2023

Perceptions and Knowledge of Information Security Policy Compliance in Organizational Personnel

Jesus M. Mosqueda
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Jesus Mosqueda

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. Brandon Simmons, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Inez Black, Committee Member, Doctor of Business Administration Faculty

Dr. Jodine Burchell, University Reviewer, Doctor of Business Administration Faculty

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

Walden University
2023

Abstract

Perceptions and Knowledge of Information Security Policy Compliance in Organizational Personnel

by

Jesus Mosqueda

BASc, Capella University, 2015

MS, Capella University, 2018

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2023

Abstract

All internet connected organizations are becoming increasingly vulnerable to cyberattacks due to information security policy noncompliance of personnel. The problem is important to information technology (IT) firms, organizations with IT integration, and any consumer who has shared personal information online, because noncompliance is the single greatest threat to cybersecurity, which leads to expensive breaches that put private information in danger. Grounded in the protection motivation theory, the purpose of this quantitative study was to use multiple regression analysis to examine the relationship between perceived importance, organizational compliance, management involvement, seeking guidance, and rate of cybersecurity attack. The research question for this study was focused on the relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence. Data was collected from the United Kingdom's 2021 Cyber Security Breaches Survey. Multiple linear regression analysis yielded that the four independent variables were not predictive of instances of cybersecurity breach or attack. The implications for positive social change include the potential to actively promote and publicly address cybersecurity as personal privacy increasing becomes a matter of public safety. One key recommendation is for IT leaders to pursue methodologically rigorous and uniform operationalization throughout IT research and practice, including the pursuit of replicable data of detailed resolution. The results of this study may potentially be used to reduce the risks for cybersecurity breaches, which ultimately contributes to social change by furthering the right of privacy and the protection of personal information.

Perceptions and Knowledge of Information Security Policy Compliance in Organizational Personnel

by

Jesus Mosqueda

BASc, Capella University, 2015

MS, Capella University, 2018

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

March 2023

Dedication

To my loving wife and my three beautiful daughters. You all are why I do everything that I do. You all are why I keep going. You all are what I look forward to every day.

Acknowledgements

Thank you to Dr. Simmons, who's kept in close touch with me up to this time. I had some confusion about the whole process at first, but you set me straight every time. You've always been very encouraging and supportive of the goals I've set. I couldn't have gone this far without your guidance.

Thank you to Dr. Klein for your very clear and insightful comments. I'm grateful for your extremely quick response times, which were always far beyond my expectations.

Thank you to Dr. Black for adapting so quickly to the needs of this project. I'm grateful for the speed at which you have responded.

Thank you to Dr. Griffith and Dr. Burchell for so faithfully reviewing my manuscripts.

Thank you to Jenny Martel Houck for your help with the form and style of the manuscript.

Last but not least, a big thanks to my loving family who have always supported me through the good times and the bad.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Historical Background

As organizations continue to integrate technology throughout their internal and external processes, their vulnerability to focused cyberattacks have likewise increased. Information security (IS) measures are unavoidable within modern organizations because, considering the advent of Industry 4.0, information technology (IT) implementations have become ubiquitous within the current economy's increasingly digitalized nature (Cram et al., 2019). The security of increasingly vulnerable IT and cyberspace implementations have become a critical organizational concern as novel cybersecurity threats continue to emerge even among unaddressed extant risks (Aceto et al., 2019; Choi et al., 2018). The nature of these threats, however, are neither obvious nor self-evident.

Cybersecurity threats are not only technological in nature. The global and highly publicized WannaCry ransomware event has revealed the necessity of solidifying the IS behaviors of organizational personnel, also called organizational insiders, as the highly successful cyberattack was possible largely due to personnel not complying to organizational information security policies (Daud et al., 2018) and lacking proper cyber hygiene practices (Baldin, 2019). The actions of insiders, particularly that of untrained non-IT employees and leadership, can pose a constant danger to organizational cybersecurity. This danger is termed insider threat (Angraini et al., 2019; Branker et al., 2016; Choi et al., 2018). The primary relevance of insider threat is that organizational cybersecurity does not only hinge upon technical solutions but human-centered policies.

