce compliance (ControlScan, 2014). These card brands also provide the guidelines for merchant classification, which identifies the merchants that are required to undergo a third-party assessment each year from a qualified security assessor (PCI Security Standards Council, 2018). In this manner, PCI DSS is a form of industry self-regulation, enforced through contract rather than government regulation, requiring strong internal control of systems that handle these financial data.

The PCI SSC was established by the major card brands in 2006 to manage and maintain the nascent PCI DSS standard, including additional standards and programs that support merchant, hardware provider, software provider, and service provider compliance (Ataya, 2010). Among these additional standards are the Payment Application Data Security Standards (PA-DSS), Software Security Framework (SSF), Personal Identification Number Security (PIN), PIN Transaction Security (PTS), Point-to-Point Encryption (P2PE), and 3-Domain Secure Core Security (3DS). Each of these standards, as well as their accompanying programs and certifications, ultimately works together to support the merchant’s underlying need to protect consumer data and attain PCI DSS compliance, which remain at the root of the chartered purpose of the PCI SSC (Williams & Chuvakin, 2014).

Present research on compliance to the PCI DSS standard encompasses several areas important to data security and practical application of the standard. J. Rees (2012) pointed out some of the common issues that merchants encounter in becoming PCI compliant, such as limiting the scope of the environment and leveraging third parties for costly controls. Williams (2010) added detail to these recommendations, providing insight on how to reduce the scope of the merchant environment and complexity of certain PCI requirements by utilizing a tokenization solution for card data storage, or point-to-point encryption for card data transmission. Each of these cybersecurity investments may bring with them an improvement of internal control, as well as reducing overall cybersecurity risk.

Research into successful compliance programs has highlighted critical success factors such as understanding risk (Bhargav, 2014), and the use of a chief information security officer (CISO) to prioritize security and separate compliance tasks from the IT organization (Bhargav, 2014). ControlScan (2012) researchers have also used benchmarking analyses to compare merchant service providers and their merchants' PCI compliance, identifying a strong correlation between merchants' use of tools and technologies and the effectiveness of their PCI compliance program. As for dealing with unsuccessful merchant compliance practices, ControlScan (2014) proposed that merchant service providers and acquirers can reduce the incidence of non-compliant merchants by bundling these tools with education on security and risk.

Numerous studies have been performed to review the efficacy of the compliance requirements themselves at addressing identified risks. Stapleton and Poore (2011) explored the various ways in which PCI secure storage requirements may be met, and the relative complexity of each, including methods ranging from truncation, masking, hashing, tokenization, and encryption, with calculations showing the relative strengths of each. Other studies looking at the threat models and impacts of corporate mobile device usage provided direct support for many of the PCI DSS version 3.2.1 requirements (Saha

& Sanyal, 2015; Shihab & Misdianti, 2014). These outcomes include support for techniques based on specific PCI DSS requirements: application-level intrusion detection (Requirement 1.4), encryption at rest (Requirement 3), encryption in transit (Requirement 4.1), web-application firewalls (Requirement 6.6), and multi-factor authentication (Requirement 8.3). In each case study, the recommendations for use of these technologies derive from prescient warnings of potential and observed security threats.

Researchers have also evaluated ways merchants may improve efficiency in meeting certain requirements. Benchmarks of initial compliance assessments found that requirements related to passing empirical security tests of critical systems were by far the most difficult, with only 33% of merchants meeting all such compliance tests on the first pass (Verizon, 2015). Specific network and system configurations may also have intrinsic security challenges, making them more inefficient to secure without the aid of a PCI-compliant service provider, such as inspecting virtual architecture in a cloud environment (Rasheed, 2011), or protecting credit card information carried over voice-over-IP (VoIP) systems (Critchley, 2015). Studies addressing optimization of security investments for compliance have recommended the use of third-party technologies to aid in meeting PCI DSS compliance requirements, as well as providing other security and economic benefits including improved internal control of financial systems (J. Rees, 2012; Saha & Sanyal, 2015; Stapleton & Poore, 2011; Verizon, 2019b; Williams & Chuvakin, 2014).

Modeling Security Cost Drivers

The junction of decision theory and security costs is modeling predictive relationships that exist between measurable drivers and outcomes. Anand and Kodali

(2008) pointed out that myriad models exist for measuring and benchmarking security cost drivers; for instance, where measurement of competitor data presents a challenge, a model that focuses on easily attainable data (in their case, inputs), and direct correlation to the metrics being benchmarked (e.g., outputs) may be utilized (Björklund, 2010; Matthews & Lave, 2003). Similarly, Barretta (2008) recommended a model to control for cost drivers, as well as exclusion of indirect costs and standardization of cost-allocation methods to reduce "disturbing factors" that impede accurate measurement of efficiency in the benchmarking process. Some processes for obtaining cost data are more reliable or efficient than others, but the process for performing cost benchmarking comparison is not complicated (Krotov, 2016). To do so, an organization must identify a set of cost drivers, or independent variables that are directly correlated to cost, use these to predict benchmarking partners' costs, and comparing these to its own. Ideal cost drivers are straightforward, consistent from company to company, and easily accessible (Fifer, 1989).

Unfortunately, current cybersecurity budget benchmarks fail to accurately reflect industry spending, varying by as much as 300% depending on source (Boston Consulting Group, 2019), thus underscoring the remaining need for accurate cost models fit for the task. Once such a predictive model is formulated, it remains only to obtain data of adequate sample size (Kelley & Maxwell, 2003) and verify the model using a correlation or multiple regression analysis to explain the relationship between the cost driver(s) and measured cost (Keith, 2019). This regression formula is then used to predict the expected costs for both the anomalous organization and the exemplar benchmarking partner (based on their distinct cost drivers) and compare these calculated costs with actual measured costs (Dai et al., 2012). Research by Bikker et al. (2013) supported the use of a multivariate model derived from previously identified cost drivers to compare costs whenever inherent variances exist between measurements, thereby ensuring an accurate comparison of time series data or competitive benchmarks. Their model used weights assigned to each identified variable to reduce the impact of these variances between dissimilar periods, setting a precedent for normalization of cost data when performing benchmarking comparisons and selecting an appropriate security investment strategy.

Effective selection of security controls relies on nuanced understanding of efficient implementations of security best practices (Trustwave, 2019), efficient alignment with other security and governance requirements (Nicho & Fakhry, 2013), and calculating ROI for proposed security investments (Verizon, 2015). Models exist that explain the relationships between cybersecurity practice and economic impact and may be used by IT management to inform the decision-making process for allocating resources at the highest security benefit per dollar (Neuhaus & Plattner, 2013). Research has also suggested that, because of the variable nature of PCI compliance and the onerous manual efforts it requires, the industry may soon become more efficient using automated means of recognizing, verifying, delegating, and monitoring compliance-related tasks within an organization (Ghaisas et al., 2015). Such research aligns well with this current study, which share as their goal the desire to better understand retail traits that influence security investment, to assist regulatory bodies and stakeholders in their efforts to educate retailers on these perceptions where they may be misaligned to extant risks.

Independent and Dependent Variables

Many management drivers, including the desire for trustworthy financial reporting systems (Islam et al., 2018), the need to reduce risk of direct or indirect loss (Haapamäki & Sihvonen, 2019), or a means of distinguishing the organization within a competitive marketplace (Moore et al., 2015), may have incremental influence on cybersecurity expenditures. These correspond to the independent and dependent variables used in this study: internal control, cybersecurity risk, competitive advantage, and cybersecurity budget. In this section, I review works that made previous use of these concepts, relevant to their usage herein.

Internal Control

The first area to be associated with cybersecurity budget is that of regulation and governance. Industry self-regulation includes contractually-enforced security audit programs, such as PCI DSS and privacy controls—although the latter is moving under the auspices of regional government oversight through such laws as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Governmental regulations are responsible for significant levels of internal control, although their presence in retail is limited. Among these financial systems and information security regulations are Gramm-Leach-Bliley Act (GBLA), Sarbanes-Oxley Act (SOX), Health Insurance Portability and Accountability Act (HIPAA), and Occupational Safety and Health Administration regulations (OSHA), each requiring increasing internal control to meet control objectives and provide requisite reporting and audit support (Karthikeyan et al., 2019)

Identifying and mitigating risk across the enterprise is one of the principal roles of governance, along with internal control (Bukhvalov & Bukhvalova, 2011). In organizational management, the role of risk management may have limited representation, through technical security tools (Berry & Berry, 2018) or a deliberate manual process (Gibson, 2017). Canelón et al. (2020) defined internal control with respect to policies and procedures that ensure reliability of financial information for meeting compliance requirements, but technologies that protect the data assets themselves. Eaton et al. (2019) confirmed that, although firms have historically relied on accounting auditors to identify vulnerabilities in control systems that enforce internal control, cybersecurity controls are also effective at mitigating these risks even if these controls fall outside of the common financial regulatory frameworks.

Cybersecurity Risk

Although risk acceptance is one possible risk management decision, the most common course chosen for cybersecurity actions is to mitigate risks associated with potential financial losses. These losses may be direct, such as those costs incurred in the event of a data breach event (private costs), or they may be indirect, in the form of lost business due to spillover costs, such as the failure of an industry to protect consumers from these threats (externalities). Together private costs and externalities comprise social cost and thus aggregate cybersecurity risk (Gordon et al., 2018).

Private costs are those costs most often considered with relation to cybersecurity breaches: financial losses attributable to the event and affecting only the breached entity. Campbell et al. (2003) described these losses as measurable by stock prices among publicly traded corporations, offering this metric as a reasonable stand-in for actual losses where investors have perfect information about the actual impacts of the incident over a reasonable period of time. Conversely, Curtis et al. (2018) described internal corporate costs as including both financial losses as well as loss of consumer trust which coincides with perceived overconfidence and mismanagement of sensitive consumer data.

In contrast to private costs, externality costs are those losses that may be attributed to an incident, which are incurred by other members of the same industry. These costs, also called spillover costs, comprise loss of revenues associated with industry-wide loss of consumer confidence, distortions to available resources driven by increased market demands (Hassan & Mertens, 2017), or increased security investment outlays that may be loosely or directly attributable to heightened awareness resulting from high-profile events (Paul & Wang, 2019). Thaw (2014) also described an externality cost whereby regulatory agencies may tighten security controls as a result of such incidents, thereby incurring long-term spillover costs throughout an industry.

Other form of social cost is that of social harm, which Agrafiotis et al. (2016) describe as cybersecurity impacts beyond individuals, affecting social welfare and employment, whether as groups of individuals or as a society. In their model, Martin et al. (2017) depicted this social cost to individuals as an emotional violation and loss of cognitive trust; and within the industry, as spillover vulnerability to rival companies. The importance of effective cybersecurity to mitigate increasing social costs is addressed by Shackelford (2017), who argued cybersecurity is a consumer human right, and should be demanded of retailers from their consumers. Mulligan and Schneider (2011) go one step further and argue that cybersecurity is a public good much like public health, calling this principle of public cybersecurity the cybersecurity doctrine.

Competitive Advantage

Additionally, cybersecurity activities are often strategic in nature as a means of differentiation with the marketplace. Among decisions related to profit modeling, pricing, and performance evaluation, capital investments—including cybersecurity investment—form one of the most important organizational decisions afforded to management for use in strategic placement (Gordon, 2004).

Strategic decisions are generally performed at senior levels of organization leadership and have long term effects on an organization. Within the realm of information security, a common strategic decision is to position security above that of the competition (Barclay, 2014). This may take shape in the form of increased product security messaging, such as conveying protections on customer data (such as end-to-end encryption for communications or increased protections on consumer records), or as an impenetrable service offering itself (such as attestations of system testing, encryption strength, or security updates). A service offering may similarly be differentiated on security, where such services provide shareholders reassurance of strong security posture to prevent potential financial or market losses. Finally, an organization’s culture can be positioned as more attuned to security as a means of creating a compelling narrative by which any product, services, or relationship can be trusted to impart best practices related to threat detection and prevention. In each of these ways an organization can use cybersecurity as a competitive advantage in their respective marketplace, either to differentiate from competition or improve perceived value, thereby increasing revenues (Kosutic & Pigni, 2020).

Security has also been associated with other forms of competitive advantage, such as cost differentiation, although organizations may make ineffective use of this approach. A. M. Johnson (2009) identified 31 motivating factors for information security investment from business and security experts and concluded that business experts do not sufficiently consider how competitive advantage contributes as a driver of information security investment. Soltanizadeh et al. (2016) showed that use of enterprise risk management tools has been shown as a mediating variable, linking organizations with increased strategic focus on cost leadership to organization performance. Proactive cybersecurity defensive strategies also avoid risks, reducing cost and positioning companies for economic growth, an approach identified by Corallo et al. (2020) as an important part of an organization’s impact analysis for security initiatives.

Cybersecurity Budget

Cybersecurity budget is the total expected annual outlay allocated for capital expenditures related to mitigating cyber threats, and a common means of measuring security budget is as a function of revenue (Gordon et al., 2018). These operational expenses and capital investitures must balance competing needs for strong financial loss-prevention and protecting assets from cybersecurity threat with other company priorities such as service delivery, inventory, marketing, and profit (Ekelund & Iskoujina, 2019). Calculating and predicting a balanced cybersecurity budget is thus the subject of much research.

Gordon and Loeb (2002) initially published their works on calculating return on security investment by offering models that incorporated risk exposure, impact analysis, and investment cost to determine optimal security investment. Subsequent revision of the Gordon-Loeb model (Gordon & Loeb, 2006b; Sonnenreich et al., 2006) was confirmed by Baryshnikov (2012), demonstrating the legitimacy of Gordon and Loeb's rule, that the cost of all individual, independent actions taken by an organization to reduce risk cybersecurity risk should never exceed ~37% of the value of expected loss (a value derived by the calculation 1/*e*). In the absence of accurate predictions, this value may be seen as useful ratio for determining whether an organization is overinvesting in security. Other models for retail cybersecurity budget have used game theory models, which factor in budget constraints, and can delay implementation even if the investment is perceived as necessary (Nagurney et al., 2017).

Research Question

The research question for this study was: What relationships exist between internal control, cybersecurity risk, competitive advantage, and cybersecurity budgets among U.S. retail merchants? The challenge of understanding the reasons for underinvestment in cybersecurity across various industries necessitates a reliable survey instrumentation for modeling a firm's optimal investment (Gordon et al., 2015b), and exploring effects of regulation to increase investment (Gordon et al., 2015c).

In addressing a similar research question, Gordon et al. (2018) conducted a study of 158 senior executives sampled from among 1,600 private firms to determine how security perceptions such as internal control, cybersecurity risk, and competitive advantage may influence overall cybersecurity spending as a percentage of revenue. This research leveraged a validated and published survey instrument they introduced 3 years prior (Gordon et al., 2015a), and analyzed the resulting data using logistic regression analysis to quantify the associations between these organizational traits and corresponding budget allocation. This study not yet been independently confirmed, nor has its approach been applied to retail enterprises specifically. Having built upon the foundation of decision theory, real options theory, risk management, cybersecurity, and optimizing cybersecurity budget, these works provided a useful framework to model the relationships and provided justification for the purpose of this study.

Summary and Conclusion

In this chapter, I have reviewed in detail the literature that supports this study, beginning with real options theory, the decision theory that underpins this research and informs discussion of managerial actions related to cybersecurity investments. In addition, I have provided a thorough catalog of research that navigates the complex landscape from risk management as a managerial practice; to investment decisions related to retail cybersecurity; to compliance, risk, and competitive advantage as factors that influence investment. In this chapter I have also discussed the independent and dependent variables in further depth, aligning each to the survey instrument previously validated for use in collecting these sentiments and measuring their influence (Gordon et al., 2015a). In the following chapter, I will provide details on the full research methodology, including recruitment, survey, data collection, and statistical analysis for this research.

Chapter 3: Research Method

The research problem was that little was known about how organizational drivers of internal control, cybersecurity risk, and competitive advantage inform U.S. retail management decisions about cybersecurity budgets. Without a defined measurement approach, industry baseline, and predictive model, management may be unable to identify cultural norms or perceptions that lead to disparate investment related to mitigating enterprise cybersecurity risks. Furthermore, without these industry data, merchants may be unable to measure their investments with respect to similar organizations in the retail industry. The purpose of this nonexperimental quantitative correlational study was to describe the relationships between cybersecurity budget and management perceptions related to internal control, cybersecurity risk, and competitive advantage within U.S.-based retail merchant organizations.

In this chapter, I provide the step-by-step processes used to examine the independent variables as predictors of cybersecurity budget. This research methodology was intended to allow future researchers to verify the validity of the chosen methods and replicate this study to confirm the reliability of the proposed management model for predicting how organizational traits impact security investment decisions. I provide a review of the purpose of the study, the variables used in the study, and the relational model by which these variables were posited to interact. Justification for each methodological decision is included, as well as an objective review of threats to validity and ethical implications that were considered.

Research Design and Rationale

The research design was a quantitative nonexperimental correlational study including survey data collection administered via a web questionnaire to a random sample of retail merchants to obtain measurements of three independent company attributes and the dependent cybersecurity budget values. The quantitative survey instrument that was used to obtain these data was introduced by Gordon et al. (See 2015a). The instrument had been operationalized for measurement of these variables and was used in its unaltered form in the current study. Upon confirming the normality of the observed residuals, I analyzed these data to test a proposed predictive model of retail merchant internal control, cybersecurity risk, and competitive advantage as determinants of cybersecurity budget using multiple linear regression instead of logistic regression, the analysis tool proposed by Gordon et al. (2018).

Multiple linear regression is useful for confirming relationships between variables in models in which one continuous outcome variable may be predicted by two or more continuous explanatory variables, as predicted via a single equation (J. Cohen, 1968; J. Myers, 2019). All independent variables within the model were operationalized as responses to individual survey questions, each measured on a Likert scale and represented as ordinal values. By transforming the value from these responses, I operationalized the dependent variable as the median value from each of the seven possible value ranges representing the percentage of information technology budget allocated for cybersecurity expenditures. This normally distributed variable was then treated as an ordinal continuous value. For these reasons, this data analytic approach was appropriate for this study. The posited relationship between these variables is illustrated in Figure 1, showing the direct predictive relationship between each of these three independent variables to the single dependent variable (Table 1).

Figure 1

Modeled Relationship Between Variables

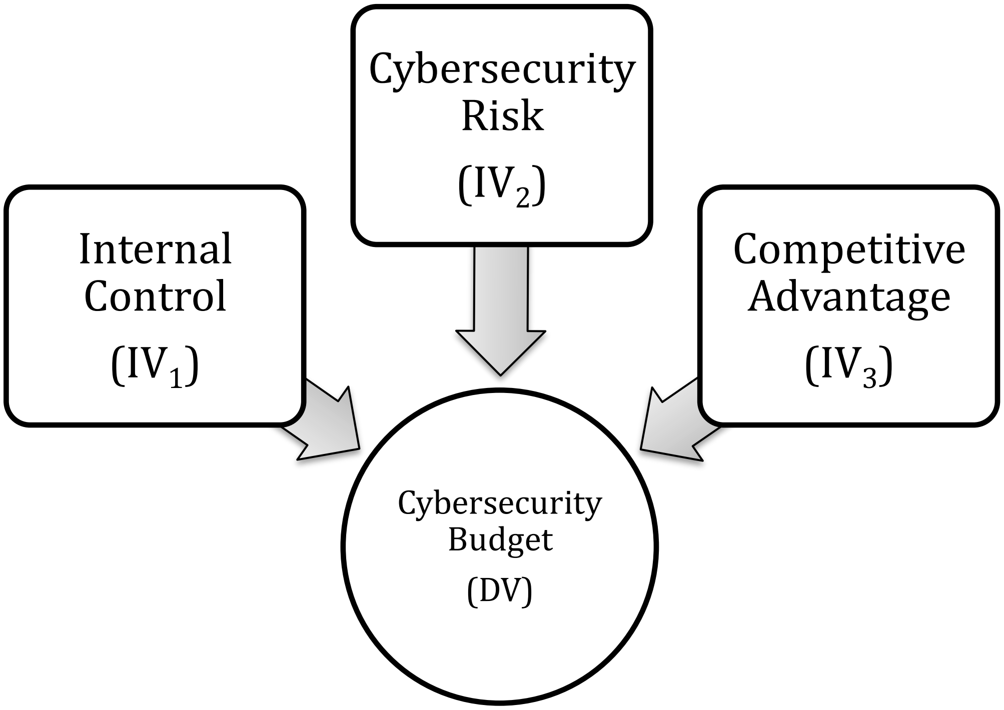


Table 1

Variables

Variable name	Variable type	Variable code	Data type
Cybersecurity budget	Dependent (DV)	CB	Ordinal (continuous)
Internal control	Independent (IV_1)	IC	Ordinal
Cybersecurity risk	Independent (IV_2)	CR	Ordinal
Competitive advantage	Independent (IV_3)	CA	Ordinal

The dependent variable of cybersecurity budget was defined as the percentage of the respondent company’s annual budget allocated to cybersecurity capital investment and operational expenditures as a function of overall information technology budget. The independent variable of internal control (IC) was defined as the degree to which the respondent organization had expected benefits from cybersecurity expenditures associated with its need for reliable financial reports driven by the need for cybersecurity controls around an organization’s financial accounting systems, whether by strong internal management or in response to regulatory requirements. The independent variable of cybersecurity risk (CR) was defined as the degree to which the respondent organization had expected benefits from cybersecurity expenditures associated with identified impacts of a significant data security incident, calculated based on financial losses including both private costs and externality costs. The independent variable of competitive advantage (CA) was defined as the degree to which the respondent organization had expected benefits from cybersecurity expenditures associated with benefits received from the market based on its perceived cybersecurity posture.

To confirm the proposed model, statistical analysis needed to demonstrate that, given a merchant profile consisting of all three independent perceptions taken together, a relationship existed by which management should be able to better predict the annual cybersecurity budget for that organization. That is, by regressing the cybersecurity budget as a percentage of IT budget on the merchant attitudes related to influence of internal control, cybersecurity risk, and competitive advantage, any variance in budget may be explained by corresponding changes in these other three factors as demonstrated by the proposed model.

Methodology

The methodology for this study was a nonexperimental quantitative internet-based approach including email-based recruitment to solicit respondents from a database of contacts constituting a sampling frame of random contacts within the population of U.S. retail merchants. Enrollment of respondents and informed consent took place online, and data collection was performed via reputable survey platforms using an existing survey instrument.

Population

The population of this study was private-sector store and nonstore retail merchants based in the United States. Nonretail private-sector industries, public sector organizations, and entities based outside of the United States may be able to obtain value from the concepts and principles found in this research, but baseline costs and attributable impacts may not be consistent to these organizations because they were omitted from the population and sampling frame. Generalizability of results outside of the identified population is discussed in Chapter 5.

According to the U.S. Census Bureau (2021), retail organizations are establishments that self-report under the North American Industry Classification System (NAICS) as “Retail Trade” (NAICS Codes 44 or 45). Recent calculations indicated that there are between 1,050,175 (U.S. Census Bureau, 2021) and 1,818,112 (NAICS Association, 2022) retail establishments in the United States ($\bar{x}$ = 1,434,143, n = 2).

Furthermore, for purposes of identifying those organizations whose cybersecurity requirements are subject to regulation under PCI DSS, merchants shall also be defined according to the definition provided by the PCI SSC as “any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services” (PCI Security Standards Council, 2016, p. 11). This additional descriptor will ensure that cash-only retailers are excluded from the population, minimizing the possibility of data skew that could occur from the disparate regulatory requirements imposed on those who accept credit cards from those who do not.

Sampling and Sampling Procedure

Two sampling approaches were taken to obtain sufficient responses from the target population. Both approaches included email-based recruitment. In the initial approach, I recruited directly from a dataset of contacts purchased from Data Axle, and respondents completed the survey on the SoGoSurvey platform. In the subsequent approach, I used a third-party recruitment service from Momentive called SurveyMonkey Audience, and respondents completed the survey on the SurveyMonkey platform. When procedural variations occurred, these are noted as “initial” and “subsequent” throughout the study.

Sampling Frame

The initial sampling frame consisted of 20,000 U.S. companies identified based on their classification as “Retail Trade” based on self-reported NAICS (Codes 44 or 45) on recent census and/or business registration documents selected randomly from a database of U.S.-based businesses collected and maintained by the data source provider, Data Axle. Criteria for inclusion in this sample frame included the known presence of a senior-level contact (owner, president, executive director, principal, partner, chairman, board member, chief executive officer (CEO), chief operating officer (COO), chief financial officer (CFO), treasurer, controller, IT executive, operations executive, executive officer, IT, chief information officer (CIO)/chief technical officer (CTO), chief administrative officer, or executive) with a name and email address. Data Axle has confirmed that the dataset matches these criteria, including NAICS code, revenue, and title as output fields. Data Axle maintains its database through active research of U.S.-based organizations and selects based on specified criteria, narrowing the record subset using a systematic random sampling process to maximize internal and external validity from the available pool (Data Axle, 2020). Organizations belonging to retail types that do not commonly accept credit cards (automobile and other motor vehicle dealers) and contacts that have requested to be removed from the database were excluded from the initial sampling frame. The subsequent sampling frame comprised individuals selected from the Momentive subscriber pool matching the following demographics, which aligned to the criteria used for the initial sampling frame:

- country: United States;
- industry: retail and consumer durables;
- job function: management; and
- job level: owner/executive/C-level, senior management, middle management, intermediate.

Data Set

For the initial recruitment procedure, I purchased a 20,000-record data set from Data Axle (formerly InfoUSA) matching the stated criteria for $3,960.00 on January 29, 2016. The data set included company name, contact name, title, and email address, and was based on all selection criteria. These records represented organizations gathered by Data Axle from numerous data sources and were confirmed to be up to date at the time of purchase, thereby improving the likelihood that the recruiting procedure would result in a random sample from within the target population (see Data Axle, 2020). Due to the age of the data (5 years at the time of its use), analysis was performed to estimate the number of valid organizations and contacts, thereby providing confidence that this data set would support the minimum sample size.

Business closures naturally and proportionally reduced the number of organizations in the data set. The mean number of retail store closures in the United States was 14,187 per year for calendar years 2017–2019 (*n* = 3; Statista, 2020). With the ongoing COVID-19 pandemic, it was difficult to predict store closures for 2020 at that time; however, estimates placed this number between 7,500 and 12,000 (H. Peterson, 2020) and between 20,000 and 25,000 ($\bar{x}$ = 16,125; *n* = 4; Statista, 2020). Extrapolating from these values, I projected that 5.0% of the organizations in the data set would no longer be in business when recruitment began:

$$\frac{(14{,}187 \times 4) + (16{,}125)}{1{,}444{,}184} = 5.0\% \qquad (1)$$

In addition, random and proportional attrition of management contacts would have reduced the number of active contacts within this data set (S. L. Peterson, 2007).

Management attrition ranged between 25% and 30% between 2016 and 2020 (Work Institute, 2019; $\bar{x}$ = 27.5%, n = 2). At these rates, it was estimated that the existing records would result in 3,805 valid records:

$$(20{,}000) \times (100\% - 5.0\%) \times (100\% - 27.5\%)^5 = 3{,}805 \qquad (2)$$

Common response rates for a survey of this size, estimated by Gordon et al. (2015a) to take no longer than 20 minutes to complete, were expected to receive a response rate of approximately 24.5% (Galesic & Bosnjak, 2009). Among those with valid information, I expected to receive responses from approximately 932 respondents, which was deemed more than sufficient to meet the minimum sample size based on the power analysis:

$$n = 3{,}805 \times 24.5\% = 932 \qquad (3)$$

In the original use of the instrument among major corporations in the U.S. critical infrastructure industry, Gordon et al. (2015a) achieved a 10% response rate. This would have been sufficient for the current study; however, I anticipated less resistance among the desired respondents from the target population of all retail organizations, which should have resulted in a response rate more consistent with that found by Galesic and Bosnjak (2009).

For the subsequent recruitment approach, the data set was maintained by Momentive and comprised more than 144 million contacts in at least 130 countries, each identified by 50 attributes that may be selected for incentivized participation (Momentive, 2021c). Respondents are incentivized for their participation by directing a small donation from Momentive of 50 cents to the charity of their choice (Momentive, 2021a). For this paid recruitment procedure, I purchased a one-time survey response campaign with a target of 60 responses from Momentive (formerly SurveyMonkey) matching these criteria for $1,540.00 on August 3, 2021. No data set was provided, and all respondents' identities were kept anonymous; however, Momentive confirmed through independent validation that the respondent cohort may be considered a quality selection with a strong satisficing likelihood from the target population based on the campaign criteria (Momentive, 2021a, 2021d).

Groups

Neither the population nor respondents were divided or assigned into any groups. When demographic information was collected within the survey (Questions A–D), these data were used for review of participant demographics and post hoc analysis and discussion of results' generalizability.

Power Analysis

For this multiple regression analysis, a priori power analysis and sample size estimation were performed using estimated f^2 and calculated using effect size for multiple regression analysis using the calculator provided by Soper (2021) leveraging power analysis methodology proposed by J. Cohen (1968).

A priori sample size calculations were performed using power analysis based on multiple linear regression analysis with three predictors and assumed results consistent with those reported by Gordon et al. (2018). Gordon et al. (2018) did not disclose goodness of fit, but since all alternative hypotheses were deemed to be supported at $p < .10$ it was reasonable to assume a significance level of $\alpha = .10$. For this reason, I assumed a modest R^2 value of 0.2, resulting in a relatively low effect size, $f^2 = 0.25$:

$$f^2 = \frac{R^2}{1-R^2} = \frac{(0.2)}{1-(0.2)} = 0.25 \tag{4}$$

Using this forecasted minimum effect size with a statistical power of 0.9 and alpha level of α = .05, I calculated a target sample size of *n* = 61 (Soper, 2021).

Procedures for Recruitment, Participation, and Data Collection (Primary Data)

Participant Selection

All participants in the initial and subsequent recruitments were selected using email recruitment methods. Contacts with management job roles were targeted for recruitment to increase likelihood of knowledge of cost and compliance initiatives; however, respondents' role selection was not a condition for inclusion or exclusion. The default roles contained within the initial sampling dataset include titles such as owner, CEO, CIO/CTO, CISO, as well as middle management positions that commonly support the ongoing information technology and cybersecurity effort (e.g., IT director, compliance manager, credit card / payments manager). The subsequent recruitment allowed for identification of candidates based on general management job function as well as job role matching intermediate to senior management level, matching the selection criteria of the initial recruitment.

The procedures for initial recruitment included sending an initial email to the sampling frame using the Walden email system and the email distribution system provided by the Momentive survey platform, followed by periodic reminder emails until sufficient responses are received. Email recipients were informed that survey responses were de-identified by the survey platform to protect participant confidentiality from the researcher and were provided a link to continue enrollment.

Website

In the initial recruitment approach each email-solicited response included a link to www.costofsecurity.com. I registered the costofsecurity.com domain name with a reputable domain name registrar and published a small website using SquareSpace. There, I displayed approved language informing visitors of my identity and credentials, the purpose of the current study, time commitments, risks, criteria, the voluntary nature of participation, and provided access to all necessary privacy and confidentiality disclosures. Given the sensitivity of disclosing financial and security information and my lack of relationship with the initial respondents, I considered it important that the confidentiality disclosure be plainly worded and clearly visible and that the respondent be immediately aware that no personally identifiable information would be obtained. This served to legitimize the current study and assuage any concerns of privacy or length of commitment. It also provided a memorable website address for those who may be unable to complete the survey in a single sitting, leveraging the continuation feature offered by SoGoSurvey using a cookie placed on the respondent’s computer.

The subsequent recruitment approach was fully handled by the SurveyMonkey Audience platform, including reassurances of legitimacy, privacy, and suitable incentivization (Momentive, 2021b). Considering the existing trust relationship established by Momentive with its Audience response pool, and conditions of the SurveyMonkey Audience survey platform, respondents were taken directly to the online questionnaire, bypassing the costofsecurity.com microsite.

Enrollment

For both recruitment approaches, all who responded to the email by clicking the provided link were taken to the survey containing the full text of the IRB-approved informed consent verbiage, acceptance of which was a programmatic condition for proceeding. This approach ensured permission was received from each respondent by requiring them to check “I agree, and wish to participate in this study” before becoming a participant in the study. A response of “I do not agree, or do not wish to participate in this study” ended the process immediately. Upon viewing the electronic consent, choosing to enroll from the website, and answering the qualification questions, the respondent was then able to complete the survey.

Protection of Participants

No vulnerable populations were targeted by the recruitment methods to be used in this research or expected to be disproportionally represented within the sampling pool of retail business leaders, although it is likely that some respondents were members of vulnerable communities. Because any such recruitment and participation by vulnerable populations (e.g., economically disadvantaged, non-English speakers) is purely by chance, risk was therefore minimal and no additional protection methods were required for protection of such populations. However, due to the sensitive data obtained related to enterprise security investment, additional procedures were put into place to proactively protect these data. All response data were entered directly into the online questionnaires provided by the SoGoSurvey (initial) or SurveyMonkey (subsequent) platforms, which offered secure entry and anonymity. The initial platform ensured this anonymity by unlinking responses from any identifying information to which the researcher is given access (SoGoSurvey, 2021). The subsequent platform was configured to protect respondent identities by use of anonymous data collector (Momentive, 2021b). Data retrieval was performed only over secure HTTPS/TLS 1.2 connection to protect security of the data in transit between the platforms and the researcher. Analysis was performed only on the researcher’s computer using locally installed IBM® SPSS® Statistics v27 statistical analysis software and all results were reported in summary form to prevent accidental disclosure of any identifiable information.

Obtaining budget data related to cybersecurity investments may have been met with some resistance, especially from security-aware respondents who may have been skeptical of emails requesting sensitive information. Extra effort was therefore invested to reassure respondents of the validity of the researcher, the research, and the controls in place to protect response data.

Respondents from the initial recruitment approach who chose to exit, either by completion of the survey or by canceling the survey, were immediately taken to a page on the www.costofsecurity.com website informing them that their participation has concluded and allowing them to request a copy of the final dissertation or contact the Walden IRB with any concerns about the ethics of the current study or researcher. Contact information obtained from this form was not linked to any value or metadata of the survey response (i.e., completion status, time, date, internet protocol address), thereby providing assurance of anonymity.

As part of the initial recruitment approach, each email included my full name and security certifications, each of which carries a code of ethics (ISC2, 2020), codes of professional ethics (ISACA, 2020), or codes of professional responsibility (PCI Security Standards Council, 2014)). The website created at www.costofsecurity.com included a posted privacy policy and contact information for the Walden University Institutional Review Board. The emails, website, and informed consent also explained the SoGoSurvey guaranteed anonymity feature and other procedures used to protect the respondent and their data. The subsequent recruitment did not allow for such verbal reassurances; however, the appropriate IRB and researcher contact information was included within the approved informed consent verbiage.

Data Collection

The data collection process was facilitated through an internet-based questionnaire. Upon collection of the minimum number of responses the data, was downloaded to the researcher’s personal computer and maintained securely on an encrypted disk volume while it was analyzed using IBM® SPSS$^{®}$ Statistics v27. After analysis, the anonymized data was encrypted within a compressed file and will be stored securely in a personal Dropbox file repository for 3 years, at which time it will be permanently deleted from all locations in accordance with Walden University retention policies.

Survey Administration

For those who chose to enroll, completion of a short online survey was required, based on the existing instrument introduced by Gordon et al. (2015a), which has been reviewed for validity and reliability for collection of the data described. In its original use, the survey was estimated to take “no longer than 20 minutes to complete” (Gordon et al., 2015a, p. 118). This survey was administered through an online questionnaire platform provided by SoGoSurvey and SurveyMonkey, two reputable online survey systems. After receiving the email sent to the list of pre-qualified executives from retail organizations, the respondent was asked to review the informed consent and confirm membership in the population before being allowed to enroll.

Upon enrollment, the respondent completed a web-based version of the Department of Homeland Security (DHS) Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector survey instrument (Gordon et al., 2015a). This survey administered by the SoGoSurvey and SurveyMonkey platforms included participant protections such as transport layer security (TLS) encryption and respondent anonymity controls to ensure privacy and confidentiality. Each question was transcribed to the respective survey platform verbatim, matching the layout, language, and workflow as described by Gordon et al. (2015a) to preserve the tested validity and reliability of the original instrument.

Upon completion of the survey, the respondent was returned to a “thank you” page—either on www.costofsecurity.com or on www.surveymonkey.com—informing them that their participation has concluded. No follow-up was performed.

Instrumentation and Operationalization of Constructs

The instrumentation for this study was the Department of Homeland Security (DHS) Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector survey (Gordon et al., 2015a). Preliminary approval for use of this instrument was obtained from its authors (L. Gordon, M. Loeb, W. Lucyshyn, & L. Zhou, personal communication, January 2, 2020; see Appendix C), conditional only IRB approval which was subsequently obtained. The contents of the instrument may be found in its entirety within Appendix D.

As part of the original publication of this instrument for the U.S. Department of Homeland Security, Gordon et al. conducted a pilot study to ensure the instrument's reliability and validity, including "appropriate" revisions to incorporate feedback from that study (2015a, p. 117), which involved review by five executives with experience in related cybersecurity matters (Gordon et al., 2018). No specific reliability or validity values were shared.

The instrument has been used in previous research to describe challenges among CFOs and CIOs of organizations within industries focused on U.S. national infrastructure (*n* = 171; Gordon et al., 2015a), and again to analyze the degree to which each of these determinants impacts the corresponding security budget (*n* = 158; Gordon et al., 2018). The latter results were statistically significant ($p < .10$), confirming face validity of the instrument for the construct and variables it was intended to measure.

Operationalization of Variables

The variables to be used in this current study were operationalized by the following responses received by the survey instrument:

Internal Control

This variable, IC, was operationalized as the response to question F-16: “F. For the following set of statements, indicate your level of agreement/disagreement by circling the number provided to the right of the statement. All answers should be in the context of the organization in which you work.” “16. Cybersecurity is an important component of my organization’s approach to the internal controls of financial reporting systems.”

The value of the response was selected from a Likert scale ranging from 1 to 7, denoting agreement from “strongly disagree” to “strongly agree”. For example, if a respondent had chosen “1”, this variable would have been assigned the value of 1, which represents the respondent’s strong disagreement with the statement that “cybersecurity is an important component of my organization’s approach to the internal controls of financial reporting systems.” This variable was treated as an ordinal value.

Cybersecurity Risk

This variable, CR, was operationalized as the response to question F-18: “F. For the following set of statements, indicate your level of agreement/disagreement by circling the number provided to the right of the statement. All answers should be in the context of the organization in which you work.” “18. In determining the risk associated with cybersecurity breaches, my organization considers the largest potential loss.”

The value of each response was selected from a Likert scale ranging from 1 to 7, denoting agreement from “strongly disagree” to “strongly agree”. For example, if a respondent had chosen “6” for F-17, this variable would have been assigned the value of 6, which represents that the respondent somewhat agrees that decisions regarding cybersecurity expenditures are based expected value from loss. This variable was treated as an ordinal value.

Competitive Advantage

This variable, CA, was operationalized as the response to question F-4: “F. For the following set of statements, indicate your level of agreement/disagreement by circling the number provided to the right of the statement. All answers should be in the context of the organization in which you work.” “4. The expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization.”

The value of the response was selected from a Likert scale ranging from 1 to 7, denoting agreement from “strongly disagree” to “strongly agree”. For example, if a respondent had chosen “7”, this variable would have been assigned the value of 7, which represents the respondent’s strong agreement with the statement that the expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization.” This variable was treated as an ordinal value.

Cybersecurity Budget

This variable, CB, was operationalized as the interpolated median value within the ranged response to question E: “E. Approximately what portion of your firm’s IT budget is devoted to cybersecurity related activities (circle the correct answer)? 1-2%, 3-5%, 6-8%, 9-11%. 12-15%, 16-20%, Greater than 20%”

For example, if a respondent had chosen “6-8%”, this variable would have been transformed to the value “7%”, because this is the median value within this range. No responses of “Greater than 20%” were obtained, therefore all transformed values were discrete. During preliminary data analysis, the ordinal values for this variable were plotted to evaluate the distribution between the ranges, and if sufficiently normal, were to be treated as an ordinal continuous outcome value for primary analysis using multiple regression (D. R. Johnson & Creech, 1983; Snijders & Bosker, 2011).

Data Analysis Plan

The data informed analysis for the research question and hypotheses each pertain to the proposed model that explains allocation of cybersecurity budget based on an organization’s internal control, cybersecurity risk, and competitive advantage:

RQ: What relationships exists between internal control, cybersecurity risk, competitive advantage, and cybersecurity budgets among U.S. retail merchants?

H_0: There is no relationship between the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = \beta_2 = \beta_3 = 0$.

H_a: At least one of the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) are useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants (DV): At least one of these inequalities is true $\beta_1 \neq 0$, $\beta_2 \neq 0$, $\beta_3 \neq 0$.

$H_0$1: There is no relationship between the independent variable of internal control (IV_1) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = 0$.

H_a1: The independent variable of internal control (IV_1) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_1 \neq 0$.

$H_0$2: There is no relationship between the independent variable of cybersecurity risk (IV_2) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_2 = 0$.

H_a2: The independent variable of cybersecurity risk (IV_2) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_2 \neq 0$.

$H_0$3: There is no relationship between the independent variable of competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_3 = 0$.

H_a3: The independent variable of competitive advantage (IV_3) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_3 \neq 0$.

To support this analysis, the data analysis was performed as follows:

Data Cleaning

Upon conclusion of the data collection phase, the data were exported from SoGoSurvey and SurveyMonkey as CSV files, which were then transformed and imported into IBM® SPSS$^{®}$ Statistics v27. Each of the three independent variables were tested for normal distribution. These values were thus represented as continuous values so that analysis of these data could be performed using multiple regression, and to support data cleaning activities.

Outliers were considered for removal by performing a scatter plot of each of the independent variables against the dependent variable and observing data points. The aggregate results of the survey were then checked for common sources of error such as multicollinearity, heteroscedasticity of residuals, and the existence of any unidentified external variables before being analyzed for the existence of correlations among the variables within the model. The data were also checked for autocorrelation and normal distribution to ensure appropriate fit of collected data to the model, and appropriate use of the chosen parametric statistical analysis methodology. Other than the conversion of cybersecurity budget category into ordinal continuous integer values for multiple regression analysis, no other data transformations were necessary.

Descriptive Statistics

Before performing detailed analysis and hypothesis testing, a review of descriptive statistics provided a valuable cross-section of the retail industry that may aid merchants seeking to conduct benchmark analysis of its own cybersecurity budgets against those found within this industry data set (Pham Evans et al., 2012; Stapenhurst, 2009). The regression equation generated from the resulting model demonstrates how the outcome response changes with respect to these three predictor variables. Furthermore, the coefficient of determination (R^2) and individual weights were tested for statistical significance to ensure the research question was answered with a higher degree of confidence.

Hypothesis Testing

I then evaluated the omnibus hypothesis (H_0) to test the existence of a relationship between the three predictors (independent variables) and the outcome (dependent variable). After first confirming the assumptions of normality, absence of multicollinearity, absence of autocorrelation, and homoscedasticity of residuals, the data were tested using multiple linear regression analysis, resulting in values for the intercept constant ($\beta_{0)}$), variable coefficients ($\beta_1, \beta_2, \beta_3$) for the following regression formula, with ε representing the error in the predicted model (D. R. Johnson & Creech, 1983; Snijders & Bosker, 2011):

$$\mathrm{CB} = \beta_0 + \beta_1\mathrm{IC} + \beta_2\mathrm{CR} + \beta_3\mathrm{CA} + \varepsilon \tag{5}$$

The coefficients table from the regression analysis were reviewed for intuitive unstandardized coefficients (signifying at least some portion of CB as being explained by one or more of IC, CR, and CA), with α = .05. Additionally, I performed an analysis of variance (ANOVA) between the observed model and evaluated the F-statistic to confirm the model fit to the observed data. To reject the omnibus null hypothesis, these conditions were to have been met by at least one coefficient.

Post Hoc Analysis

After performing the omnibus hypothesis test and confirming the significance of the finding using the ANOVA F-test, post-hoc analysis was performed to evaluate each of the individual hypotheses (H_01, H_02, H_03), testing for the existence of individual relationships as possible sources of difference within the model. This approach provided insight into how and to what degree each individual predictor (IC, CR, and CA) contributed to the outcome of cybersecurity budget (CB).

Threats to Validity

External Validity

The degree to which the results of this current study may be generalized to other U.S.-based retail merchants for identifying determinants of cybersecurity budget depends greatly on the statistical significance of the resulting regression coefficients, introduction of selection or response biases, and the ability for researchers to replicate the study.

The strength of the outcomes of the statistical analysis are subject to the suitability of the proposed regression model for describing the relationship of cybersecurity budgets (as a function of total information technology allocation), and are largely dependent upon aspects of internal control, cybersecurity risk, and/or competitive advantage. Insufficient statistical power as observed by analysis of the data collected within this current study would threaten the external validity of these results and the explanatory power of the proposed model.

In addition, it is possible for external validity to be threatened by biases which may enter the process due to the age of the initial recruitment dataset being used. It was my assumption that errors would enter the dataset randomly and proportionally to all other traits (that is, larger organizations are equally as likely to go out of business as smaller companies; employees are equally likely to attrite from companies located in the Western United States as they are from companies in the Midwest). Where this assumption may have been incorrect, selection bias may have been possible, skewing responses towards companies with less turnover, or company staying power. Where sufficient responses were obtained to ensure statistical significance, this bias may have been minimized. Furthermore, this bias is acknowledged as a potential threat to external validity and discussed in Chapter 5.

Finally, the replicability of this study also depended on the rigor of the research design and administration. Within the research methodology section, numerous controls were detailed to ensure that the recruitment, enrollment, and data collection were clearly defined and replicable. These controls, specifying population attributes, dataset criteria, email recruitment, website enrollment, and survey completion may have aided in facilitating replication of this study.

Internal Validity

This research was based on a non-experimental design and was thus subject to fewer issues of internal validity that might otherwise have arisen during test-retest or interventional studies or experimental designs. The instrument and the administration of the survey thus comprised the greatest threats to internal validity.

Although validity coefficients were not provided for this instrument, Gordon et al. (2015a) have attested to its validity. Instrument validity for this intended use could have been assessed in several ways, including content, response process, relationships to other variables, and consequences (Sullivan, 2011). Similarly, response validity was confirmed by adding a single question after the end of the survey requesting “feedback, suggestions, or issues you had from completing this survey,” the responses to which demonstrated that respondents understood the questions and felt their responses were accurately recorded.

As with validity coefficients, no reliability coefficients were available for this instrument. DeVon et al. (2007) identifies two tests necessary to measure the reliability of an instrument: stability and equivalence. Stability reliability testing is generally performed during field and pilot testing, where field test panelists may raise concerns about inter-rater reliability, or consistency in measurement from one self-reporting participant to the next. A moderately-high coefficient of determination from the current study's resulting analysis ($R^2 > .75$) serves as a reasonable confirmation of the stability of the instrument to consistently capture organizational traits between diverse participants and survey administration method. Equivalence reliability was not applicable for this instrument, as no two values within the instrument measured the same construct.