Organizations typically attempt to mitigate insider threat through the implementation of information security policies (ISP), documents that delineate organization-wide procedures, best practices, guidelines, and requirements that all organizational personnel are mandated to follow (Angraini et al., 2019). Information security policy compliance (ISPC) refers to whether organizational personnel, be they IT or non-IT employees, adhere to their organization's ISP (Angraini et al., 2019). Cyber hygiene refers to a diverse set of actions that promote cyber resilience and cybersecurity within an organization (Vishwanath et al., 2020). Together, the concepts of insider threat, ISP, ISPC, and cyber hygiene can be used to characterize the degree to which insiders can pose a threat to the cybersecurity of their organizations.

Organizational/Industrial Context

This study involved conducting a secondary data analysis on the quantitative data that was part of the 2021 Cyber Security Breaches Survey (CSBS), a data collection effort administered annually by the United Kingdom's Department for Digital, Culture, Media and Sport (DCMS; Ipsos MORI, 2021a; 2021b; 2021c). Since 2016, the DCMS has contracted Ipsos MORI, a third-party market research firm, to conduct an annual randomly sampled survey of private businesses and charities of various sizes. Sole proprietorships and business sectors without industry-wide IT implementations (e.g., fishing) were excluded (Ipsos MORI, 2021a; 2021b; 2021c). The context of the data, then, encompasses private organizations with current and next-generation IT implementations. This study is applicable to those companies with IT integration and particularly those moving toward Industry 4.0, which refers to the integration of

technology within all or most aspects of organizations, from the minute operational details to large-scale strategic decision-making (Bhaharin et al., 2019). As the business landscape shifts its paradigm toward Industry 4.0, the implementation of IT has only grown, which has greatly expanded the need to contextualize the organizational landscape in the internal and external domains (Bhaharin et al., 2019). As technology become even more ubiquitous, organizations must adapt to the resultant cybersecurity implications.

Information security standards are established at the level of national ordinance. In the United States, the National Institute of Standards and Technology (NIST) standardizes the internal organization-level frameworks of cybersecurity. The NIST's standards also serve as a prototype for cybersecurity governance in other nations. The NIST (2011; 2018) established a three-tiered cybersecurity risk management framework (RMF) for businesses, structured as a pyramid with the first tier on the top and third at the bottom: (a) the organization, (b) mission/business processes, and (c) information technology systems—in increasing levels of granularity of detail in management response. The organization is the first tier of cybersecurity risk management and establishes the top-level context for all risk management efforts initiated throughout the organization, including governance, risk executive, risk management strategy, and investment strategy (NIST, 2011). The organization directly influences all decisions at the other two tiers, by dictating how its business processes are structured and how its technical, operational, and management resources will be deployed in its IT systems. The second tier involves cybersecurity risk management activities that directly pertain to

strategic decision-making, goal alignment, business processes, and performance measurement. This includes risk-aware goals and policies, enterprise architecture, and IS architecture. The third tier involves the ground-level IT/IS risk management perspective, including the accounting of information systems, resource allocation, and IS management (NIST, 2011). In total, the NIST RMF outlines how information security risk management is conceptualized at the organizational level.

Standard cybersecurity risk frameworks reveal the primary cybersecurity issues that organizations must address. According NIST's (2011; 2018) RMF, organizations manage cybersecurity risk according to information that runs along various key risk management concepts—among which three are trustworthiness, risk tolerance, and organizational culture—which they use to make decisions throughout its tiers. The various dimensions of quantitative data collected in the 2021 CSBS (Ipsos MORI, 2021a; 2021b; 2021c) are highly significant to the organizational context according to these concepts. Survey data regarding the prevalence of cybersecurity breaches (Ipsos MORI, 2021c), for example, directly relate to both trustworthiness and risk tolerance, as breaches mostly involve the theft or corruption of client-privileged information. Data regarding the severity of the breaches can be used to enrich decisions that pertain to trustworthiness and risk tolerance, particularly regarding budgeting. Likewise, CSBS data on cybersecurity training, information sources, and ISPs directly pertain to decisions on organizational culture.

Frameworks contextualizing cybersecurity factors external to the organization have tended to be fragmented and lacking in cohesion as they are not standardized by an

agency like the NIST. Kuerbis and Badiei (2017) stated that a cohesive account of the institutional cybersecurity landscape should address both governance structures (such as the markets, governance hierarchies, and networks) and cybersecurity activities (such as information sharing, disclosure, standardization, and risk management). In accounting for these factors, the researchers characterized the industry-wide context across two fundamental categories that temporally characterize actions surrounding cybersecurity incidents and breaches: (a) ex ante, or before-the-fact, cases which focus upon the prevention of cybersecurity breaches and (b) ex post, or after-the-fact, market offerings designed for responding to breaches. This distinction provides a clear perspective of the cybersecurity landscape, clarifies the role of governing structures and hierarchies according to stages of cybersecurity incidents, and contextualizes the analysis of transaction and resource costs (Kuerbis & Badiei, 2017). Current efforts in developing and evaluating holistic ISPC frameworks largely only account for limited, personnel-level ex ante cybersecurity activities, not fully accounting for the greater cybersecurity landscape (Koohang et al., 2021; Moody et al., 2018). Any emphasis on this weakness in ISPC research and market offerings must, however, be tempered by the fact that the field is relatively new and highly emergent in nature.