Construct Validity

Construct validity is the accuracy with which a construct is empirically measured, that is, how well the operationalizations of the identified variables measure the underlying concepts of internal control, cybersecurity risk, competitive advantage, and cybersecurity budgets. This threat was minimized by using the instrument and variable definition that had already undergone multiple use (Gordon et al., 2015a, 2018), peer review, and journal publication.

Ethical Procedures

The second Belmont principle of beneficence dictates that all risks and benefits be identified to the respondents, and that these risks justify the research (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 1979). The nature of this research required that financial information be gathered (gross revenue and cybersecurity budget), which represented a minimal financial or commercial risk to some potential respondents. Disclosing financial information can be a concern, and thus it was important that respondents received reassurance that these data were to be treated with the utmost confidentiality. Confidentiality was addressed by utilizing TLS 1.2 for the survey submission itself (Witte et al., 2000), and removing all identifiers via the certified anonymity and anonymous data collector functions available on the respective survey platforms (Momentive, 2021b; SoGoSurvey, 2021).

Another source of risk was the potential for inadvertent breach of confidentiality due to indirect identification of respondents. This risk was communicated within the informed consent, including mitigation efforts such as ensuring all responses are aggregated and presented in summary form within the discussion of actual responses. No certificate of confidentiality was required because the respondents were not in physical or financial harm where this data may have caused identification to occur within the context of compulsory data release due to civil or criminal investigation.

The research proposal was reviewed and approved by the Walden University dissertation chair, dissertation committee, and university research reviewer for research design and methodology in conjunction with compliance to the university’s prescribed dissertation process. Approval was obtained from the Institutional Review Board (IRB) considering research ethics and scientific merit prior to collection of data (approval number 05-05-21-0998178). Two additional data collection modifications were subsequently submitted and approved by IRB before reaching a sufficient number of responses.

Summary

The research design for this current study supported a thorough research methodology. The population accurately represented the U.S. retail merchant industry, an audience whose membership may benefit from the outcomes proposed herein. The sampling procedures were appropriate for the data collection approach, and adequate to ensure sufficient sample size for statistically significant results. The data collection approach included email recruitment, website enrollment, and platform-based survey administration, reflecting a thorough and professional design suitable for the desired audience. The use of an existing survey instrument ensured valid operationalization of the variables necessary to test the proposed regression model. Finally, the data analysis techniques including descriptive, evaluative, and post-hoc statistical tests ensured that the research question and hypotheses were fully tested, providing insight for discussion and future research. In the next chapter, I include the results of the data collection and detailed analysis of the findings.

Chapter 4: Results

The purpose of this nonexperimental quantitative study was to describe the relationships between cybersecurity budget and management perceptions related to internal control, cybersecurity risk, and competitive advantage within U.S.-based retail merchant organizations. The goal of this research was to help business leaders, compliance managers, and security administrators better understand what relationships exist between internal control, cybersecurity risk, competitive advantage, and cybersecurity budget, enabling them to evaluate more reliably the prioritization of investment in cybersecurity initiatives using real cost theory and decision analytics. I tested whether at least one of the independent variables of internal control (IC), cybersecurity risk (CR), and competitive advantage (CA) were useful in explaining and/or predicting cybersecurity budgets (CB) among U.S. retail merchants.

This chapter is divided into two sections. Data collection contains a description of the process by which data were obtained, including timeline, recruitment, and response rates. I also describe the size, power analysis, demographics, central tendency, and other descriptive statistics of the population sampled. In the second section, study results are presented, including the outcomes of the hypothesis testing, confirmation of assumptions, probability values and confidence intervals for each statistic used, effect size of each relationship as empirically observed, and the acceptance or rejection of each null hypothesis.

Data Collection

Upon receipt of IRB approval, I commenced data collection by sending initial 20,000 recruitment emails, followed by multiple rounds of reminder emails over the course of 5 weeks. The initial data collection resulted in 30 usable responses. Over the ensuing 6 weeks, two IRB amendments were submitted due to insufficient responses to the initial approach, resulting in approval to perform the subsequent paid recruitment using SurveyMonkey Audience. This subsequent approach resulted in 72 additional responses in 1 week's time. In all, data collection required 12 weeks to complete, resulting in 66 valid and usable responses, which included acceptance of the informed consent and a response for the dependent variable (CB) and at least one of the three independent variables (IC, CR, or CA).

During the data analysis for the individual hypotheses, cases were excluded listwise due to the omission of the tested dependent variables, resulting in analyses being run only on cases with complete sets of data relative to the variables evaluated ($H_0$1 n = 61, $H_0$2 n = 61, and $H_0$3 n = 63). Similarly, for evaluation of the omnibus hypothesis, 54 cases provided responses including all four variables in the regression model. When I reviewed descriptive statistics related to these variables, the number of cases was also affected due to the necessary listwise exclusion of cases lacking response for the respective variables. No discrepancies in the data collection occurred from the research plan as amended and approved by the committee and IRB.

Study Results

In this section, I review the descriptive characteristics of the sample related to the population of retail merchants, evaluate the statistical assumptions for use of the statistical analysis techniques, and review the procedures and outcomes by which the four hypotheses were tested using multiple linear regression. In addition, the results are provided for each of the research hypotheses.

Descriptive Statistics

The analyzed sample comprised 66 retail merchant organizations from the sampling pool of over 20,000 contacts. To confirm that the sample was representative of the target population, I compared response frequencies for demographic questions related to company size to frequencies found in data tables published as part of the latest census data (U.S. Census Bureau, 2020, 2021). Visualizations of employee count and revenues comparing census data for the defined population, with corresponding demographic data from the sample set, are provided in Figures 2 and 3. Not all revenue and employee ranges were available from the census data, so histogram bins were combined to align the population and sample and compare frequencies. These distributions provided visual confirmation that the respondent organizations were demographically diverse. However, the randomly obtained sample data were not representative of all subsets of the target population, because due to the limited sample size, the proportion of samples from larger organizations exceeded those in the population.

Figure 2

Comparison of Population and Sample - Revenue

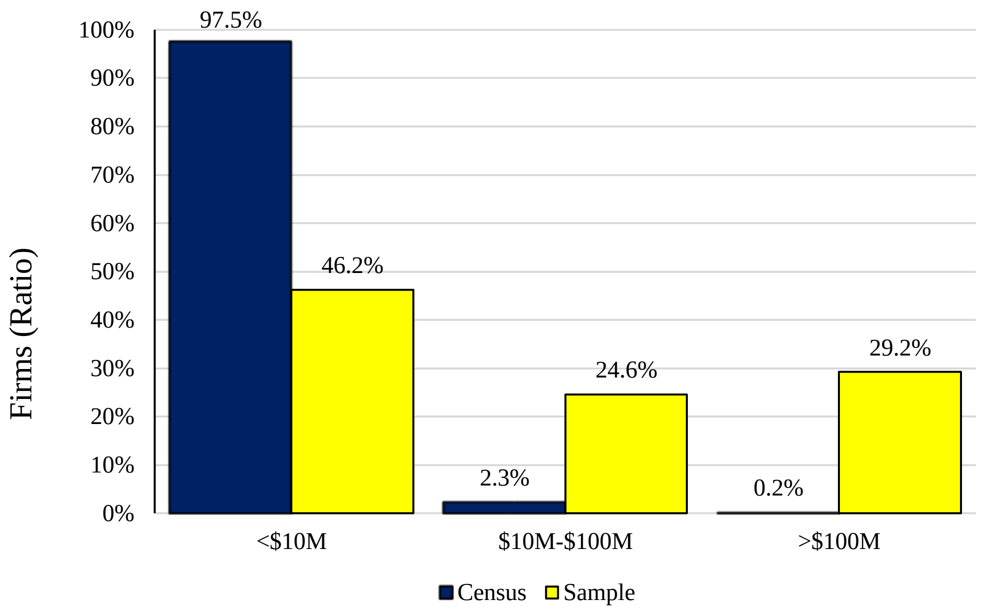
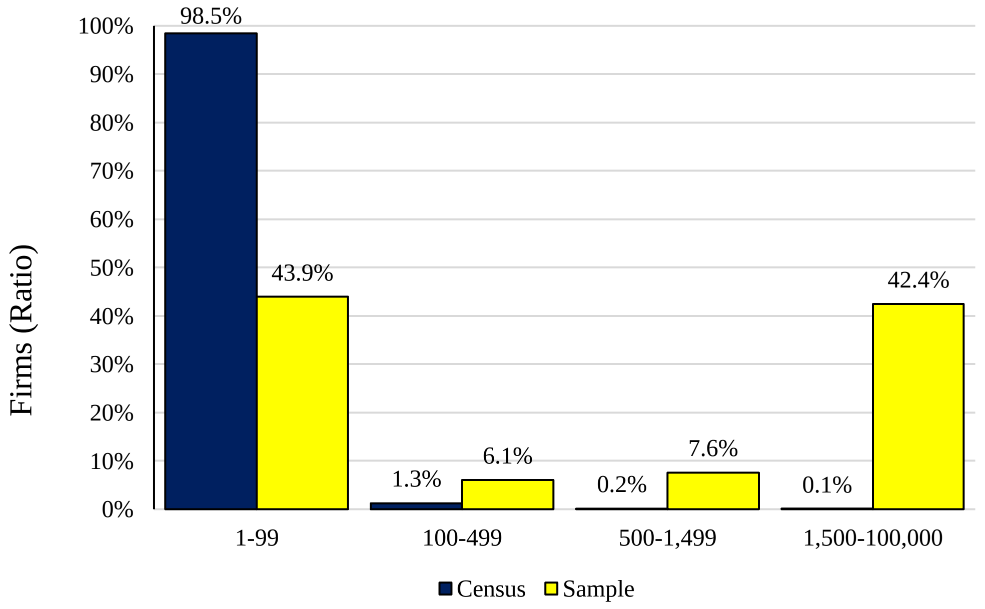


Figure 3

Comparison of Population and Sample - Employees



Among U.S. retail organizations, the mean CB was observed to be 5.183% of the organization’s total information technology budget, with a standard deviation of 4.198%. When evaluating the three survey response components intended to predict this value, I found the mean response values for IC and CR were both 4.46, with IC having a standard deviation of 1.608, while the standard deviation of CR was 1.728. The mean response value for CA was 4.83, with a standard deviation of 1.530, indicating more consistent responses to the corresponding survey question (see Table 2).

Table 2

Descriptive Statistics for Model Variables

	N	Minimum	Maximum	Mean	Median	Std. Deviation
CB	63	1.5%	18.5%	5.183%	4.00	4.198%
IC	61	1	7	4.46	4.00	1.608
CR	61	1	7	4.46	5.00	1.728
CA	63	2	7	4.83	5.00	1.530

Power Analysis

In conjunction with the multiple regression analysis, a statistical power analysis was performed. This calculation was based on the observed coefficient of determination value of the initial regression analysis (R^2 = .162), the number of predictors (N = 3), and the observed significance from the ANOVA test of the model (p = .030; see Table 10). Observed statistical power was calculated at 0.750, corresponding to $\beta = 0.250$ (J. Cohen, 1968, 2013; Soper, 2021).

Survey Administration

Among valid responses received, 22.72% of respondents completed the survey via SoGoSurvey, and the balance (77.28%) were collected via SurveyMonkey Audience (see Table 3). Due to anonymity settings on the online survey platforms, it was not possible to determine how many members of the sample pool attempted to complete the survey but withdrew before finishing.

Table 3

Recruitment Method

	Platform	Total frequency	Total percentage	Valid frequency	Valid percentage
Initial	SoGoSurvey	30	29.41%	15	22.72%
Subsequent	Survey Monkey	72	70.59%	51	77.28%
Total		102	100.00%	66	100.00%

Demographics

The participants were recruited using criteria that ensured responses from knowledgeable individuals within each retail merchant organization. The approved survey instrument included the option for all respondents to select the title that best described their position within their organization or supply their job role. I grouped custom-entered job roles based on common job types and reviewed these responses to understand the demographic profile of my survey respondents. Among valid responses, most prominently represented positions were CEO (*n* = 15; 22.73%), systems administration (*n* = 8; 12.12%), general managers and store managers (*n* = 7; 10.61%), or no response (*n* = 13; 19.70%). Other roles included management in finance, privacy, security, and ecommerce (see Table 4).

Table 4

Participant Roles

	Frequency	Percentage	Cumulative percentage
CEO	15	22.73%	22.73%
CFO	4	6.06%	28.79%
Chief Privacy Officer	2	3.03%	31.82%
CIO	2	3.03%	34.85%
CSO (Chief Security Officer) / Security Officer	1	1.52%	36.36%
Systems Administrator	8	12.12%	48.48%
Other: Assistant Manager / Assistant Sales Manager / Supervisor	4	6.06%	54.55%
Other: eCommerce Manager	1	1.52%	56.06%
Other: General Manager / Store Manager / Manager / Management	7	10.61%	66.67%
Other: Owner / Co-owner / Owner, Operator	4	6.06%	72.73%
Other: Regional Manager	1	1.52%	74.24%
Other	4	6.06%	80.30%
No Response	13	19.70%	100.00%
Total	66	100.00%	

Organizations varied in employee count (see Table 5) and revenue (see Table 6). Smaller companies comprised the largest response group by both measures (1–99 employees, *n* = 29; under $10 million, *n* = 30), but all tiers were well represented, with medium-size retail companies comprising over 37% by both employee count and revenue

(100–49,999 employees, *n* = 26; $10 million to $1 billion, *n* = 25). The largest retailers were also well represented (50,000 or more employees, *n* = 11; over $1 billion, *n* = 10).

Table 5

Employee Count

	Frequency	Percentage	Cumulative percentage
1–99	29	43.94%	43.94%
100–499	4	6.06%	50.00%
500–1,499	5	7.58%	57.58%
1,500–9,999	12	18.18%	75.76%
10,000–49,999	5	7.58%	83.33%
50,000 or more	11	16.67%	100.00%
No response	0	0.00%	100.00%
Total	66	100.0%	

Table 6

Gross Annual Revenue

	Frequency	Percentage	Cumulative percentage
Under $10 million	30	45.45%	45.45%
$10 million to $99 million	16	24.24%	69.70%
$100 to $1 billion	9	13.64%	83.33%
Over $1 billion	10	15.15%	98.48%
No response	1	1.52%	100.00%
Total	66	100.00%	

Review of demographics confirmed a representative sample of knowledgeable personnel from U.S. retail organizations of various size, supporting the intended analysis approach and confirming external validity for the larger population from which the sample was obtained.

Statistical Assumptions

Before testing the data, I explored key assumptions of normality of residuals, linearity, noncollinearity, and homoscedasticity to ensure suitability for the selected statistical analysis and to support assertions of research validity.

Outliers

Initial review of the histogram of standardized residuals (see Figure 4) revealed only two cases that fell near three standard deviations from the mean standardized residual, suggesting that no significant variance was found from the observed model. A scatterplot of regression standardized predicted values to the standardized residual for the corresponding case (Figure 5) similarly did not result in extreme outliers. Finally, the data set was also visually reviewed for the existence of clear outliers that may have negatively influenced the results of the analysis, and none were found.

Figure 4

Histogram of Standardized Residuals Used to Visualize Outliers

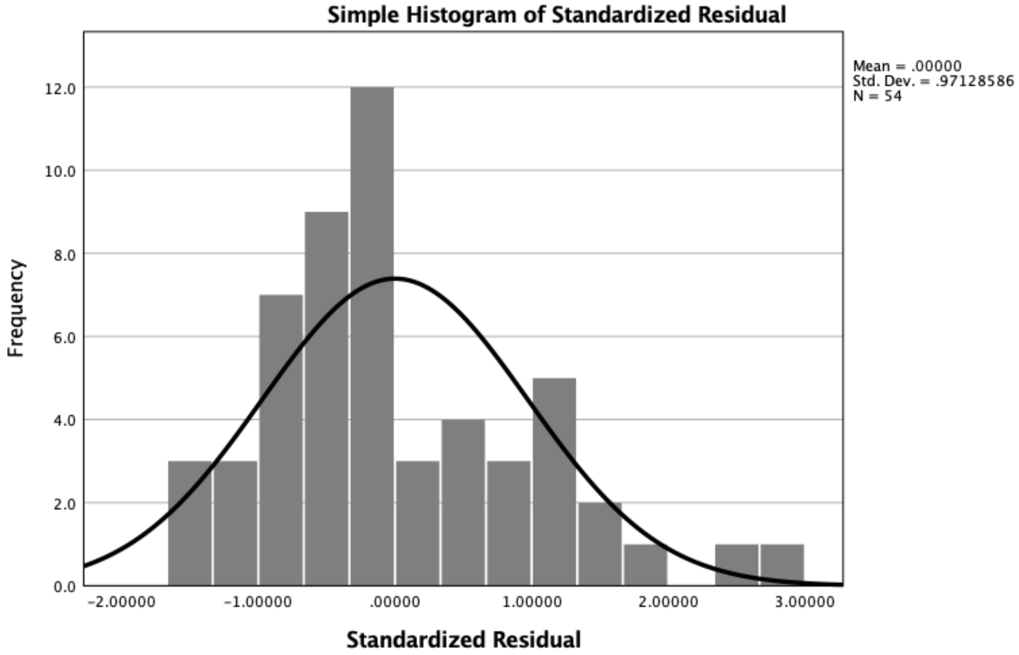
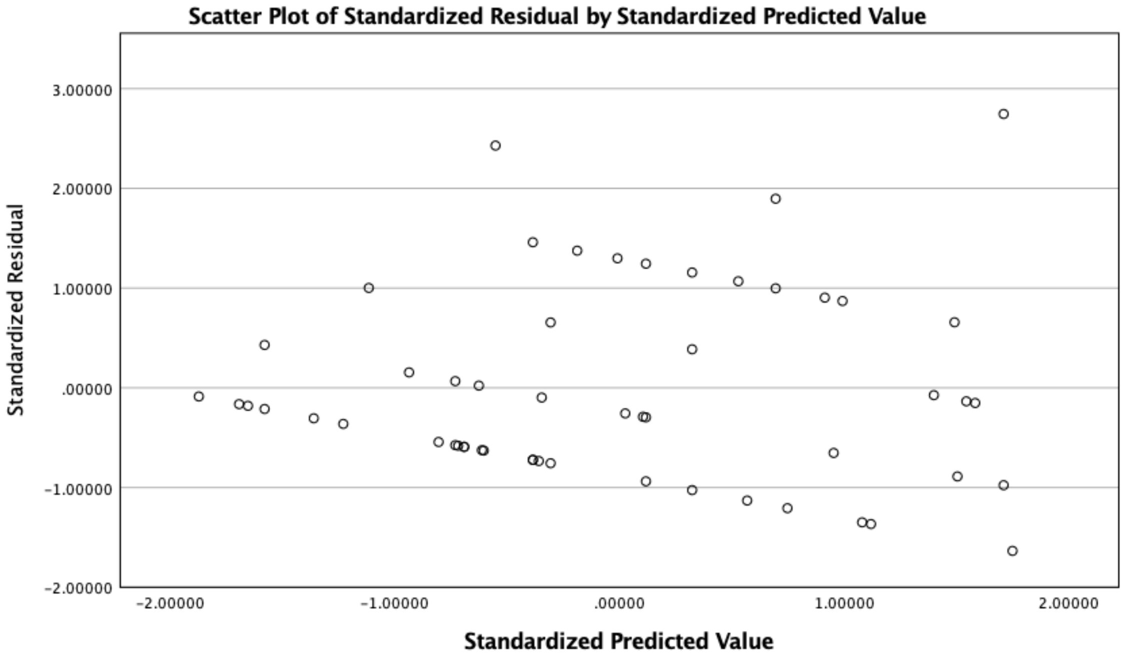


Figure 5

Scatterplot of Residuals and Predicted Values to Identify Outliers and Visualizing Assumption of Homoscedasticity.



Testing Assumptions

The use of multiple linear regression as a statistical analysis technique requires a data set that meets my stated assumptions of normality, homoscedasticity, multicollinearity, and independence of errors. These were tested using visualizations and data analysis to confirm basic assumptions, in order to ensure validity of the resulting conclusions.

Normal Distribution of Errors. Regression analysis is a parametric test and assumes that all errors from the regression are normally distributed. Normality may be visualized on histograms, frequency distributions, and data plots for a qualitative assessment, but a more accurate test of normality is provided by way of observing a histogram of standardized residuals and reviewing skewness and kurtosis statistics for signs of non-normality. The histogram shows that the fit of the residuals to the normal probability curve is positively skewed (see Figure 4). This is further visualized via a P-P-plot (Figure 6) with a dip to the right, which is also consistent with a sample distribution that is skewed slightly to the right. The measured level of skewness was .835 with kurtosis of .340 (see Table 7), and because these values exceed neither threshold for excess kurtosis nor skew (±1.96 for $p < .05$), the evidence confirms that the assumption of normality is met, and therefore justifies utilizing parametric analysis techniques to analyze these data (Mishra et al., 2019).

Table 7

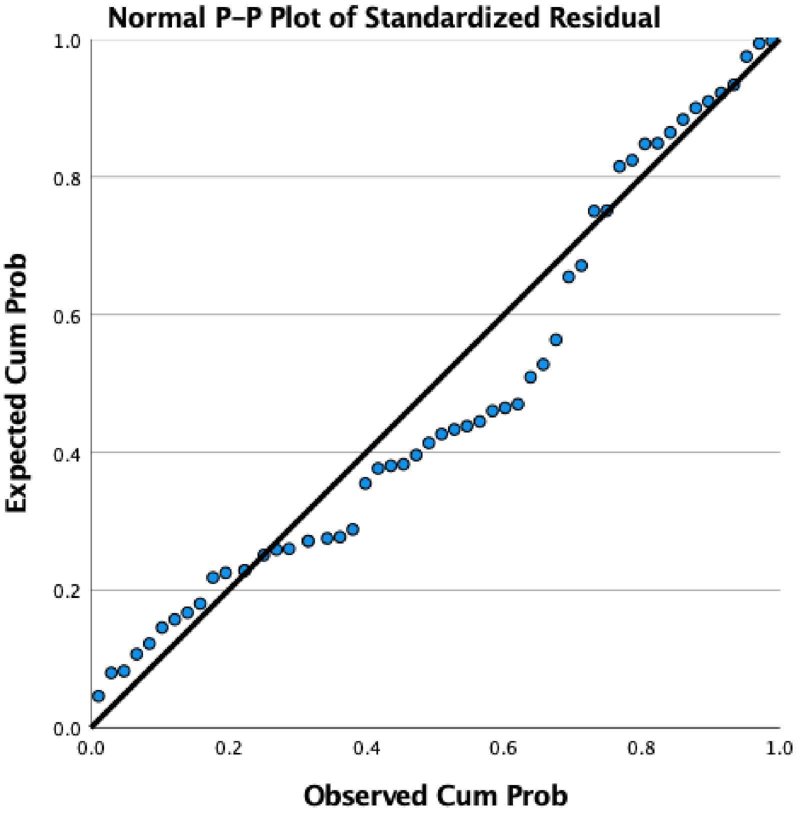
Descriptive Statistics for Normality

Statistic	Category	Value
N	Valid	54
	Missing	12
Mean		0
Std. deviation		.97128586
Skewness		.835
Std. error of skewness		.325
Kurtosis		.340
Std. error of kurtosis		.639
Range		4.38112
Minimum		-1.63455
Maximum		2.74657

Homoscedasticity. Homogeneity of variance, or homoscedasticity, connotes that error trends will not appear within the data indicative of poor uniformity of fit, thus impacting the validity of the regression model. Visualization was conducted of standardized predicted (expected) values to their standardized residuals using a scatterplot (see Figure 5). The scatterplot points appear to broaden slightly as predicted value increases; however, the scatter plot appears to be free from significant concerns of heteroscedasticity (Vogt, 2007).

Figure 6

Testing Assumption of Normality With P-P Plot



Multicollinearity. I assumed that the independent variables are uncorrelated, and that their impacts on the dependent are uniquely measurable. This assumption requires checking for indicators of collinearity between the independent variables, using such methods as correlation matrix and variance inflation factor (VIF; Greene, 2003). Correlation coefficients for each of the model variables are shown in Table 8 and appear to show low amounts of correlation between all three independent variables (-.423 <= ρ <= -.276). VIF values were far below the threshold of 10 for all independent variables, which provides reassurance of the lack of multicollinearity (Senaviratna & Cooray, 2019) as shown in Table 9 (1.375 <= VIF <= 1.546).

Table 8

Coefficient Correlations

Model			IC	CR	CA
		IC	1.000	-.276	-.285
1	Correlations	CR	-.276	1.000	-.423
		CA	-.285	-.423	1.000

a. Dependent Variable: CB

Table 9

Correlation and Collinearity Indices

Model	Variable	Zero-order	Partial	Part	Tolerance	VIF
1	(Constant)					
	IC	.383	.322	.311	.647	1.546
	CR	.153	-.101	-.093	.650	1.538
	CA	.252	.117	.108	.727	1.375

a. Dependent Variable: CB

Independence of Errors. The possible presence of autocorrelation was examined using the Durbin-Watson test (see Table 11), the presence of which might have indicated correlation between individual cases. The value of the Durbin-Watson statistic was 1.635, which is close to 2, thus indicating no substantial concern for autocorrelation.

Hypothesis Testing

The primary means of testing the hypotheses was multiple linear regression, having confirmed the suitability of this parametric test and the dataset being analyzed. I compared the observed and predicted distributions using analysis of variance (ANOVA) in order to evaluate the omnibus hypothesis (Table 10). For the omnibus analysis, 12 cases were excluded listwise due to missing responses for one or more independent variables (*n* = 54).

Table 10

ANOVA[ab]

Model		Sum of squares	*df*	Mean square	*F*	Sig.
	Regression	146.973	3	48.991	3.229	.030[b]
1	Residual	758.662	50	15.173		
	Total	905.634	53			

a. Dependent Variable: CB
b. *n* = 54
c. Predictors: (Constant), CA, CR, IC

The alpha level of .05 was chosen as the threshold to reject a null hypothesis ($p < .05$). Such an alpha level accepts that there is a 1:20 probability that the observed data will result in rejecting a true null hypothesis (Type I error), a tolerance that demonstrates the viability of the model to support its accuracy in decision analysis as part of a larger strategic business analysis toolkit. This analysis was intended to answer the research question “What relationships exist between internal control, cybersecurity risk, competitive advantage, and cybersecurity budgets among U.S. retail merchants?” by testing one omnibus hypothesis and three individual hypotheses:

Omnibus Hypothesis Results

H_0: There is no relationship between the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = \beta_2 = \beta_3 = 0$.

H_a: At least one of the independent variables of internal control (IV_1), cybersecurity risk (IV_2), and competitive advantage (IV_3) are useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants (DV): At least one of these inequalities is true $\beta_1 \neq 0$, $\beta_2 \neq 0$, $\beta_3 \neq 0$.

The results of the omnibus model evaluation were $F = 3.229$, $p = .030$, $p < .05$; $R = .403$, $R^2 = .162$, R^2adj = .112 (Tables 10 and 11). The omnibus null hypothesis (H_0) is thus rejected.

Table 11

Omnibus Model Summary [ab]

Model	*R*	*R* square	Adjusted *R* square	Std. error of the estimate	Durbin-Watson
1	.403[c]	.162	.112	3.8953	1.635

a. Dependent Variable: CB

b. *n* = 54

c. Predictors: (Constant), CA, CR, IC

Table 12

Omnibus Model Coefficients[ab]

Model		Unstandardized coefficients		Standardized coefficients	t	Sig.	95.0% confidence interval for B	
		B	Std. error	beta			Lower bound	Upper bound
1	(Constant)	.248	1.925		.129	.898	-3.619	4.116
	IC	.983	.409	.387	2.404	.020	.162	1.804
	CR	-.277	.386	-.115	-.717	.477	-1.051	.498
	CA	.342	.411	.126	.832	.409	-.484	1.169

a. Dependent Variable: CB
b. $n = 54$

Post-Hoc Analysis

Additional post-hoc analysis was performed to evaluate the individual hypotheses, by assessing the significance of each dependent variable with respect to dependent variable:

First Hypothesis Results

$H_0 1$: There is no relationship between the independent variable of internal control (IV_1) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_1 = 0$.

$H_a 1$: The independent variable of internal control (IV_1) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_1 \neq 0$.

The result of the first coefficient evaluation was $t(53) = 2.404$, $p = .020$ (Table 12). As $p < .05$, the null hypothesis ($H_0 1$) is thus rejected.

Second Hypothesis Results

$H_0 2$: There is no relationship between the independent variable of cybersecurity risk (IV_2) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_2 = 0$.

$H_a 2$: The independent variable of cybersecurity risk (IV_2) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_2 \neq 0$.

The result of the second coefficient evaluation was $t(53) = -.717$, $p = .477$, $p > .05$ (Table 12). The null hypothesis ($H_0 2$) is thus not rejected.

Third Hypothesis Results

$H_0 3$: There is no relationship between the independent variable of competitive advantage (IV_3) and the dependent variable of cybersecurity budgets among U.S. retail merchants (DV): $\beta_3 = 0$.

$H_a 3$: The independent variable of competitive advantage (IV_3) is useful in explaining and/or predicting cybersecurity budgets among U.S. retail merchants: $\beta_3 \neq 0$. The result of the third coefficient evaluation was $t(53) = .832$, $p = .409$, $p > .05$ (Table 12). The null hypothesis ($H_0 3$) is thus not rejected.

Univariate Model Summary

Because only one of the individual null hypotheses was rejected, the model was adapted to contain only the single independent variable, IC, and the degree to which it predicts the dependent variable of CB. The regression analysis was then performed on this univariate linear regression model, including all cases within the sample set containing both variables (*n* = 61). The results of are summarized in Tables 13, 14, and 15.

Table 13

Univariate ANOVA[ab]

Model		Sum of squares	*df*	Mean square	*F*	Sig.
1	Regression	23.803	1	23.803	10.369	.002[c]
	Residual	135.442	59	2.296		
	Total	159.246	60			

a. Dependent Variable: CB
b. *n* = 61
c. Predictors: (Constant), IC

Table 14

Univariate Model Summary [ab]

Model	*R*	*R* square	Adjusted *R* square	Std. error of the estimate	Durbin-Watson
1	.387[a]	.149	.135	1.515	.661

a. Dependent Variable: CB
b. *n* = 61
c. Predictors: (Constant), IC

Table 15

Univariate Final Model Coefficients[ab]

Model		Unstandardized coefficients		Standardized coefficients	*t*	Sig.	95.0% confidence interval for B	
		B	Std. error	Beta			Lower bound	Upper bound
1	(Constant)	.762	.576		1.322	.191	-.391	1.914
	IC	.392	.122	.387	3.220	.002	.148	.635

a. Dependent Variable: CB
b. *n* = 61

Summary

In Chapter 4, the sampled data were analyzed for suitability for this study, including review of descriptive statistics, identification of outliers, and testing of multiple linear regression assumptions. The omnibus hypothesis was then tested to answer the research question; I rejected the omnibus null hypothesis (H_0). I then conducted the post-hoc analyses using multiple linear regression to determine which of the predictor variables were statistically significant in predicting the dependent variable; I rejected the first null hypothesis (H_01), however I failed to reject the second null hypothesis (H_02) and the third null hypothesis (H_03). A univariate linear regression equation corresponding to the first alternative hypothesis (H_a1) was confirmed to be statistically significant, relating to the independent variable of internal control and the dependent variable of cybersecurity budget. In Chapter 5, these results will be discussed in light of the intended research objectives, including practical application of this research, its limitations, and recommendations for future research.

Chapter 5: Discussion, Conclusions, and Recommendations

The purpose of this study was to describe the relationship between the dependent variable of cybersecurity budget and three determinants of internal control, cybersecurity risk, and competitive advantage within retail merchant organizations in the United States. The nature of the study was a nonexperimental quantitative correlational analysis using an email recruitment data collection approach to enlist a random sample of participants from this population. Response data were collected via an internet survey using a previously validated survey instrument. Data were tested for normality and analyzed using multiple linear regression techniques. The goal of the study was to confirm whether the posited model explained the relationship between the three predictors (internal control, cybersecurity risk, and competitive advantage) and the organization's resulting cybersecurity budget.

In Chapter 4, the results of this study were provided, including the statistical analysis of the resulting data sample and the resulting univariate model coefficients (see Table 15). The outputs from these analyses were used to develop a regression formula expressed in the format $\mathrm{CB} = \beta_0 + \beta_1 \mathrm{IC}$, which detailed the observed relationship between these variables:

$$\text{CB} = 0.762\% + (0.392\% \text{ x IC}) \tag{6}$$

Interpretation of Findings

The first alternative hypothesis was that overall budget may be predicted in a nonrandom way by the manner in which internal control is framed by leaders within an organization. The extent to which this hypothesis reflects observation is the principal value of the confirmed model, which demonstrates the predictive relationship between this easily measured aspect of the industry and organization's culture and messaging, and its eventual prioritization of cybersecurity spending. Statistically speaking, the analysis of the model using ANOVA (see Table 13) resulted in a significant observed effect at the $p < .05$ level [$F_{(1,\ 60)} = 4.0012$, $p = .002$], demonstrating a significant ratio of variance between the modeled fit and the general population. These statistics provide assurance that the linear relationship described by the coefficient and intercept within the model fit the sampled data.

The coefficient of determination for the univariate linear regression analysis was relatively low ($R^2 = .149$; see Table 14). When coupled with the ANOVA results, this indicates that, although reliable, the proposed model explains only 14.9% of the variance within the sample, leaving 85.1% of the variance unexplained by this variable. This is understandable and does not undermine the results of this study because there are many factors that contribute to budget decisions of this nature. Although the impacts of only one tested determinant on cybersecurity budget were found to statistically significant, further studies of these variables may result in more conclusions with increased explanatory power. Furthermore, the inclusion of additional variables represented by perceptions (measured by this instrument or other means) may improve the R^2 value (e.g., by identifying whether an organization's cybersecurity budget is directly impacted by its ability to accurately measure the probability of cybersecurity events or potential losses).

Finally, the power analysis from the univariate regression test, using the ANOVA F test, resulted in an effect size of $R^2 = .149$ or $f^2 = .17509$, with a statistical power of

.750, corresponding with $\beta = .250$. This moderately high statistical power indicates a relatively low chance of making a Type II error (i.e., not rejecting a null hypothesis when it is false). In rejecting the null hypothesis, I am able to assert with some degree of confidence that the regression does have at least some explanatory power and thereby aids in addressing the original research question.

Practically speaking, the regression formula is one of the key values of this research. Retail industry baselines have not been established for modeling budget from management perceptions. One useful impact of this study is its empirical measurement of current industry benchmark among current retail merchants. For example, for a merchant organization who is not subject to regulatory compliance requirements requiring strong internal control (e.g., IC = 1), this value may be inserted into the regression formula to calculate forecasted cybersecurity budget as

$$\text{CB} = 0.762\% + (0.392\% \text{ x } 1) = 1.154\% \tag{7}$$

By contrast, for a merchant with a high compliance requirement (e.g., IC = 7), the organization baseline value for cybersecurity budget is

$$\text{CB} = 0.762\% + (0.392\% \text{ x } 7) = 3.506\% \tag{8}$$

Benchmarking cybersecurity budget to this baseline, then, is a matter of using the DHS Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector assessment tool (see Appendix D) to determine a company’s perceptions related to cybersecurity driver of internal control and comparing this against the calculated value.

The informative results produced by this study were a direct outcome of several contributing factors within the research design. A multivariate correlational study with a nonexperimental design was well suited for gathering and analyzing existing perceptions from entities to test the proposed model (see Krotov, 2016). The instrument was designed and tested to capture the needed information in a format that is flexible enough to accommodate diverse analysis requirements, providing a quick evaluation mechanism that is also informative to the respondent (Diem, 2004). By recruiting inexpensively from a sample containing tens of thousands of merchant contacts, I increased the likelihood of producing the needed sample size, although in this case additional effort was required to meet the necessary sample size for the desired statistical power. Although this low response rate may have been due to solicited recipients choosing to decline participation due to policies or other concerns in sharing high-level cybersecurity data, the subsequent approach of incentivizing respondents using a trusted research partner via a confidential online survey platform resulted in sufficient responses to meet the necessary statistical power for testing the fit of the proposed model and generalizing those results to the larger population (see Austin & Steyerberg, 2015).

Research confirmed the importance of survey instruments for measuring perceptions and attitudes as cybersecurity drivers (Kusserow, 2014) and the value of regression analysis as a means of confirming straightforward models for benchmarking expenditures against these influences (Gordon et al., 2015b). The current study confirms the approaches suggested by Björklund (2010), Matthews and Lave (2003), and Keith (2019) by identifying one or more measurable values by which to model cost drivers. This study contributes to this body of knowledge revealing one aspect of this predictive relationship, thereby helping U.S.-based retail merchants better understand the influence of cybersecurity as part of an organization’s internal controls for financial reporting systems.

Real options theory informs the strategic management practice of decision making, which can be defined using the construct proposed by Spendolini (1992) as “a continuous, analytical process for measuring the business practices, work processes, and cost drivers of organizations that are recognized as representing best practices for the purpose of meeting or surpassing industry best practices” (pp. 8–9). To accurately measure these costs for comparison against exemplar organizations, it is recommended that researchers “develop and empirically validate theoretically sound regression models that can potentially improve reliability and validity of IT cost benchmarking” (Krotov, 2016, p. 23). The current study contributes to a cost measurement and comparison approach by testing one regression model that may be used in IT cost benchmarking activities.

In addition to confirming the validity of the univariate predictive model, three relationships were initially posited as being important for predicting budget. Although only IC was found to be a reliable measure of prediction, the ANOVA analysis of the omnibus model (see Table 10; p < .05) provides justification for a multivariate relationship that may include aspects of CR and CA for better understanding their impact on CB. Multiple regression analysis was the appropriate statistical analysis method for this analysis, resulting in regression coefficients assigned to each of the predictors presented in the model diagram (see Figure 1) and demonstrating the size of the effect each variable had on the determination of the dependent value (see Vogt, 2007). Future research may benefit from obtaining more granular data by which to measure these relationships more accurately.

The causal understanding of such relationships, as informed by real options theory and described in part within these results, supports the budget modeling process. Organizations may use this model in conjunction with their established benchmarking processes to evaluate their measured costs against this baseline measurement. This process follows the flow described by Fifer (1989) in which mutual cost drivers are identified and used to model cost, and cost is calculated for both organizations using the same approach. Research confirmed that an established instrument (Kusserow, 2014) and cost model (Brecht & Nowey, 2013) may be used to measure security cost drivers and support the competitive benchmarking process (Eichfelder & Vaillancourt, 2014; Fifer, 1989). Such an approach is cost-effective for identifying compliance process and cost inefficiencies (Krotov, 2016), especially for entities subject to security regulation, such as retail merchants (Matthews & Lave, 2003).

The current study contributes to this body of knowledge, revealing one aspect of this specific predictive relationship. This understanding—that retail merchants who recognize the role of cybersecurity for control of financial reporting systems invest in such measures at an increased rate—provides justification for initiatives that influence such recognition. It is therefore reasonable to expect that increased industry investments in education, research, and regulation for accounting system controls may result in industry-wide increases in overall cybersecurity investment (more than risk awareness alone).

Limitations of the Study

There were three limitations identified in this study. First, the statistical strength of the results was limited. Second, analysis of the obtained data resulted in two regression assumptions that I would have liked to have met with a greater degree of confidence. Finally, although the initial multivariate analysis provided value in understanding of the impact of internal control on total cybersecurity budget, it was limited in its ability to explain the influences of other factors on cybersecurity budgetary decisions.

Statistical Strength

The a priori analysis suggested that effect size would require a minimum sample size of $N = 61$. This approach is appropriate in multiple regression correlation analysis of models with both omnibus and individual hypotheses, and when statistical power of the resulting regression is unknown (J. Cohen, 1968; J. Cohen et al., 2003). Using this a priori sample size calculation method, a researcher must presuppose a lower effect size than hoped to ensure a large enough sample to ensure adequate statistical power associated with the resulting analysis.

With three predictors, I originally expected that the proposed model would explain at least 20% of the variance leading to a higher R^2 and therefore a larger effect size. The original target value of $N = 61$ was deemed a reasonable minimum sample size for planning purposes given the uncertainty of the data and optimistic sampling results. Although no attempt was made to limit the number of responses obtained, during the data collection phase only 66 respondents provided valid survey responses. As such, during the data collection, the effect size of the observed data was found to be lower than expected ($R^2 = .162$, $f^2 = .1933$, $\beta = .250$). It is therefore possible that a larger sample could both improve the statistical power of the observed relationships, as well as provide more confidence in model describing these observed relationships.

To ensure results were generalizable to the full population of U.S. merchants, I ensured receipt of sufficient responses to meet the minimum sample size. This supported external validity by ensuring that the results could be generalized to the broader population (see Kelley & Maxwell, 2003) and could be relied upon when replicated in practice. Multiple regression studies with many predictors generally require more samples to ensure that the results are generalizable (Bartlett et al., 2001; Israel, 1992), but for analyses with fewer predictors and sufficiently large effect sizes, the required number of responses can be contained to an attainable number (Abramowitz & Stegun, 1965; J. Cohen, 1968; J. Cohen et al., 2003; Soper, 2021). Austin and Steyerberg (2015) asserted that analyses with as few as two samples per predictor can be valid with sufficient statistical power. In spite of this, the calculated statistical power failed to justify strong assertions related to the generalizability of two variables within the tested model.

Assumptions

The assumptions required for the use of multiple linear regression include nonexistence of outliers, normal distribution of errors, homoscedasticity, noncollinearity, independence of errors, and linear relationship. Testing of these assumptions was used to confirm suitability for this analysis technique. However, two of these assumptions warranted further discussion as possible limitations of this study: homoscedasticity and normal distribution of errors.

Homoscedasticity

In my testing for homoscedasticity, the scatterplot showed a broadening to the right (see Figure 5), an indicator that the dataset had nonrandom distribution of errors. Some of this lack of homogeneity of variance, especially among the larger predicted values, could be explained by the lack of accuracy within the obtained budgetary estimates based on the increasing ranges within the survey instrument. An alternate explanation may be the influence of other factors, which are more pronounced for larger budgets. Both of these factors warrant additional research through extension of this model and/or fine-tuning of the survey instrument.

Normal Distribution of Errors

Upon reviewing the descriptive statistics for the standardized residual, the errors show a skewness of $z = .835$, which describes a distribution that is heavier on the left than a normal probability curve, with a longer tail to the right. Skewness should be as close to 0 as possible with values exceeding an absolute value of 1.96 to be considered non-normally distributed (Mishra et al., 2019). This measured skewness can be further visualized by the histogram in Figure 4, and the right protrusion in the P-P plot (Figure 6). This residual distribution of errors is therefore moderately skewed, but without significant deviations from the desired normal distribution.

Observing the histogram (Figure 4), however, there also appears to be a bimodal trait in the right, which may in fact reflect the artifact of a true normal distribution as represented by a limited set of data points (Doane & Seward, 2011). In fact, for smaller samples, $n < 50$, Kim (2019) recommends only considering a distribution truly skewed when the test statistic falls outside ±1.96. For these reasons, the dataset was assumed to be normal, even though it showed moderate skewness. A larger data set may resolve this artefact, or conversely, confirm nonnormality of the data set and the need to modify the instrument to use numeric (scalar) responses for estimates of cybersecurity budget rather than ranges.

Model Limitations

The model tested in this current study (see Figure 1) attributed budgetary drivers to these three variables (IC, CR, CA) and attempted to predict annual budget decisions based on coefficients attributed to each. In fact, a regression model that is explanatory and statistically significant may be more valuable than one that includes more predicators or other mediating or moderating variables, but lacks reliability (Harrell, 2015). Even so, the resulting model accounted for only 14.9% of the variance observed, and the individual coefficients for CR and CA were not statistically significant and were thus omitted.

Recommendations

The scope of this study was sufficient to meet its original purpose, but there is ample room to extend its findings through introduction of additional factors to improve the model, enhancements to the survey instrument, improvements to recruitment methodologies, and better addressing matters of confidentiality. Additional recommendations for future research include replication studies or sampling of additional populations.

For this study, the limitation on the number of factors was primarily due to the need to focus on those predictors that are most explanatory. the model may, however, be improved through the inclusion of one or more of other nuanced factors that are predictive of budget, were there time and budget to research them fully. For instance, the model and research design limitation discussed in the Limitations of the Study section could have been mitigated through the inclusion of other measured perceptions in predicting this outcome, such as the tendency for organizations to incorporate probability of cybersecurity breach (question F8) and magnitude of potential losses (question F9). Some additional independent variables not measured by this study could also have been incorporated, such as the influence of specific regulatory compliance obligations on internal controls (e.g., SOX, PCI DSS, HIPAA), or measurements of the respondent organization's attack surface (i.e., merchants with larger retail footprints have more assets which must be protected). Finch et al. (2019) caution that, although including additional factors may increase the coefficient of determination (R^2), this doesn't always correspond to increased statistical significance unless the new predictor variables aid in explaining changes to the outcome variable. Thus, by delimiting this current study on the most prominent predictors, my goal was to arrive at results which were both significant and valuable; but with additional resources and time additional predictors may be studied which may render an improved outcome.

In addition to the inclusion of additional factors, improvements may be made to the instrument itself to aid in quickly and accurately recording costs. The language used in the survey may not have been familiar to all respondents, as smaller organizations have been shown to lack awareness of concepts such as internal control, and cybersecurity risk (Gafni & Pavel, 2019; Itang, 2020). There exists an opportunity for researchers and practitioners to create a more interactive and intelligent data collection instrument that guides the respondent through specific questions and technologies rather than relying upon the respondent's recollection of relevant budget ratios. Such an instrument was deemed too complex for use in this current study, and would require validation, but could have commercial as well as academic value to better measure these perceptions among small and medium enterprises and their impact on security investments.

Reflecting upon the limited statistical power as a methodology challenge, there are two additional changes which may increase the validity and reliability of the resulting model. First, the survey itself may need to be modified to allow for more accurate measurement of the operationalized variables. For instance, the transformation of budget from the original ranges to interpolated scalar values may have introduced unnecessary inaccuracy. Although range options allowed for more quickly obtaining budget data using an estimate-based approach, the inaccuracy of this value may ultimately have impacted the ability of this study to produce stronger outcomes, and such approaches should be investigated. Secondly, statistical power may be improved through obtaining a larger sample size. To address this weakness, the design of the research may need to be modified to allow use of a controlled convenience-based sampling approach, such as snowball sampling, whereby participants are more inclined to respond based on relational trust, while also introducing weights to offset the natural introduction of sampling bias (Emerson, 2021; Farrokhi & Mahmoudi-Hamidabad, 2012).

The limited response size from this current research demonstrated a potential resistance of retail security professionals to disclosing enterprise security information. A recommendation for future research is to investigate ways in which to coordinate information sharing among security professionals that maintains the rigors of objective research, but also assuages concerns of privacy and confidentiality risk that accompany any form of information sharing. Attempts have been made in the past to address sharing concerns through technology (Dandurand & Serrano, 2013), methodology (Zhao & G. White, 2017), and improved attitudes toward sharing (Ibragimova et al., 2012), but additional study may be warranted to connect these approaches in the form of a framework for accessing valuable data while simultaneously addressing concerns of confidentiality.

For future research, I recommend confirmatory research be performed to validate the proposed instrument, derived regression formula, and conclusions vis-à-vis the underlying research questions and hypotheses. Although the results are significant within the respondent cases, given the limited sample size a confirmatory study that replicates these results to a larger audience would aid in validating the tools and methodologies proposed herein. Replication studies may be used to test the strength of observed relationships, as well as flush out additional insights through exploratory analysis, thereby strengthening the proposed model (Widaman, 2018).

Finally, for reasons of population access, delimitations were made in this current study to exclude non-retail organizations and organizations outside of the United States. Cultural and regulatory drivers may influence the outcomes of such a study, thus inclusion of these segments may significantly alter the results. Future research is therefore encouraged to extend this study's approach into these additional populations.

Implications

All companies have finite resources, and recent health and economic impacts highlight how pronounced these constraints are among today's retailers. Therefore, risk prediction accuracy and cost savings in one area of budgets can be reallocated to non-security investments that improve the lives of individuals, families, and organizations. Even entities that have obtained an optimal investment in cybersecurity may use the model herein alongside other models, such as the Gordon-Loeb model (Gordon et al., 2015b), to gain confidence in these decisions and reallocate surplus resources to capital improvements.

Besides the retail merchants themselves, other entities may also leverage these results within the retail and payments industries. Meeting regulatory compliance requirements, such as PCI DSS, is often an effort of coordinating vendor relationships, security tools, and payments interoperability (Williams & Chuvakin, 2014). For vendors offering security and compliance solutions in this industry, understanding and communicating drivers for cybersecurity investment may support the vendor's value proposition while helping their customers justify the cost of the investment. Acquiring banks and card brands may also use this information to create messaging that encourages merchants to stay informed of inefficiencies that may be diverting funds away from areas of weakened security, or by offering enhanced technologies that provide cost-effective technologies that smaller merchants want and need (ControlScan, 2014).

Organizations may use this regression model to perform benchmarking functions. Benchmarking using a quantitative regression formula is a mathematical process, by which organizations first normalize disparate aspects between their environments, insert known values into the formula, and evaluate the unknown value or compare results against known values. An organization may calculate its own benchmark for budget to ensure optimization of capital expenditures (Dai et al., 2012). A retail enterprise engaged in competitive benchmarking may compare its security budget with benchmarking partners to ensure sufficient investment relative to similar firms or competitors who calculate using the same regression formula (Atallah et al., 2004; Budur et al., 2019; Matthews & Lave, 2003; Rajaniemi, 2007). This approach may also be leveraged as part of a vendor risk management process to perform due diligence screening for vendors or partners using a scorecard method (Müller, 2020).

Another implication of this research is improving the industry’s understanding of the degree to which compliance (as expressed within the requirement for internal control) influences the investment behaviors of organizations where actual expected loss (as expressed within the use of cybersecurity risk to inform these decisions) may not. The use of industry and government regulation are important balances to the profit (and loss) drivers present in free markets which often drive innovation and accessibility (Gordon et al., 2015c). However, exposing this inconsistency demonstrates an inherent inadequacy within free markets to effectively counter risk absent the influence of such governing bodies and regulatory roles.

Finally, the ultimate effect of improving cybersecurity investment is the positive social change brought about by improving access to products and marketplaces to those most effected by price increases resulting from cybersecurity breaches and fraud (Janakiraman et al., 2018). Cost-effective improvements to the retail industry’s cybersecurity posture can reverse the trend of lost customer confidence and attrition from markets due to economic losses and eroded consumer confidence (Curtis et al., 2018; Manworren et al., 2016). Whether through increased regulation, improved education of risk of economic losses, or renewed focus on the positive impacts of cybersecurity as a competitive advantage, these important social changes are the end result of improved security in retail markets, whereby customer information is protected from identity theft or fraud, and consumers are afforded a safer, more secure purchasing experience.

Conclusions

The findings of this study confirmed the relationship between U.S. retailers’ perceptions of cybersecurity as a crucial part of its internal control of financial reporting systems, and their ultimate investment in improved cybersecurity. Confirming this predictive relationship provides a valuable tool for merchants to identify the current industry baseline and affirm the value of addressing perceptions which influence decision making related to these security program investments.

This predictive relationship between internal control and cybersecurity budget further highlights the trade-off between regulation of financial systems and resource management decisions for retail security. The retail industry can benefit from a holistic perspective on cybersecurity, by continuing to enact a culture of security in addition to financial system governance and regulatory compliance.

With this study it is my sincere hope that compliance teams, C-level management, and board-level stakeholders from merchants, service providers, acquirers, and card brands can deepen their understanding and practical application of these relationships to improve the efficiency of their security investments, thereby creating a more secure environment for retailers and consumers alike.

References

Abramowitz, M., & Stegun, I. A. (Eds.). (1965). *Handbook of mathematical functions*. Dover.

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94–116. https://aisel.aisnet.org/icis2006/94

Adner, R., & Levinthal, D. A. (2004). What is not a real option: Considering boundaries for the application of real options to business strategy. *Academy of Management Review*, *29*(1), 74–85. https://doi.org/10.2307/20159010

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., Roberts, T., & Upton, D. M. (2016). Cyber harm: Concepts, taxonomy and measurement. *Saïd Business School Research Papers*, *23*, 1–45. https://doi.org/10.2139/ssrn.2828646

Al Rubaie, E. M. H. (2021). Improvement in credit card fraud detection using ensemble classification technique and user data. *International Journal of Nonlinear Analysis and Applications*, *12*(2), 1255–1265. https://doi.org/10.22075/IJNAA.2021.5228

Amram, M., & Kulatilaka, N. (1999). Uncertainty: The new rules for strategy. *Journal of Business Strategy*, *20*(3), 25–29. https://doi.org/10.1108/eb040003

Anand, G., & Kodali, R. (2008). Benchmarking the benchmarking models. *Benchmarking: An International Journal*, *15*(3), 257–291. https://doi.org/10.1108/14635770810876593

Anderson, C., Baskerville, R. L., & Kaul, M. (2017). Information security control theory:

Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *Journal of Management Information Systems*, *34*(4), 1082–1112. https://doi.org/10.1080/07421222.2017.1394063

Asen, A., Bohmayr, W., Deutscher, S., González, M., & Mkrtchian, D. (2019). *Are you spending enough on cybersecurity?* Boston Consulting Group. https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity

Atallah, M., Bykova, M., Li, J., Frikken, K., & Topkara, M. (2004). Private collaborative forecasting and benchmarking. In *Proceedings of the 2004 ACM workshop on privacy in the electronic society* (pp. 103–114). Association for Computing Machinery. https://doi.org/10.1145/1029179.1029204

Ataya, G. (2010). PCI DSS audit and compliance. *Information Security Technical Report*, *15*(4), 138–144. https://doi.org/10.1016/j.istr.2011.02.004

Austin, P. C., & Steyerberg, E. W. (2015). The number of subjects per variable required in linear regression analyses. *Journal of Clinical Epidemiology*, *68*(6), 627–636. https://10.1016/j.jclinepi.2014.12.014

Barclay, C. (2014, June). Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM^2). In *Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world - Impossible without standards?* (pp. 275-282). IEEE. https://doi.org/10.1109/Kaleidoscope.2014.6858466

Barretta, A. D. (2008). The exclusion of indirect costs from efficiency benchmarking. *Benchmarking: An International Journal*, *15*(4), 345–367.

https://doi.org/10.1108/14635770810887195

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, *19*(1), 43–50. https://www.opalco.com/wp-content/uploads/2014/10/Reading-Sample-Size1.pdf

Baryshnikov, Y. (2012, June). IT Security Investment and Gordon-Loeb's 1/e Rule. *Proceedings of the 11th Annual Workshop on the Economics and Information Security (WEIS)*, 1–7. https://www.researchgate.net/publication/242072740_IT_Security_Investment_and_Gordon-Loeb's_1e_rule/

Bellman, R. (1954). Decision making in the face of uncertainty - II. In R. M. Thrall, C. H. Coombs & R. L. Davis (Eds.), *Decision processes* (pp. 327–332). John Wiley & Sons, Inc. https://doi.org/10.1002/nav.3800010411

Benaroch, M. (2018). Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. *Information Systems Research*, *29*(2), 315–340. https://doi.org/10.1287/isre.2017.0714

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1–10. https://doi.org/10.1504/IJBCRM.2018.090580

Bhargav, A. (2014). *PCI compliance: The definitive guide*. CRC Press.

https://doi.org/10.1201/b16846

Bikker, R., Daalmans, J., & Mushkudiani, N. (2013). Benchmarking large accounting frameworks: A generalized multivariate model. *Economic Systems Research*, *25*(4), 390–408. https://doi.org/10.1080/09535314.2013.801010

Björklund, M. (2010). Benchmarking tool for improved corporate social responsibility in purchasing. *Benchmarking: An International Journal*, *17*(3), 340–362. https://doi.org/10.1108/14635771011049335

Blau, P. M. (1968). The hierarchy of authority in organizations. *American Journal of Sociology*, *73*(4), 453–467. https://doi.org/10.1086/224506

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2008). Information security and risk management. *Communications of the ACM*, *51*(4), 64–68. https://doi.org/10.1145/1330311.1330325

Böhme, R., & Moore, T. (2016). The "iterated weakest link" model of adaptive security investment. *Journal of Information Security*, *7*(02), 81. https://doi.org/10.4236/jis.2016.72006

Brecht, M., & Nowey, T. (2013). A closer look at information security costs. In *The economics of information security and privacy* (pp. 3–24). Springer.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, *48*(4), 265–276. https://doi.org/10.1016/j.lrp.2014.07.005

Budur, T., Faraj, K. M., & Karim, L. A. (2019). The benchmarking operations strategies via hybrid model: A case study of café-restaurant sector. *Amazonia*

Investiga, *8*(23), 842–854.

Bukhvalov, A., & Bukhvalova, B. (2011). The principal role of the board of directors: The duty to say. *Corporate Governance: International Journal of Business in Society*, *11*(5), 629–640. https://doi.org/10.1108/14720701111177028

Buonaguidi, B., Mira, A., Bucheli, H., & Vitanis, V. (2021). Bayesian quickest detection of credit card fraud. *Bayesian Analysis*, *1*(1), 1–30. https://doi.org/10.1214/20-BA1254

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448. https://doi.org/10.3233/JCS-2003-11308

Canelón, J., Huerta, E., Leal, N., & Ryan, T. (2020, January). Unstructured data for cybersecurity and internal control. In *Proceedings of the 53rd Hawaii International Conference on System Sciences* (pp. 5411–5420). https://doi.org/10.24251/HICSS.2020.665

Chang, Y. T., Chen, H., Cheng, R. K., & Chi, W. (2019). The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. *Journal of Contemporary Accounting & Economics*, *15*(1), 1–19. https://doi.org/10.1016/j.jcae.2018.11.002

Cheney, J. S., Hunt, R. M., Jacob, K. R., Porter, R. D., & Summers, B. J. (2012). The efficiency and integrity of payment card systems: Industry views on the risks posed by data breaches. *Economic Perspectives*, *36*(4), 130–146.

https://doi.org/10.2139/ssrn.2162536

Chronopoulos, M., Panaousis, E., & Grossklags, J. (2018). An options approach to cybersecurity investment. *IEEE Access*, *6*, 12175–12186. https://doi.org/10.1109/ACCESS.2017.2773366

Cisco. (2019). Anticipating the unknowns: Chief information security officer (CISO) benchmark study. https://ebooks.cisco.com/story/anticipating-unknowns

Clutterbuck, P. (2010). Security on the cards. *Charter*, *81*(1), 26–28. https://espace.library.uq.edu.au/view/UQ:221337

Cohen, J. (1968, December). Multiple regression as a general data-analytic system. *Psychological Bulletin*, *70*(6, Pt.1), 426–443. https://doi.org/10.1037/h0026714

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences (2nd Edition).* Academic Press, 1988. https://doi.org/10.4324/9780203771587

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). *Applied multiple regression/correlation analysis for the behavioral sciences (3rd Edition)*. Routledge.

Cohen, M. D., March, J. G., & Olsen, J. P. (1972). A garbage can model of organizational choice. *Administrative Science Quarterly*, 1–25. https://doi.org/10.2307/2392088

Conroy, J. (2014). *EMV: Lessons learned and the U.S. outlook*. Aite Group, Inc. https://aite-novarica.com/report/emv-lessons-learned-and-us-outlookControlScan. (2012). *Benchmarking level 4 merchant PCI compliance: The acquirer's perspective*. https://www.controlscan.com/the-acquirers-perspective-on-compliance-white-paper/

ControlScan. (2014). *Building momentum: The third annual survey of the acquirer's perspective on level 4 merchant PCI compliance*. https://www.controlscan.com/the-acquirers-perspective-on-compliance-white-paper/

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

Critchley, T. (2015). Why DTMF masking is critical to payment security. *Computer Fraud & Security*, *2015*(11), 8–10. https://doi.org/10.1016/S1361-3723(15)30101-9

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, *33*(4), 425–435. https://doi.org/10.1108/MAJ-11-2017-1692

Dai, J., Mulva, S., Suk, S. J., & Kang, Y. (2012, May). Cost Normalization for Global Capital Projects Benchmarking. In *2012 Construction Research Congress* (pp. 2400–2409). American Society of Civil Engineers. https://doi.org/10.1061/9780784412329.241

Dandurand, L., & Serrano, O. S. (2013, June). Towards improved cyber security information sharing. In K. Podins, J. Stinissen, M. Maybaum (Eds.), *2013 5th*

International Conference on Cyber Conflict (CyCon) (pp. 1–16). IEEE.

Data Axle. (2020). *Data quality*. Retrieved January 10, 2021 from https://www.dataaxleusa.com/about-us/data-quality/

DeVon, H. A., Block, M. E., Moyle-Wright, P., Ernst, D. M., Hayden, S. J., Lazzara, D. J., Savoy, S. M., & Kostas-Polston, E. (2007). A psychometric toolbox for testing validity and reliability. *Journal of Nursing Scholarship*, *39*(2), 155–164. https://doi.org/10.1111/j.1547-5069.2007.00161.x

Diem, K. G. (2004). *A step-by-step guide to developing effective questionnaires and survey procedures for program evaluation & research*, 1–6. Rutgers-Cook College. http://fs.cahnrs.wsu.edu/wp-content/uploads/2015/09/A-Step-By-Step-Guide-to-Developing-Effective-Questionnaires.pdf

Dixit, A. K., Dixit, R. K., & Pindyck, R. S. (1994). *Investment under uncertainty.* Princeton University Press. https://doi.org/10.1515/9781400830176

Doane, D. P., & Seward, L. E. (2011). Measuring skewness: A forgotten statistic? *Journal of Statistics Education*, *19*(2), 1–18. https://doi.org/10.1080/10691898.2011.11889611

Donaldson, L. (2003). Organization theory as a positive science. In H. Tsoukas & C. Knudsen (Eds.), *The Oxford handbook of organization theory: Meta-theoretical perspectives* (pp. 39–62). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199275250.003.0002

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers & Security*, *63*, 1–13.

https://doi.org/10.1016/j.cose.2016.09.006

Dumanska, I., Hrytsyna, L., Kharun, O., & Matviiets, O. (2021). E-commerce and m-commerce as global trends of international trade caused by the COVID-19 pandemic. *WSEAS Transactions on Environment and Development*, *17*, 386–397. https://doi.org/10.37394/232015.2021.17.38

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and cybersecurity risk management. *Current Issues in Auditing*, *13*(2), C1–C9. https://doi.org/10.2308/ciia-52419

Economides, N. (1999). Real options and the costs of the local telecommunications network. In J. Alleman & E. Noam (Eds.), *The New Investment Theory of Real Options and its Implications for the Cost Models in Telecommunications (Vol. 34).* Springer Science & Business Media. https://doi.org/10.2139/ssrn.175128

Edwards, W. (1961). Behavioral decision theory. *Annual Review of Psychology*, *12*(1), 473–498. https://doi.org/10.1146/annurev.ps.12.020161.002353

Eichfelder, S., & Vaillancourt, F. (2014). *Tax compliance costs: A review of cost burdens and cost structures*. (SSRN Working Paper No. 2535664). https://doi.org/10.2139/ssrn.2535664

Eilts, D., & Levy, Y. (2018). *Towards an empirical assessment of cybersecurity readiness and resilience in small businesses*. Paper presented at 2018 KSU Conference on Cybersecurity Education, Research and Practice, Kansas, 18–30. https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1080&context=ccerp

Ekelund, S., & Iskoujina, Z. (2019). Cybersecurity economics–balancing operational security spending. *Information Technology & People*, 1–36. https://doi.org/10.1108/ITP-05-2018-0252

El Madhoun, N., Bertin, E., & Pujolle, G. (2018). An overview of the EMV protocol and its security vulnerabilities. In *2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ)* (pp. 1–5). IEEE. https://doi.org/10.1109/MOBISECSERV.2018.8311444

Emerson, R. W. (2021). Convenience sampling revisited: Embracing its limitations through thoughtful study design. *Journal of Visual Impairment & Blindness*, *115*(1), 76–78. https://doi.org/10.1177/0145482X20987707

Farrokhi, F., & Mahmoudi-Hamidabad, A. (2012). Rethinking convenience sampling: Defining quality criteria. *Theory & Practice in Language Studies*, *2*(4). https://doi.org/10.4304/tpls.2.4.784-792

Fichman, R. G. (2004). Real options and IT platform adoption: Implications for theory and practice. *Information Systems Research*, *15*(2), 132–154. https://doi.org/10.1287/isre.1040.0021

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Fifer, R. M. (1989). Cost benchmarking functions in the value chain. *Planning Review*, *17*(3), 18. https://doi.org/10.1108/eb054255

Finch, W. H., Bolin, J. E., & Kelley, K. (2019). *Multilevel modeling using R*. CRC Press.

https://doi.org/10.1201/9781351062268

Flamholtz, E. G., Das, T. K., & Tsui, A. S. (1985). Toward an integrative framework of organizational control. *Accounting, Organizations and Society*, *10*(1), 35–50. https://doi.org/10.1016/0361-3682(85)90030-3

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. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

Galesic, M., & Bosnjak, M. (2009). Effects of questionnaire length on participation and indicators of response quality in a web survey. *Public Opinion Quarterly*, *73*(2), 349–360. https://doi.org/10.1093/poq/nfp031

Ghaisas, S., Motwani, M., Balasubramaniam, B., Gajendragadkar, A., Kelkar, R., & Vin, H. (2015). Towards automating the security compliance value chain. In *Proceedings of the 2015 10th Joint Meeting on Foundations of Software Engineering (ESEC/FSE 2015)* (pp. 1014–1017). ACM. https://doi.org/10.1145/2786805.2804435

Gibson, A. M. (2017). Internal control: The human risk factor. *Faculty Publications. 552*. https://digitalcommons.andrews.edu/pubs/552

Gordon, L. A. (2004). *Managerial accounting: Concepts and empirical evidence.* McGraw Hill.

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. https://doi.org/10.1145/581271.581274

Gordon, L. A., & Loeb, M. P. (2006a). Budgeting process for information security expenditures. *Communications of the ACM*, *49*(1), 121–125. https://doi.org/10.1145/1107458.1107465

Gordon, L. A., & Loeb, M. P. (2006b). *Managing cyber-security resources: A cost-benefit analysis*. McGraw Hill.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, *19*, 1–7.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). *Reducing the challenges to making cybersecurity investments in the private sector: Department of Homeland Security contract #N66001-112-C-0132: Final Report*, 1–148. Retrieved January 10, 2021, from https://cpppe.umd.edu/sites/default/files/2020-05/UMD_11012_Reducing the Challenges to Making Cybersecurity Investments in the Private Sector_June 2015.pdf

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, *6*, 24–30. https://doi.org/10.4236/jis.2015.61003

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015c). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. https://doi.org/10.1093/cybsec/tyv011

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015d). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*, 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2018). Empirical evidence on the determinants of cybersecurity investments in private sector firms. *Journal of Information Security*, *9*, 133–153. https://doi.org/10.4236/jis.2018.92010

Gordon, L. A., Miller, D., & Mintzberg, H. (1975). *Normative models in managerial decision-making*. National Association of Accountants.

Gordon, L. A., & Pinches, G. E. (1984). *Improving capital budgeting: A decision support system approach*. Addison-Wesley Publishing Company, 1–116.

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), 60. https://doi.org/10.5430/ijba.v6n2p60

Greene, W. H. (2003). *Econometric analysis*. Pearson Education.

Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*. https://doi.org/10.1108/MAJ-09-2018-2004

Harrell, F. E. (2015). *Regression modeling strategies*. Vanderbilt University of Medicine. https://doi.org/10.1007/978-3-319-19425-7

Hassan, T. A., & Mertens, T. M. (2017). The social cost of near-rational investment. *American Economic Review*, *107*(4), 1059–1103. https://doi.org/10.1257/aer.20110433

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the US retail economy: Restoring confidence in information technology security standards. *Technology in Society*, *44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007

Herath, H. S. B., & Herath, T. C. (2008). Investments in information security: A real options perspective with Bayesian post audit. *Journal of Management Information Systems*, *25*(3), 337–375. https://doi.org/10.2753/MIS0742-1222250310

Hussein, A. S., Khairy, R. S., Najeeb, S. M. M., & al-Rikabi, H. T. (2021). Credit card fraud detection using fuzzy rough nearest neighbor and sequential minimal optimization with logistic regression. *International Journal of Interactive Mobile Technologies*, *15*(5), 24–42. https://doi.org/10.3991/ijim.v15i05.17173

IBM. (2021). *Cost of a data breach report 2021*. https://www.ibm.com/security/data-breach

Ibragimova, B., Ryan, S. D., Windsor, J. C., & Prybutok, V. R. (2012). Understanding the antecedents of knowledge sharing: An organizational justice perspective. *Informing Science: The International Journal of an Emerging Transdiscipline*, *15*, 183–205. https://doi.org/10.28945/1694

Imenda, S. (2014). Is there a conceptual difference between theoretical and conceptual frameworks? *Journal of Social Sciences*, *38*(2), 185–195. https://doi.org/10.1080/09718923.2014.11893249

ISACA. (2020). *Code of professional ethics*. https://www.isaca.org/credentialing/code-of-professional-ethics

ISC2. (2020). *Code of ethics*. https://www.isc2.org/Ethics

Islam, M. S., Farah, N., & Stafford, T. F. (2018). Factors associated with security/cybersecurity audit by internal audit function. *Managerial Auditing Journal*, *33*(4), 377–409. https://doi.org/10.1108/MAJ-07-2017-1595

Israel, G. D. (1992). *Determining sample size.* University of Florida Cooperative Extension Service, Institute of Food and Agriculture Sciences, EDIS.

Itang, A. E. (2020). Do small and medium enterprises optimally utilize computerized accounting systems internal controls? An empirical study. *Research Journal of Finance and Accounting*, *11*(20), 16–28. https://doi.org/10.7176/RJFA/11-17-03

Janakiraman, R., Joon H. L., Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(March 2018), 85–105. https://doi.org/10.1509/jm.16.0124

Johnson, A. M. (2009). Business and security executives' views of information security investment drivers: Results from a Delphi study. *Journal of Information Privacy and Security*, *5*(1), 3–27. https://doi.org/10.1080/15536548.2009.10855855

Johnson, D. R., & Creech, J. C. (1983). Ordinal measures in multiple indicator models: A simulation study of categorization error. *American Sociological Review*, *48*, 398–407. https://doi.org/10.2307/2095231

Kaplan, R. S., & Mikes, A. (2016). Risk management—The revealing hand. *Journal of Applied Corporate Finance*, *28*(1), 8–18. https://doi.org/10.1111/jacf.12155

Karthikeyan, C., Krishna, & Benjamin, A. (2019). A conceptual and analytical study on modern compliance reporting for corporate performance management: A technobusiness leadership perspective. *International Journal of Research in Social Sciences*, *9*(4), 100–130. https://www.ijmra.us/2019ijrss_april.php

Keith, T. Z. (2019). *Multiple regression and beyond: An introduction to multiple regression and structural equation modeling*. Routledge. https://doi.org/10.4324/9781315162348

Kelley, K., & Maxwell, S. E. (2003). Sample size for multiple regression: Obtaining regression coefficients that are accurate, not simply significant. *Psychological Methods*, *8*(3), 305. https://doi.org/10.1037/1082-989X.8.3.305

Kim, J. H. (2019). Multicollinearity and misleading statistical results. *Korean Journal of Anesthesiology*, *72*(6), 558. https://doi.org/10.4097/kja.19087

Kosutic, D., & Pigni, F. (2020). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy*, 1–9. https://doi.org/10.1108/JBS-06-2020-0116

Krotov, V. (2016). Using regression analysis to address methodological and theoretical issues in IT cost benchmarking. *Electronic Journal of Information Systems Evaluation*, *19*(1), 22–35. https://academic-publishing.org/index.php/ejise/article/view/169

Kulatilaka, N. (1995). The value of flexibility: A general model of real options. *Real Options in Capital Investment: Models, Strategies, and Applications*, 89–107.

Kulatilaka, N., & Marcus, A. J. (1988). General formulation of corporate real options. *Research in Finance*, *7*, 183–199.

Kusserow, R. P. (2014). Metrics to evidence and benchmark compliance program effectiveness. *Journal of Health Care Compliance*, *16*(6), 49–52.

Larsson, S., Jensen-Urstad, A., & Heintz, F. (2021). Notified but unaware: Third-party tracking online. *Critical Analysis of Law*, *8*(1), 101–120. https://cal.library.utoronto.ca/index.php/cal/article/download/36282/27585

Levy, M., & Powell, P. (2003). Exploring SME internet adoption: Towards a contingent model. *Electronic Markets*, *13*(2), 173–181. https://doi.org/10.1080/1019678032000067163

Li, X., & Johnson, J. D. (2002). Evaluate IT investment opportunities using real options theory. *Information Resources Management Journal (IRMJ)*, *15*(3), 32–47. https://doi.org/10.4018/irmj.2002070103

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257–266. https://doi.org/10.1016/j.bushor.2016.01.002

Martakis, A. (2015). *Framework for enterprise uncertainty-driven decision-making: FEUD* [Master's thesis]. University of Twente. http://purl.utwente.nl/essays/68738

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Mason, S. P., & Merton, R. C. (1985). The role of contingent claims analysis in corporate finance. In E. Altman and M. Subrahmanyam (Eds.), *Recent Advances in Corporate Finance*, (pp. 9–54), Richard D. Irwin. https://doi.org/10.1142/9789814759588_0005

Matthews, H. S., & Lave, L. B. (2003). Using input-output analysis for corporate benchmarking. *Benchmarking: An International Journal*, *10*(2), 152–167. https://doi.org/10.1108/14635770310469671

McGrath, R. G. (1999). Falling forward: Real options reasoning and entrepreneurial failure. *Academy of Management Review*, *24*(1), 13–30. https://doi.org/10.5465/amr.1999.1580438

Mishra, P., Pandey, C. M., Singh, U., Gupta, A., Sahu, C., & Keshri, A. (2019). Descriptive statistics and normality tests for statistical data. *Annals of Cardiac Anaesthesia*, *22*(1), 67–72. https://doi.org/10.4103/aca.ACA_157_18

Momentive. (2021a). *How we find survey participants around the world*. https://www.surveymonkey.com/mp/find-survey-participants/

Momentive. (2021b). *Making responses anonymous.* https://help.surveymonkey.com/articles/en_US/kb/How-do-I-make-surveys-anonymous

Momentive. (2021c). *Marketing research solutions*. https://www.surveymonkey.com/market-research/solutions/audience-panel/

Momentive. (2021d). *Response quality across online sources.* https://prod.smassets.net/assets/cms/sm/uploads//Audience-Data-Quality-Study-v2.pdf

Moore, T., & Anderson, R. (2012). Internet security. *The Oxford Handbook of the Digital Economy*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195397840.013.0021

Moore, T., Dynes, S., & Chang, F. R. (2016, June). Identifying how firms manage cybersecurity investment. *Proceedings of the 15th Annual Workshop on Economics of Information Security (WEIS)*, 1-32. https://cpb-us-w2.wpmucdn.com/blog.smu.edu/dist/e/97/files/2015/10/SMU-IBM.pdf

Müller, C. (2020). *Challenges and Opportunities in the Due Diligence Process: Illustrated on Packaging Machinery Industry*. Tectum Wissenschaftsverlag. https://doi.org/10.5771/9783828876545

Mulligan, D. K., & Schneider, F. B. (2011). Doctrine for cybersecurity. *Daedalus, 140*(4), 70–92. https://doi.org/10.1162/DAED_a_00116

Myers, J. (2019). *Modeling continuous variables: Multiple regression*.

Myers, S. C. (1977). Determinants of corporate borrowing. *Journal of Financial Economics*, *5*(2), 147–175. https://doi.org/10.1016/0304-405X(77)90015-0

Myers, S. C. (1984). Finance theory and financial strategy. *Interfaces*, *14*(1), 126–137. https://doi.org/10.1287/inte.14.1.126

Nagurney, A., Daniele, P., & Shukla, S. (2017). A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of Operations Research*, *248*(1–2), 405–427. https://doi.org/10.1007/s10479-016-2209-1

NAICS Association. (2022). *NAICS code description*. https://www.naics.com/naics-code-description/?code=44-45

National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. (1979). *The Belmont report: Ethical principles and* *guidelines for the protection of human subjects of research*. U.S. Department of Health and Human Services. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

National Institute of Standards and Technology. (2018). *NIST special publication 800-37 Revision 2: Risk management framework for information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-37r2

Neuhaus, S., & Plattner, B. (2013). Software security economics: Theory, in practice. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 75–92). Springer. https://doi.org/10.1007/978-3-642-39498-0_4

Nicho, M., & Fakhry, H. (2013). An integrated security governance framework for effective PCI DSS implementation. *International Journal of Information Security and Privacy*, *5*(3), 50–67. https://doi.org/10.4018/978-1-4666-2050-6.ch012

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8–20. https://doi.org/10.1111/j.1745-6622.2006.00106.x

Parashar, P., & Bhati, P. (2020). Credit card fraud detection using machine learning algorithms. *International Research Journal in Advanced Science & Technology (IRJAST)*, *1*(1), 5–8. https://www.irjast.org/archives/vol-1-issue-1/V1I1P002.pdf

Paul, J. A., & Wang, X. J. (2019). Socially optimal IT investment for cybersecurity. *Decision Support Systems*, *122*, 113069. https://doi.org/10.1016/j.dss.2019.05.009

PCI Security Standards Council. (2014). *PCI SSC code of professional responsibility, v 1.0.*

https://www.pcisecuritystandards.org/documents/PCI_SSC_Code_of_Professional_Responsibility.pdf

PCI Security Standards Council. (2016). *PCI DSS and PA-DSS glossary of terms, abbreviations, and acronyms v3.2*. https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf

PCI Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard: Requirements and security assessment procedures: v3.2.1*. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

Peterson, H. (2020, August 17). More than 7,500 stores are closing in 2020 as the retail apocalypse drags on. Here's the full list. *Business Insider*. https://www.businessinsider.com/stores-closing-in-2020-list-2020-1?op=1

Peterson, S. L. (2007). Managerial turnover in US retail organizations. *Journal of Management Development*, *26*(8), 770–789. https://doi.org/10.1108/02621710710777273

Pham Evans, M. T., Tisak, D. J., & Williamson, D. F. (2012). Twenty-first century benchmarking: Searching for the next generation. *Benchmarking: An International Journal*, *19*(6), 760–780. https://doi.org/10.1108/14635771211284314

Pindyck, R. S. (1991). Irreversibility, uncertainty and investment. *Journal of Economic Literature*, 1110–1148. https://EconPapers.repec.org/RePEc:aea:jeclit:v:29:y:1991:i:3:p:1110-48

Pivorienė, A. (2017). Real options and discounted cash flow analysis to assess strategic investment projects. *Economics and Business*, *30*(1), 91–101. https://doi.org/10.1515/eb-2017-0008

Port, D., & Wilf, J. (2017, January). A Decision-Theoretic Approach to Measuring Security. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 6100–6109). https://doi.org/10.24251/HICSS.2017.737

Prabowo, H. Y. (2011). Building our defence against credit card fraud: A strategic view. *Journal of Money Laundering Control*, *14*(4), 371–386. https://doi.org/10.1108/13685201111173848

Raghavan, K., Desai, M. S., & Rajkumar, P. V. (2017). Managing cybersecurity and e-commerce risks in small businesses. *Journal of Management Science and Business Intelligence*, *2017*(2–1), 9–15. https://doi.org/10.5281/zenodo.581691

Rahimian, F., Bajaj, A., & Bradley, W. (2016). Estimation of deficiency risk and prioritization of information security controls: A data-centric approach. *International Journal of Accounting Information Systems*, *20*, 38–64. https://doi.org/10.1016/j.accinf.2016.01.004

Raiffa, H., & Schlaifer, R. (1961). *Applied statistical decision theory*. Harvard University.

Rajaniemi, K. (2007). Internet-based scanning of the competitive environment. *Benchmarking: An International Journal*, *14*(4), 465–481. https://doi.org/10.1108/14635770710761870

Rasheed, H. (2011). Auditing for standards compliance in the cloud: Challenges and directions. *The International Arab Journal of Information Technology*.

Rashmi, S., Roopashree, S., & Sathiyamoorthi, V. (2021). Challenges for convergence of cloud and IoT in applications and edge computing. In *Challenges and Opportunities for the Convergence of IoT, Big Data, and Cloud Computing* (pp. 17–36). IGI Global. https://doi.org/10.4018/978-1-7998-3111-2.ch002

Rasmussen, J. (1997). Risk management in a dynamic society a modelling problem. *Safety Science*, *27*(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Rees, J. (2012). Tackling the PCI DSS challenges. *Computer Fraud & Security*, *2012*(1), 15–17. https://doi.org/10.1016/S1361-3723(12)70009-X

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. https://doi.org/10.1016/j.dss.2011.02.013

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, *65*, 77–89. https://doi.org/10.1016/j.cose.2016.10.009

Saha, A., & Sanyal, S. (2015). *Review of considerations for mobile device based secure access to financial services and risk handling strategy for CIOs, CISOs and CTOs*. arXiv. https://doi.org/10.48550/arXiv.1502.00724

Seera, M., Lim, C. P., Kumar, A., Dhamotharan, L., & Tan, K. H. (2021). An intelligent payment card fraud detection system. *Annals of Operations Research*, 1–23.

https://doi.org/10.1007/s10479-021-04149-2

Segal, L., Ngugi, B., & Mana, J. (2011). Credit card fraud: A new perspective on tackling an intransigent problem. *Fordham Journal of Corporate & Financial Law*, *743–781*.

Senaviratna, N. A. M. R., & Cooray, T. M. J. A. (2019). Diagnosing multicollinearity of logistic regression model. *Asian Journal of Probability and Statistics*, 1–9. https://doi.org/10.9734/ajpas/2019/v5i230132

Shackelford, S. (2017). Exploring the 'shared responsibility' of cyber peace: Should cybersecurity be a human right? *Stanford Journal of International Law*, *2019*, 17–55. https://doi.org/10.2139/ssrn.3005062

Shihab, M. R., & Misdianti, F. (2014, October). Moving towards PCI DSS 3.0 compliance: A case study of credit card data security audit in an online payment company. In *Advanced Computer Science and Information Systems (ICACSIS), 2014 International Conference on* (pp. 151–156). IEEE. https://doi.org/10.1109/ICACSIS.2014.7065872

Sillince, J. A., Macdonald, S., Lefang, B., & Frost, B. (1998). Email adoption, diffusion, use and impact within small firms: A survey of UK companies. *International Journal of Information Management*, *18*(4), 231–242. https://doi.org/10.1016/S0268-4012(98)00012-7

Simon, H. A. (1960). *The new science of management decision.* Harper & Brothers. https://doi.org/10.1037/13978-000

Simpson, M. D. (2016). All your data are belong to us: Consumer data breach rights and remedies in an electronic exchange economy. *University of Colorado Law Review*, *87*, 669–709. https://lawreview.colorado.edu/volume-87/

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1977). Behavioral decision theory. *Annual Review of Psychology*, *28*(1), 1–39. https://doi.org/10.1146/annurev.ps.28.020177.000245

Smith, J. E., & McCardle, K. F. (1998). Valuing oil properties: Integrating option pricing and decision analysis approaches. *Operations Research*, *46*(2), 198–217. https://doi.org/10.1287/opre.46.2.198

Snijders, T. A., & Bosker, R. J. (2011). *Multilevel analysis: An introduction to basic and advanced multilevel modeling*. Sage.

SoGoSurvey. (2021). *Build confidence with total confidentiality.* https://www.sogosurvey.com/create-anonymous-survey/

Soltanizadeh, S., Rasid, S. Z. A., Golshan, N. M., & Ismail, W. K. W. (2016). Business strategy, enterprise risk management and organizational performance. *Management Research Review*, 1–18. https://doi.org/10.1108/MRR-05-2015-0107

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI) — A practical quantitative model. *Journal of Research and Practice in Information Technology*, *38*(1), 45–56. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.83.5483

Soper, D. S. (2021). A-priori sample size calculator for multiple regression [Software]. https://www.danielsoper.com/statcalc

Spendolini, M. (1992). *The Benchmarking Book*. Amacom.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. *Decision Support Systems*, *75*, 49–62. https://doi.org/10.1016/j.dss.2015.04.011

Stapenhurst, T. (2009). *The benchmarking book: A how-to-guide to best practice for managers and practitioners*. Butterworth-Heinemann.

Stapleton, J., & Poore, R. S. (2011). Tokenization and other methods of security for cardholder data. *Information Security Journal: A Global Perspective*, *20*(2), 91–99. https://doi.org/10.1080/19393555.2011.560923

Statista. (2020). Number of retail store openings and closures in the United States from 2017–2019. https://www.statista.com/statistics/757160/retail-store-opening-closing/

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly*, 441–469. https://doi.org/10.2307/249551

Sullivan, G. M. (2011). *A primer on the validity of assessment instruments. Journal of Graduate Medical Education*, *3*(2), 119–120. https://doi.org/10.4300/JGME-D-11-00075.1

Thaw, D. (2014). The efficacy of cybersecurity regulation. *Georgia State University Law Review*, *30(2)*, 287–374. https://doi.org/10.2139/ssrn.2241838

TransUnion. (2021). *Digital holiday fraud in 2021*. https://solutions.transunion.com/holiday-fraud-trends-infographic-2021/

Trustwave. (2019). *2019 Trustwave global security report*.

https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/

Tversky, A., & Kahneman, D. (1973). Judgment under uncertainty: Heuristics and biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Zdzikot, T. (2022). Cyberspace and cybersecurity. In K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (Eds.), *Cybersecurity in Poland* (pp. 9–31). Springer, Cham. https://doi.org/10.1007/978-3-030-78551-2_2

U.S. Census Bureau. (2020). *Data by enterprise receipt size: U.S., 6-digit NAICS*. https://www.census.gov/data/tables/2017/econ/susb/2017-susb-annual.html

U.S. Census Bureau. (2021). *U.S. and states: U.S. & states, NAICS, detailed employment sizes (U.S., 6-digit and states, NAICS sectors)*. https://www.census.gov/data/tables/2018/econ/susb/2018-susb-annual.html

Verizon. (2015). *Verizon 2015 PCI compliance report*. http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

Verizon. (2019a). *2019 data breach investigations report* (12th ed.). https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Verizon. (2019b). *2019 payment security report*. https://enterprise.verizon.com/resources/reports/2019-payment-security-fullreport-bl.pdf

Vogt, W. P. (2007). *OM8020: Quantitative research methods for professionals*. Pearson Education Inc.

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security*, *26*(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025

Wallsten, T. S. (1971). Subjectively expected utility theory and subjects' probability estimates: Use of measurement-free techniques. *Journal of Experimental Psychology*, *88*(1), 31. https://doi.org/10.1037/h0030669

Walters, R. (2014). Cyber attacks on U.S. companies in 2014. *Heritage Foundation Issue Brief*, 4289. https://www.heritage.org/defense/report/cyber-attacks-us-companies-2014

Weiss, N. E., & Miller, R. S. (2015). The Target and other financial data breaches: Frequently asked questions. *Congressional Research Service*, 1–33. https://fas.org/sgp/crs/misc/R43496.pdf

Widaman, K. F. (2018). On common factor and principal component representations of data: Implications for theory and for confirmatory replications. *Structural Equation Modeling: A Multidisciplinary Journal*, *25*(6), 829–847. https://doi.org/10.1080/10705511.2018.1478730

Willey, L., & White, B. J. (2013). Teaching case: Do you take credit cards? Security and compliance for the credit card payment industry. *Journal of Information Systems Education*, *24*(3). http://jise.org/Volume24/n3/JISEv24n3p181.pdf

Williams, B. R. (2010). How tokenization and encryption can enable PCI DSS compliance. *Information Security Technical Report*, *15*(4), 160–165. https://doi.org/10.1016/j.istr.2011.02.005

Williams, B. R., & Chuvakin, A. (2014). *PCI compliance: Understand and implement effective PCI data security standard compliance*. Syngress.

Wilson, S. (2012). Calling for a uniform approach to card fraud offline and on. *Journal of Internet Banking and Commerce*, *17*(3), 1–5. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.299.6922&rep=rep1&type=pdf

Witte, J. C., Amoroso, L. M., & Howard, P. E. (2000). Research methodology: Method and representation in Internet-based survey tools—Mobility, community, and cultural identity in Survey2000. *Social Science Computer Review*, *18*(2), 179–195. https://doi.org/10.1177/089443930001800207

Work Institute. (2019). *2020 retention report: Insights on 2019 turnover trends, reasons, costs & recommendations*, 1–40. https://info.workinstitute.com/hubfs/2020%20Retention%20Report/Work%20Institutes%202020%20Retention%20Report.pdf

Zhao, W., & White, G. (2017, January). An evolution roadmap for community cyber security information sharing maturity model. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 2369–2378). https://doi.org/10.24251/HICSS.2017.287

Appendix A: Management Journals Searched

The following business and management journals were included in searches within the Walden University online library:

Academy of Business Journal
Academy of Business Research Journal
Academy of Educational Leadership Journal
Academy of Information and Management Sciences Journal
Academy of Management Journal
Academy of Management Learning and Education
Academy of Management Perspectives
Academy of Management Review
Academy of Strategic Management Journal
AD-minister
Administrative Science Quarterly
Administrative Sciences
Advanced Management Journal
Advances in Management
Advances in Management and Applied Economics
African Journal of Business Ethics
American Business Review
American Journal of Business
Amity Management Review
Annals of Finance
Annals of Innovation & Entrepreneurship
Annual Advances in Business Cases
ABSM Journal of Management
Asci Journal of Management
Asia Pacific Journal of Management
Asia Pacific Management Review = APMR
Asian Business & Management
Australian Journal of Management

Aweshakar Research Journal
Baltic Journal of Management
BAR. Brazilian Administration Review
Benchmarking: An International Journal
Board Leadership: Policy Governance in Action
Brazilian Business Review (English Edition)
British Journal of Administrative Management
British Journal of Industrial Relations
British Journal of Management
Business and Society Review
Business Case Journal
Business Forum
Business Journal of Hispanic Research
Business Management Dynamics
Business Process Management Journal
Business Renaissance Quarterly
Business Systems Research
BVIMR Management Edge
C O R S Journal
California Management Review
Canadian Journal of Administrative Sciences
Chinese Management Studies
Clinician in Management
Computational Management Science
Consulting to Management
Contemporary Management Research
Corporate Governance: An International Review
Corporate Knights Magazine
Corporate Reputation Review
Creativity and Innovation Management
Cross Cultural Management: An International Journal
Current Topics in Management
Decision Support Systems

Drishtikon: A Management Journal
E-Journal of Organizational Learning and Leadership
Economics, Management, and Financial Markets
EconoQuantum
Electronic Journal of Business Research Methods
Electronic Journal of Knowledge Management
Emergence
Emory Bankruptcy Developments Journal
Enterprise & Innovation Management Studies
Euro Asia Journal of Management
European Journal of Innovation Management
European Management Journal
European Management Review
Executive: An Academy of Management Publication
Executive Development
Financial Executive
Financial Management: The Magazine from CIMA
Future Studies Research Journal: Trends and Strategies
Gazi University Journal of Economics & Administrative Sciences
Global Business and Management Research: An International Journal
Global Management Journal
Global Management Review
Global Partnership Management Journal
Globsyn Management Journal
Group & Organization Management: An International Journal
Group Decision & Negotiation
Handbook of Business Strategy
Health Care Management Science
Human Resource Management International Digest
Human Systems Management
I-Manager’s Journal on Management
ICFAI Journal of Bank Management
ICFAI Journal of Brand Management

ICFAI Journal of Business Strategy
ICFAI Journal of Corporate Governance
ICFAI Journal of Entrepreneurship Development
ICFAI Journal of Infrastructure
ICFAI Journal of Knowledge Management
ICFAI Journal of Management Research
ICFAI Journal of Managerial Economics
ICFAI Journal of Marketing Management
ICFAI Journal of Operations Management
ICFAI Journal of Organizational Behavior
ICFAI Journal of Supply Chain Management
Indian Journal of Commerce & Management Studies
Industrial Management
Industrial Management & Data Systems
Industrial Management Review: IMR
Industrial Marketing Management
Industrial Relations
Industry & Innovation
Information Resources Management Journal (IRMJ)
Intangible Capital
Interdisciplinary Journal of Information, Knowledge and Management
International Journal of Agile Management Systems
International Journal of Business & Accountancy
International Journal of Business & Management Science
International Journal of Business and Information
International Journal of Business Insights & Transformation
International Journal of Business Science and Applied Management
International Journal of Business Studies
International Journal of Commerce and Management
International Journal of Contemporary Management
International Journal of E-Business Management
International Journal of Electronic Business Management
International Journal of Engineering Business Management

International Journal of Global Management Studies
International Journal of Global Management Studies Professional
International Journal of Hospitality Management
International Journal of Information Management
International Journal of Information, Business and Management
International Journal of Knowledge Management (IJKM)
International Journal of Knowledge, Culture & Change Management
International Journal of Lean Six Sigma
International Journal of Management
International Journal of Management & Information Systems
International Journal of Management & Innovation
International Journal of Management Cases
International Journal of Management Perspectives
International Journal of Management Reviews
International Journal of Management Science
International Journal of Management Science & Technology Information
International Journal of Managerial Finance
International Journal of Organization Theory and Behavior
International Journal of Production Research
International Journal of Project Management
International Journal of Quality & Reliability Management
International Journal of Quality and Service Sciences
International Journal of Quality Science
International Journal of Service Industry Management
International Journal of Strategic Communication
International Journal of Training & Development
International Journal of Value-Based Management
International Journal on Media Management
International Management Review
International Review of Management and Marketing
International Studies of Management & Organization
IPE Journal of Management
Iranian Journal of Management Studies

IUP Journal of Bank Management
IUP Journal of Business Strategy
IUP Journal of Corporate Governance
IUP Journal of Entrepreneurship Development
IUP Journal of Management Research
IUP Journal of Risk & Insurance
IUP Journal of Supply Chain Management
JABM: Journal of Accounting, Business & Management
Journal for East European Management Studies
Journal for Global Business Education
Journal of Advanced Research in Management
Journal of Advances in Management Research
Journal of Applied Management and Entrepreneurship
Journal of Applied Management Studies
Journal of Asset Management
Journal of Business & Management
Journal of Business and Entrepreneurship
Journal of Business Communication
Journal of Business Economics & Management
Journal of Business Management
Journal of Business Market Management
Journal of Business Strategies
Journal of Business Systems, Governance and Ethics
Journal of Case Research
Journal of Change Management
Journal of Collective Negotiations
Journal of Communication Management
Journal of Comparative International Management
Journal of Contemporary Management Research
Journal of Contemporary Research in Management
Journal of Contingencies & Crisis Management
Journal of Critical Incidents
Journal of Economics & Management

Journal of Economics & Management Strategy
Journal of Economics, Finance & Administrative Science
Journal of Enterprise Information Management
Journal of Enterprising Communities: People and Places in The Global Economy
Journal of Family Business Management
Journal of General Management
Journal of Global Business and Technology
Journal of Global Management
Journal of High Technology Management Research
Journal of Intellectual Capital
Journal of International Management
Journal of King Abdulaziz University: Economics & Administration
Journal of Knowledge Management
Journal of Leadership & Organizational Studies
Journal of Leadership Studies
Journal of Management
Journal of Management & Business Research
Journal of Management & Economics
Journal of Management & Governance
Journal of Management & Organization
Journal of Management Accounting Research
Journal of Management Control
Journal of Management Development
Journal of Management Education: A Publication of the OBTS Teaching Society for Management Educators
Journal of Management History
Journal of Management Inquiry
Journal of Management Policy & Practice
Journal of Management Research
Journal of Management Science
Journal of Managerial Issues
Journal of Managerial Psychology
Journal of Managerial Sciences

Journal of Market-Focused Management
Journal of Marketing & Management
Journal of Medical Practice Management: MPM
Journal of Ministry Marketing & Management
Journal of Modelling in Management
Journal of Organizational Change Management
Journal of Organizational Computing and Electronic Commerce
Journal of Organizational Culture, Communications and Conflict
Journal of Organizational Excellence
Journal of Performance Management
Journal of Promotion Management
Journal of Quality Management
Journal of Quality Technology
Journal of Relationship Marketing
Journal of Risk Research
Journal of Service Research
Journal of Services Research
Journal of Small Business & Entrepreneurship
Journal of Small Business Management
Journal of Sport Management
Journal of Statistics and Management Systems
Journal of Strategic Change
Journal of Strategic Marketing
Journal of Strategy and Management
Journal of Systems Management
Journal of Technology Management in China
Journal of The Academy of Business Education
Journal of Theoretical and Applied Electronic Commerce Research
Journal of Transnational Management
Journal of Transnational Management Development
KCA Journal of Business Management
Knowledge Management for Development Journal
Knowledge Management Research & Practice

Leadership
Leadership & Organization Development Journal
Leadership in Action
LogForum
Logistics Information Management
Long Range Planning (LRP)
M@N@Gement
Management
Management (1820-0222)
Management & Marketing Journal
Management & Marketing. Challenges for The Knowledge Society
Management Accounting Quarterly
Management Communication Quarterly
Management Decision
Management Education and Development
Management International / Gestiòn Internacional
Management International Review
Management Learning: The Journal for Critical, Reflective Scholarship on Organization and Learning
Management Research and Practice
Management Research News
Management Research Review
Management Revue
Management Science
Management Science Letters
Management: Journal of Contemporary Management Issues
Management: Journal of Sustainable Business & Management Solutions in Emerging Economies
Managerial & Decision Economics
Managerial Auditing Journal
Managing Service Quality
Marmara University Journal of The Faculty of Economic & Administrative Sciences
Measuring Business Excellence
Melbourne Review

Michigan Journal of Business
MIS quarterly executive
MIT Sloan management review
National Contract Management Journal
Nonprofit Management and Leadership
Omega
Operations Management Education Review
Organization Development Journal
Organization Management Journal
Organization Science
Organizational Dynamics
Paradigm
Polish Journal of Management Studies
Portuguese Journal of Management Studies
Pranjana: The Journal of Management Awareness
Problems & Perspectives in Management
Production and Inventory Management Journal
Project Management Journal
Public Management Review
Public Management: An International Journal of Research and Theory
Public Personnel Management
Qualitative Research in Accounting & Management
Qualitative Research in Organizations and Management: An International Journal
Records Management Quarterly
Research in Organizational Behavior
Research Management Review
Review of General Management
Review of Management
Review of Management Innovation & Creativity
Review of Managerial Science
Risk Decision and Policy
SAM Advanced Management Journal
Scandinavian Journal of Management

Scientific Papers of The University of Pardubice. Series D, Faculty of Economics & Administration
SCMS Journal of Indian Management
Serbian Journal of Management
Service Business
SIES Journal of Management
Singapore Management Review
Sloan Management Review
Smart Business Los Angeles
Social Enterprise Journal
South African Journal of Business Management
South African Journal of Information Management
South Asian Journal of Management
Strategic Finance
Strategic Management Journal
Strategic Organization
Studies in Business and Economics
Suleyman Demirel University, The Journal of Faculty of Economics & Administrative Sciences
Supply Chain Forum: An International Journal
Team Performance Management
The Academy of Management Executive
The Coastal Business Journal
The International Entrepreneurship and Management Journal
The International Food and Agribusiness Management Review
The International Journal of Management Education
The International Journal of Organizational Analysis
The Leadership Quarterly
The TQM Journal
The TQM Magazine
Tourism & Hospitality Management
Tourism Management
Training and Management Development Methods
Universia Business Review

Vezetéstudomány / Budapest Management Review
Vidwat: The Indian Journal of Management
Vikalpa: The Journal for Decision Makers
Vilakshan: The Ximb Journal of Management
Work Study

Appendix B: Technology Journals Searched

The following technology journals were included in searches within the Walden University online library:

Bulletin of The Association for Business Communication
Business Communication Quarterly
CLEAR International Journal of Research in Management, Sciences & Technology
College and University Media Review
Collnet Journal of Scientometrics & Information Management
Computer
Computers & Operations Research
Corporate Communications: An International Journal
Decision Analysis
Electronic Commerce Research
EMedia Professional
Engineering & Technology
IEEE Engineering Management Review
IEEE Transactions on Computers
IEEE Transactions on Engineering Management
Information and Systems Engineering
Information Design Journal: IDJ
Information Systems Journal
Information Systems Management
INFORMS Journal on Computing
International Commerce Review
International Journal of Cases on Electronic Commerce (IJCEC)
International Journal of E-Business Development
International Journal of E-Business Research (IJEBR)
International Journal of Electronic Business Management
International Journal of Electronic Commerce
International Journal of Electronic Commerce Studies
International Journal of Energy Sector Management
International Journal of Enterprise Information Systems (IJEIS)
International Journal of Strategic Communication
International Journal of Web Services Research (IJWSR)
International Journal on Media Management

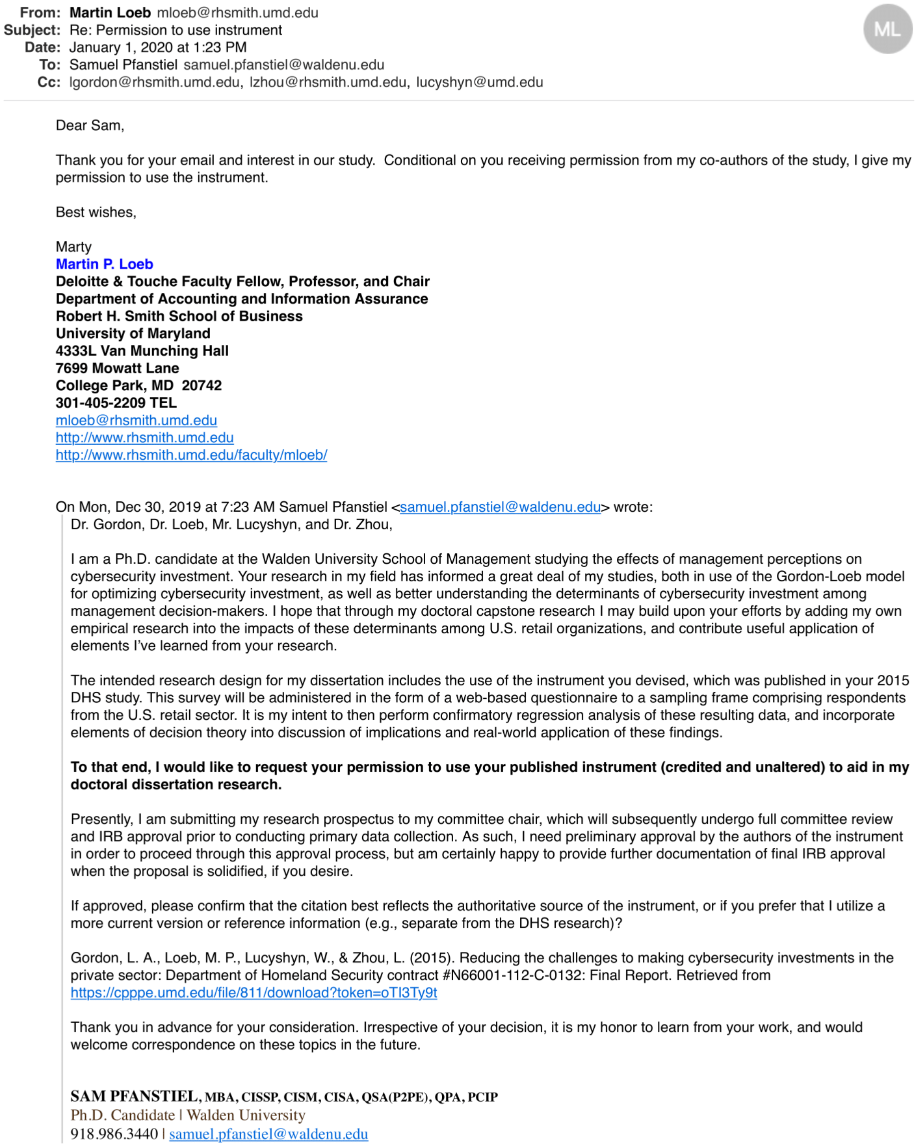
International Transactions in Operational Research
Journal of Business and Technical Communication
Journal of Business Communication
Journal of Electronic Commerce in Organizations (JECO)
Journal of Electronic Commerce Research
Journal of Global Information Management (JGIM)
Journal of Global Information Technology Management
Journal of Information Systems
Journal of Internet Commerce
Journal of Marketing & Communication
Journal of Organizational Culture, Communications and Conflict
Journal of Strategic E-Commerce
Journal of Technical Writing and Communication
Journal of Technology Management & Innovation
Journal of Telecommunications Management
Journal of Textile and Apparel Technology and Management
Journal of The American Taxation Association
Journal of Theoretical and Applied Electronic Commerce Research
Journal on Chain and Network Science
Management Communication Quarterly
MIS Quarterly
Operations Research
Review of The Electronic and Industrial Distribution Industries
Scandinavian Journal of Information Systems
The International Journal of Applied Management and Technology
The International Journal of Life Cycle Assessment
The Journal of Strategic Information Systems
The Quarterly Journal of Electronic Commerce: QJEC

Appendix C: Approval to Use Instrument

Approval was obtained by the authors of the instrument used in this study, as provided below:

Figure C1

Approval From Martin Loeb



From: **Martin Loeb** mloeb@rhsmith.umd.edu
Subject: Re: Permission to use instrument
Date: January 1, 2020 at 1:23 PM
To: Samuel Pfanstiel samuel.pfanstiel@waldenu.edu
Cc: lgordon@rhsmith.umd.edu, lzhou@rhsmith.umd.edu, lucyshyn@umd.edu

Dear Sam,

Thank you for your email and interest in our study. Conditional on you receiving permission from my co-authors of the study, I give my permission to use the instrument.

Best wishes,

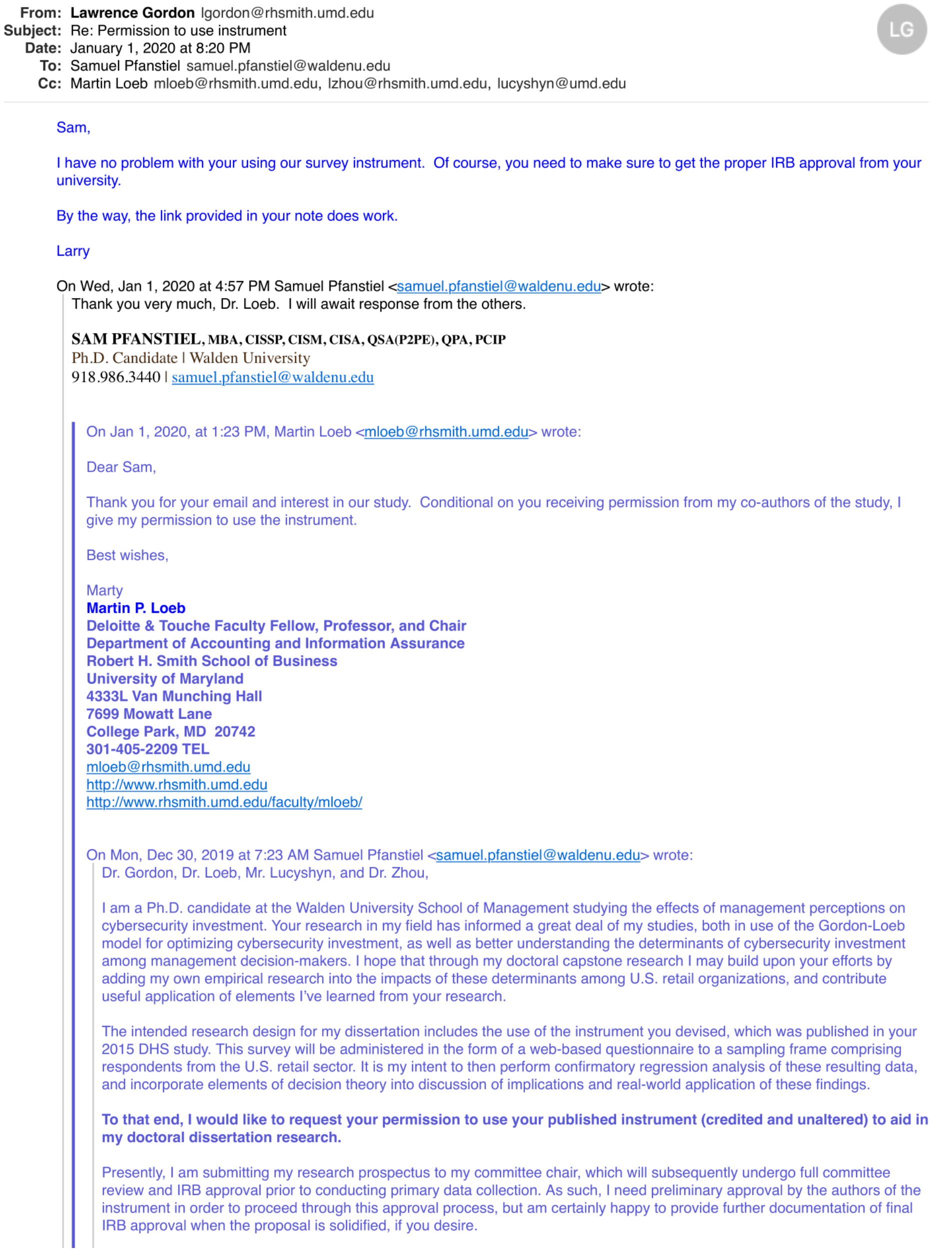
Marty
Martin P. Loeb
Deloitte & Touche Faculty Fellow, Professor, and Chair
Department of Accounting and Information Assurance
Robert H. Smith School of Business
University of Maryland
4333L Van Munching Hall
7699 Mowatt Lane
College Park, MD 20742
301-405-2209 TEL
mloeb@rhsmith.umd.edu
http://www.rhsmith.umd.edu
http://www.rhsmith.umd.edu/faculty/mloeb/

On Mon, Dec 30, 2019 at 7:23 AM Samuel Pfanstiel <samuel.pfanstiel@waldenu.edu> wrote:

> Dr. Gordon, Dr. Loeb, Mr. Lucyshyn, and Dr. Zhou,
>
> I am a Ph.D. candidate at the Walden University School of Management studying the effects of management perceptions on cybersecurity investment. Your research in my field has informed a great deal of my studies, both in use of the Gordon-Loeb model for optimizing cybersecurity investment, as well as better understanding the determinants of cybersecurity investment among management decision-makers. I hope that through my doctoral capstone research I may build upon your efforts by adding my own empirical research into the impacts of these determinants among U.S. retail organizations, and contribute useful application of elements I've learned from your research.
>
> The intended research design for my dissertation includes the use of the instrument you devised, which was published in your 2015 DHS study. This survey will be administered in the form of a web-based questionnaire to a sampling frame comprising respondents from the U.S. retail sector. It is my intent to then perform confirmatory regression analysis of these resulting data, and incorporate elements of decision theory into discussion of implications and real-world application of these findings.
>
> **To that end, I would like to request your permission to use your published instrument (credited and unaltered) to aid in my doctoral dissertation research.**
>
> Presently, I am submitting my research prospectus to my committee chair, which will subsequently undergo full committee review and IRB approval prior to conducting primary data collection. As such, I need preliminary approval by the authors of the instrument in order to proceed through this approval process, but am certainly happy to provide further documentation of final IRB approval when the proposal is solidified, if you desire.
>
> If approved, please confirm that the citation best reflects the authoritative source of the instrument, or if you prefer that I utilize a more current version or reference information (e.g., separate from the DHS research)?
>
> Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Reducing the challenges to making cybersecurity investments in the private sector: Department of Homeland Security contract #N66001-112-C-0132: Final Report. Retrieved from https://cpppe.umd.edu/file/811/download?token=oTI3Ty9t
>
> Thank you in advance for your consideration. Irrespective of your decision, it is my honor to learn from your work, and would welcome correspondence on these topics in the future.
>
> **SAM PFANSTIEL, MBA, CISSP, CISM, CISA, QSA(P2PE), QPA, PCIP**
> Ph.D. Candidate | Walden University
> 918.986.3440 | samuel.pfanstiel@waldenu.edu

Figure C2

Approval From Lawrence Gordon



From: **Lawrence Gordon** lgordon@rhsmith.umd.edu
Subject: Re: Permission to use instrument
Date: January 1, 2020 at 8:20 PM
To: Samuel Pfanstiel samuel.pfanstiel@waldenu.edu
Cc: Martin Loeb mloeb@rhsmith.umd.edu, lzhou@rhsmith.umd.edu, lucyshyn@umd.edu

Sam,

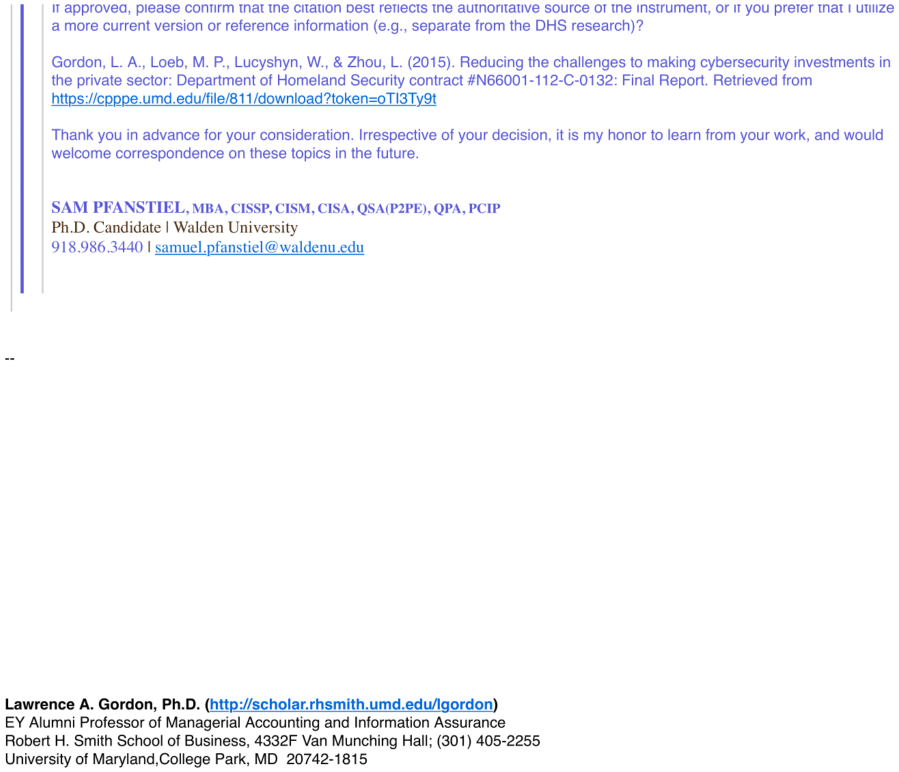
I have no problem with your using our survey instrument. Of course, you need to make sure to get the proper IRB approval from your university.

By the way, the link provided in your note does work.

Larry

On Wed, Jan 1, 2020 at 4:57 PM Samuel Pfanstiel <samuel.pfanstiel@waldenu.edu> wrote:

> Thank you very much, Dr. Loeb. I will await response from the others.
>
> **SAM PFANSTIEL, MBA, CISSP, CISM, CISA, QSA(P2PE), QPA, PCIP**
> Ph.D. Candidate | Walden University
> 918.986.3440 | samuel.pfanstiel@waldenu.edu
>
> > On Jan 1, 2020, at 1:23 PM, Martin Loeb <mloeb@rhsmith.umd.edu> wrote:
> >
> > Dear Sam,
> >
> > Thank you for your email and interest in our study. Conditional on you receiving permission from my co-authors of the study, I give my permission to use the instrument.
> >
> > Best wishes,
> >
> > Marty
> > **Martin P. Loeb**
> > **Deloitte & Touche Faculty Fellow, Professor, and Chair**
> > **Department of Accounting and Information Assurance**
> > **Robert H. Smith School of Business**
> > **University of Maryland**
> > **4333L Van Munching Hall**
> > **7699 Mowatt Lane**
> > **College Park, MD 20742**
> > **301-405-2209 TEL**
> > mloeb@rhsmith.umd.edu
> > http://www.rhsmith.umd.edu
> > http://www.rhsmith.umd.edu/faculty/mloeb/
> >
> > On Mon, Dec 30, 2019 at 7:23 AM Samuel Pfanstiel <samuel.pfanstiel@waldenu.edu> wrote:
> >
> > > Dr. Gordon, Dr. Loeb, Mr. Lucyshyn, and Dr. Zhou,
> > >
> > > I am a Ph.D. candidate at the Walden University School of Management studying the effects of management perceptions on cybersecurity investment. Your research in my field has informed a great deal of my studies, both in use of the Gordon-Loeb model for optimizing cybersecurity investment, as well as better understanding the determinants of cybersecurity investment among management decision-makers. I hope that through my doctoral capstone research I may build upon your efforts by adding my own empirical research into the impacts of these determinants among U.S. retail organizations, and contribute useful application of elements I've learned from your research.
> > >
> > > The intended research design for my dissertation includes the use of the instrument you devised, which was published in your 2015 DHS study. This survey will be administered in the form of a web-based questionnaire to a sampling frame comprising respondents from the U.S. retail sector. It is my intent to then perform confirmatory regression analysis of these resulting data, and incorporate elements of decision theory into discussion of implications and real-world application of these findings.
> > >
> > > **To that end, I would like to request your permission to use your published instrument (credited and unaltered) to aid in my doctoral dissertation research.**
> > >
> > > Presently, I am submitting my research prospectus to my committee chair, which will subsequently undergo full committee review and IRB approval prior to conducting primary data collection. As such, I need preliminary approval by the authors of the instrument in order to proceed through this approval process, but am certainly happy to provide further documentation of final IRB approval when the proposal is solidified, if you desire.



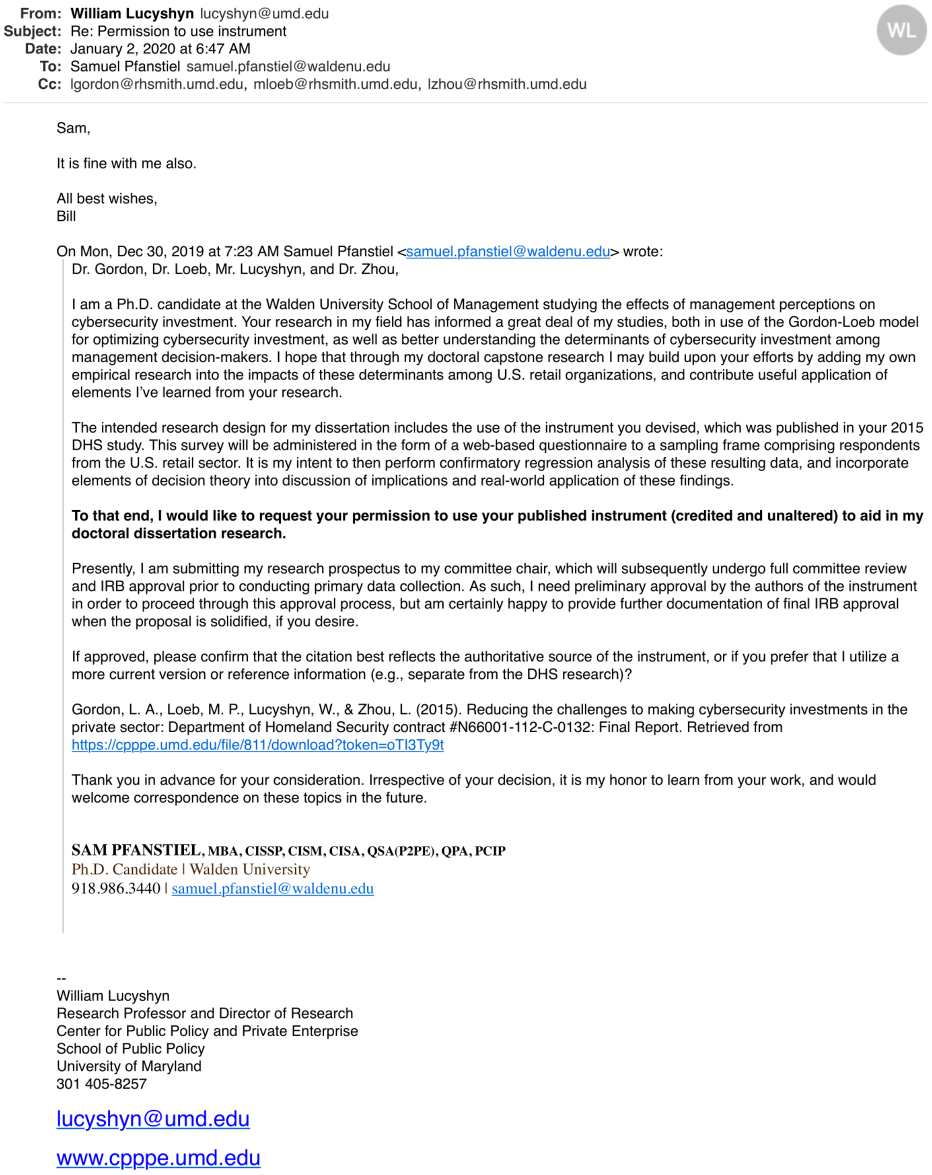
> If approved, please confirm that the citation best reflects the authoritative source of the instrument, or if you prefer that I utilize a more current version or reference information (e.g., separate from the DHS research)?
>
> Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Reducing the challenges to making cybersecurity investments in the private sector: Department of Homeland Security contract #N66001-112-C-0132: Final Report. Retrieved from https://cpppe.umd.edu/file/811/download?token=oTI3Ty9t
>
> Thank you in advance for your consideration. Irrespective of your decision, it is my honor to learn from your work, and would welcome correspondence on these topics in the future.
>
> **SAM PFANSTIEL, MBA, CISSP, CISM, CISA, QSA(P2PE), QPA, PCIP**
> Ph.D. Candidate | Walden University
> 918.986.3440 | samuel.pfanstiel@waldenu.edu

--

Lawrence A. Gordon, Ph.D. (http://scholar.rhsmith.umd.edu/lgordon)
EY Alumni Professor of Managerial Accounting and Information Assurance
Robert H. Smith School of Business, 4332F Van Munching Hall; (301) 405-2255
University of Maryland,College Park, MD 20742-1815

Figure C3

Approval From William Lucyshyn



From: **William Lucyshyn** lucyshyn@umd.edu
Subject: Re: Permission to use instrument
Date: January 2, 2020 at 6:47 AM
To: Samuel Pfanstiel samuel.pfanstiel@waldenu.edu
Cc: lgordon@rhsmith.umd.edu, mloeb@rhsmith.umd.edu, lzhou@rhsmith.umd.edu

Sam,

It is fine with me also.

All best wishes,
Bill

On Mon, Dec 30, 2019 at 7:23 AM Samuel Pfanstiel <samuel.pfanstiel@waldenu.edu> wrote:

> Dr. Gordon, Dr. Loeb, Mr. Lucyshyn, and Dr. Zhou,
>
> I am a Ph.D. candidate at the Walden University School of Management studying the effects of management perceptions on cybersecurity investment. Your research in my field has informed a great deal of my studies, both in use of the Gordon-Loeb model for optimizing cybersecurity investment, as well as better understanding the determinants of cybersecurity investment among management decision-makers. I hope that through my doctoral capstone research I may build upon your efforts by adding my own empirical research into the impacts of these determinants among U.S. retail organizations, and contribute useful application of elements I've learned from your research.
>
> The intended research design for my dissertation includes the use of the instrument you devised, which was published in your 2015 DHS study. This survey will be administered in the form of a web-based questionnaire to a sampling frame comprising respondents from the U.S. retail sector. It is my intent to then perform confirmatory regression analysis of these resulting data, and incorporate elements of decision theory into discussion of implications and real-world application of these findings.
>
> **To that end, I would like to request your permission to use your published instrument (credited and unaltered) to aid in my doctoral dissertation research.**
>
> Presently, I am submitting my research prospectus to my committee chair, which will subsequently undergo full committee review and IRB approval prior to conducting primary data collection. As such, I need preliminary approval by the authors of the instrument in order to proceed through this approval process, but am certainly happy to provide further documentation of final IRB approval when the proposal is solidified, if you desire.
>
> If approved, please confirm that the citation best reflects the authoritative source of the instrument, or if you prefer that I utilize a more current version or reference information (e.g., separate from the DHS research)?
>
> Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Reducing the challenges to making cybersecurity investments in the private sector: Department of Homeland Security contract #N66001-112-C-0132: Final Report. Retrieved from https://cpppe.umd.edu/file/811/download?token=oTI3Ty9t
>
> Thank you in advance for your consideration. Irrespective of your decision, it is my honor to learn from your work, and would welcome correspondence on these topics in the future.
>
> **SAM PFANSTIEL, MBA, CISSP, CISM, CISA, QSA(P2PE), QPA, PCIP**
> Ph.D. Candidate | Walden University
> 918.986.3440 | samuel.pfanstiel@waldenu.edu

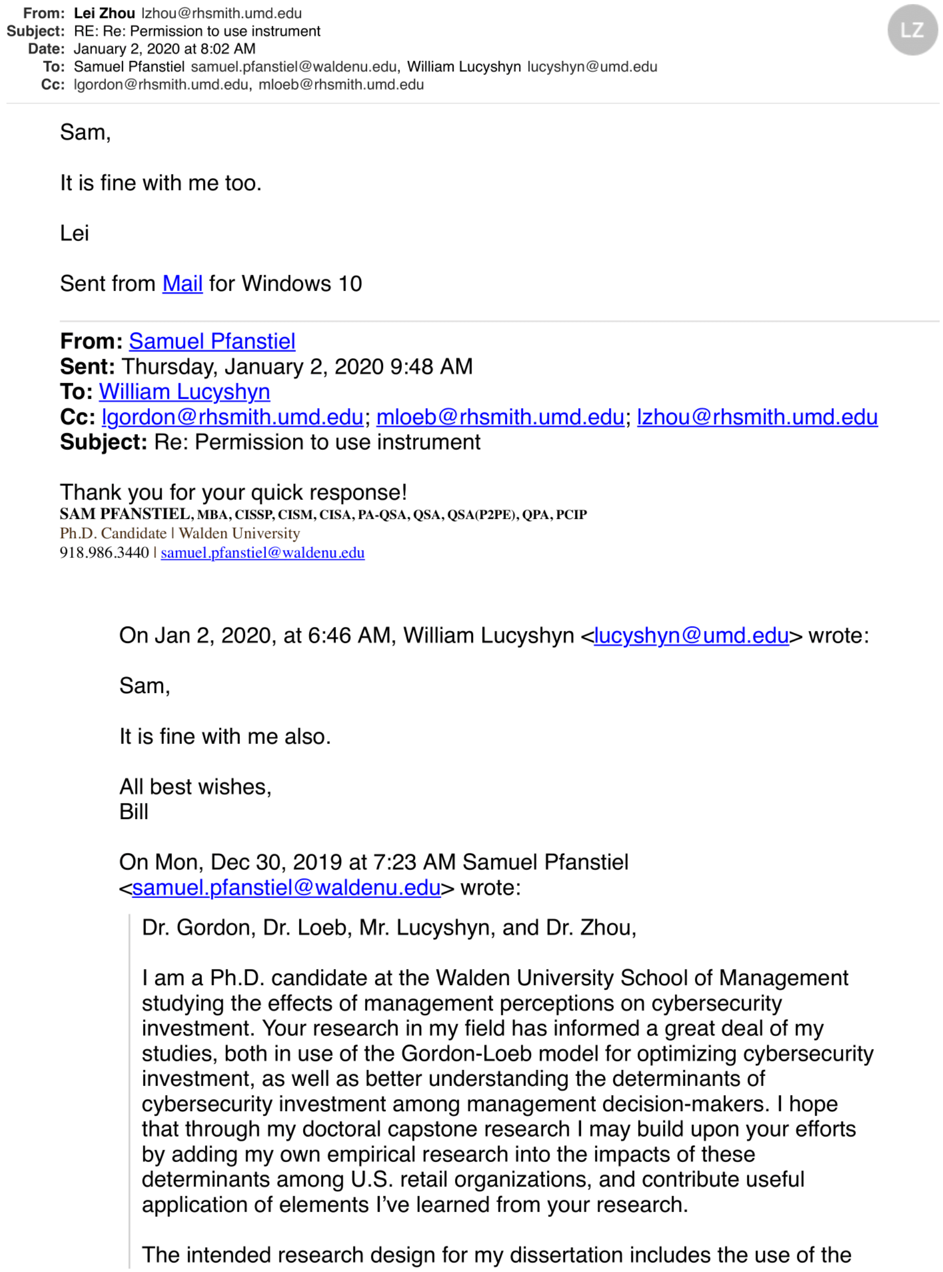
--
William Lucyshyn
Research Professor and Director of Research
Center for Public Policy and Private Enterprise
School of Public Policy
University of Maryland
301 405-8257

lucyshyn@umd.edu

www.cpppe.umd.edu

Figure C4

Approval From Lei Zhou



From: Lei Zhou lzhou@rhsmith.umd.edu
Subject: RE: Re: Permission to use instrument
Date: January 2, 2020 at 8:02 AM
To: Samuel Pfanstiel samuel.pfanstiel@waldenu.edu, William Lucyshyn lucyshyn@umd.edu
Cc: lgordon@rhsmith.umd.edu, mloeb@rhsmith.umd.edu

Sam,

It is fine with me too.

Lei

Sent from Mail for Windows 10

From: Samuel Pfanstiel
Sent: Thursday, January 2, 2020 9:48 AM
To: William Lucyshyn
Cc: lgordon@rhsmith.umd.edu; mloeb@rhsmith.umd.edu; lzhou@rhsmith.umd.edu
Subject: Re: Permission to use instrument

Thank you for your quick response!
SAM PFANSTIEL, MBA, CISSP, CISM, CISA, PA-QSA, QSA, QSA(P2PE), QPA, PCIP
Ph.D. Candidate | Walden University
918.986.3440 | samuel.pfanstiel@waldenu.edu

On Jan 2, 2020, at 6:46 AM, William Lucyshyn <lucyshyn@umd.edu> wrote:

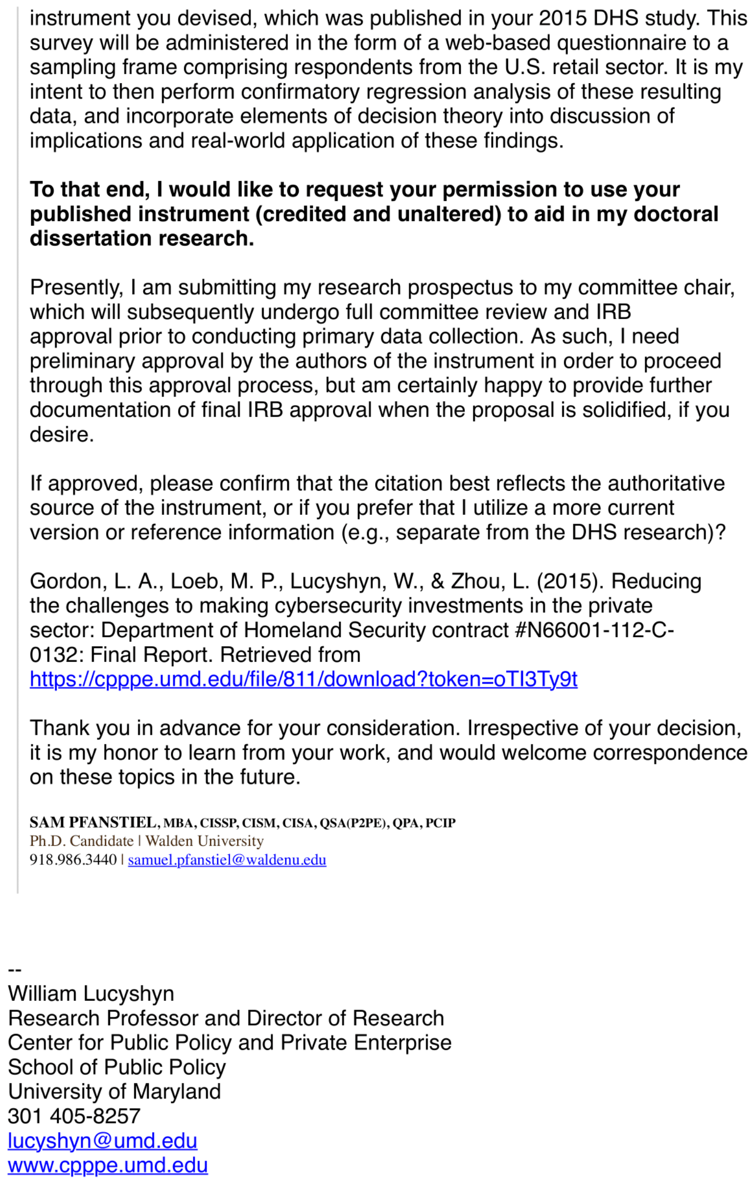
Sam,

It is fine with me also.

All best wishes,
Bill

On Mon, Dec 30, 2019 at 7:23 AM Samuel Pfanstiel
<samuel.pfanstiel@waldenu.edu> wrote:

> Dr. Gordon, Dr. Loeb, Mr. Lucyshyn, and Dr. Zhou,
>
> I am a Ph.D. candidate at the Walden University School of Management studying the effects of management perceptions on cybersecurity investment. Your research in my field has informed a great deal of my studies, both in use of the Gordon-Loeb model for optimizing cybersecurity investment, as well as better understanding the determinants of cybersecurity investment among management decision-makers. I hope that through my doctoral capstone research I may build upon your efforts by adding my own empirical research into the impacts of these determinants among U.S. retail organizations, and contribute useful application of elements I've learned from your research.
>
> The intended research design for my dissertation includes the use of the



> instrument you devised, which was published in your 2015 DHS study. This survey will be administered in the form of a web-based questionnaire to a sampling frame comprising respondents from the U.S. retail sector. It is my intent to then perform confirmatory regression analysis of these resulting data, and incorporate elements of decision theory into discussion of implications and real-world application of these findings.
>
> **To that end, I would like to request your permission to use your published instrument (credited and unaltered) to aid in my doctoral dissertation research.**
>
> Presently, I am submitting my research prospectus to my committee chair, which will subsequently undergo full committee review and IRB approval prior to conducting primary data collection. As such, I need preliminary approval by the authors of the instrument in order to proceed through this approval process, but am certainly happy to provide further documentation of final IRB approval when the proposal is solidified, if you desire.
>
> If approved, please confirm that the citation best reflects the authoritative source of the instrument, or if you prefer that I utilize a more current version or reference information (e.g., separate from the DHS research)?
>
> Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Reducing the challenges to making cybersecurity investments in the private sector: Department of Homeland Security contract #N66001-112-C-0132: Final Report. Retrieved from https://cpppe.umd.edu/file/811/download?token=oTI3Ty9t
>
> Thank you in advance for your consideration. Irrespective of your decision, it is my honor to learn from your work, and would welcome correspondence on these topics in the future.
>
> **SAM PFANSTIEL**, MBA, CISSP, CISM, CISA, QSA(P2PE), QPA, PCIP
> Ph.D. Candidate | Walden University
> 918.986.3440 | samuel.pfanstiel@waldenu.edu

--
William Lucyshyn
Research Professor and Director of Research
Center for Public Policy and Private Enterprise
School of Public Policy
University of Maryland
301 405-8257
lucyshyn@umd.edu
www.cpppe.umd.edu

Appendix D: Survey Instrument

The following instrument is entitled “Department of Homeland Security (DHS) Sponsored Survey on Cybersecurity Investments by Firms in the Private Sector,” and reproduced with permission from Gordon et al. (2015a).

A. Which of the below categories describes your organization’s principal operations (circle the correct answer/s):

Consulting
Defense
Education
Energy
Financial Services
Health Care
Information Technology
Law Enforcement
Legal
Manufacturing
Retail
Telecommunications
Transportation
Utilities
Other (please specify)

B. How many employees are in your organization (circle the correct answer)?

1-99
100-499
500-1,499
1,500-9,999
10,000-49,999
50,000 or more

C. What is your organization’s approximate gross annual revenue (circle the correct answer)?

Under $10 million
$10 million to $99 million

$100 to $1 billion
Over $1 billion

D. Which of the below titles best describes your position within your organization (circle the correct answer)?

CEO (Chief Executive Officer)
CFO (Chief Financial Officer)
CIO (Chief Information Officer)
CSO (Chief Security Officer)
Chief Privacy Officer
Security Officer
Systems Administrator
Other (please specify)

E. Approximately what portion of your firm's IT budget is devoted to cybersecurity related activities (circle the correct answer)?

1-2%	12-15%
3-5%	16-20%
6-8%	Greater than 20%
9-11%	

F. For the following set of statements, indicate your level of agreement/disagreement by circling the number provided to the right of the statement. All answers should be in the context of the organization in which you work.

	Strongly Disagree						Strongly Agree
1. Decisions regarding cybersecurity expenditures are made based on a comparison of the expected benefits resulting from defrayed costs associated with cybersecurity breaches.	1	2	3	4	5	6	7
2. Deriving the expected benefits from cybersecurity expenditures is a relatively straightforward process.	1	2	3	4	5	6	7
3. The expected benefits from cybersecurity expenditures are based largely on the expected cost avoidance/savings associated with preventing cybersecurity breaches.	1	2	3	4	5	6	7

4. The expected benefits from cybersecurity expenditures take into consideration the potential competitive advantage derived from strong cybersecurity within your organization.	1	2	3	4	5	6	7
5. The externalities (i.e., spill-over costs to other organizations that in no way affect your organization) are considered in decisions regarding cybersecurity expenditures.	1	2	3	4	5	6	7
6. My organization is actively involved in sharing information regarding our cybersecurity activities.	1	2	3	4	5	6	7
7. My organization would likely share much more information concerning our cybersecurity activities if the government could guarantee limited liability associated with any information shared.	1	2	3	4	5	6	7
8. The likelihood (or probability) that a cybersecurity breach will occur in my organization is extremely difficult to estimate.	1	2	3	4	5	6	7
9. It is a straightforward process to estimate the future dollar value of losses associated with:	Strongly Disagree						Strongly Agree
a. costs of detecting future cybersecurity breaches	1	2	3	4	5	6	7
b. costs of correcting future cybersecurity breaches	1	2	3	4	5	6	7
c. potential lost revenue due to future cybersecurity breaches	1	2	3	4	5	6	7
d. potential liability resulting from future cybersecurity breaches	1	2	3	4	5	6	7
10. My organization usually decides on major cybersecurity investments based on some form of net present value or return on investment.	1	2	3	4	5	6	7
11. The following federal government incentives would encourage my organization to spend more than is currently the case on cybersecurity activities:	1	2	3	4	5	6	7
a. Tax incentives	1	2	3	4	5	6	7
b. Cost sharing	1	2	3	4	5	6	7
c. Grants	1	2	3	4	5	6	7
d. Technical assistance	1	2	3	4	5	6	7
e. Priority government contracting	1	2	3	4	5	6	7
f. Expedited security clearance process	1	2	3	4	5	6	7
g. Public recognition	1	2	3	4	5	6	7
h. Regulation	1	2	3	4	5	6	7
i. Information Sharing	1	2	3	4	5	6	7

j. Other (Specify) _______________	1	2	3	4	5	6	7
12. Cybersecurity breaches in my organization are more often due to insider threats or carelessness than external threats.	1	2	3	4	5	6	7
13. A critical determinant of the actual expenditures on cybersecurity activities in my organization is whether or not a major cybersecurity breach has recently occurred in my firm.	1	2	3	4	5	6	7
14. A critical determinant of the actual expenditures on cybersecurity activities in my organization is whether or not a high visibility cybersecurity breach recently occurred in other firms.	1	2	3	4	5	6	7
15. The 2011 SEC Disclosure Guidance on Cybersecurity Risks and Cyber Incidents has increased my organization's focus on cybersecurity related activities.	1	2	3	4	5	6	7
16. Cybersecurity is an important component of my organization's approach to the internal controls of financial reporting systems.	1	2	3	4	5	6	7
17. In determining the risk associated with cybersecurity breaches, my organization considers the expected value of the loss.	1	2	3	4	5	6	7
18. In determining the risk associated with cybersecurity breaches, my organization considers the largest potential loss.	1	2	3	4	5	6	7
19. My organization has insurance that covers, at least in part, the costs associated with cybersecurity breaches.	1	2	3	4	5	6	7

Other comments (attach additional sheets if required):