As understanding of the cybersecurity landscape increases, it is possible to better contextualize the emerging issue of insider threat. Kuerbis and Badiei's (2017) study helps contextualize insider threat as an ex ante issue. The researchers found that ex ante offerings by governing hierarchies or organizations to address cybersecurity were struggling due to a lack of market demand (Kuerbis & Badiei, 2017). Despite the fact that

that ISPs, ISPC, and cyber hygiene have been found to be critical ex ante efforts to reduce the prevalence and severity of security breaches (Addae et al., 2019; Alzahrani et al., 2018; Angraini et al., 2019), this finding helps explicate the overall lack of initiative in developing organizational processes and cultures that promote internal cybersecurity efforts (Daud et al., 2018). In contrast, Kuerbis and Badiei found that cybersecurity products regarding post-cyberattack mitigation were far more developed with regards to offerings and governing hierarchies (Kuerbis & Badiei, 2017). This finding may explicate any significant results regarding the breach severity data within the 2021 CSBS (Ipsos MORI, 2021c). As such, this study contributes valuable information to the body of cybersecurity research on ex ante cases.

Insider threat is beginning to be acknowledged as a critical concern in research and practice. Due to the ongoing Industry 4.0 paradigm shift, information security has increasingly become a paramount issue in both the internal organization and the external industry contexts (Bhaharin et al., 2019). With the advent of the COVID-19 pandemic, 40% of organizations have accelerated the digitization of their operations and 39% have begun transitioning toward full-time remote workers, which necessitate cybersecurity measures due to increased risk of cybersecurity breaches (PricewaterhouseCoopers, 2021). As such, consumer trust has become inextricably linked to the information security capabilities of the organizations in question, hence both the organization- and industry-level trend toward increase security (Kuerbis & Badiei, 2017; PricewaterhouseCoopers, 2021; NIST, 2018). At the same time, the risk landscape continues to evolve as novel threats continually emerge (Caratas et al., 2019). In

summary, improved information security has become increasingly necessary at all levels of organizational function that involves information technology.

Problem Statement

Employee noncompliance toward information security policies is the greatest threat to companies that implement information technology in their operations, as it greatly increases vulnerability to cyberattack (Angraini et al., 2019; Nord et al., 2020). The global average cost of cybersecurity breach rose from $3.86 million in 2020 to $4.24 million in 2021, with the average US and UK breach costing $9.05 million and $4.67 million, respectively (Ponemon Institute, 2021). The general business problem is that noncompliance and cyber hygiene harms profitability across industries with IT implementations through increased vulnerability, leading to cybersecurity breaches. The specific business problem is that some organizational leaders do not know the relationship between the perceived importance of cybersecurity, senior management involvement, information security policy compliance (ISPC), knowledge of cyber hygiene, and number of cyberattack incidents.

Purpose Statement

The purpose of this quantitative correlational study was to investigate the relationship between ISPC factors, cyber hygiene factors, and organizational vulnerability to cyberattack. The independent variables were: (a) perceived importance of cybersecurity, (b) senior management involvement, (c) use of organizational ISPC, and (d) seeking of information or guidance on cybersecurity. The dependent variable was instance of cybersecurity breach or attack. The targeted population consists of top-level

IT leadership in United Kingdom businesses that use IT implementations in daily operations. The implication for social change originates in the potential to increase the cybersecurity of organizations. Increased organizational cybersecurity ultimately aids in protecting the confidential personnel and client information stored in IT systems, which can be vulnerable in any networked or online interaction, such as ubiquitous monetary transactions (Cain et al., 2018). As such, increased cybersecurity ultimately promotes positive social change by protecting the human right to privacy, particularly as networked and online transactions become increasingly commonplace.

Target Audience

The two groups of stakeholders targeted in this study correspond to relevant agents in NIST's (2011; 2018) cybersecurity RMF, as well as Kuerbis and Badiei's (2017) cybersecurity industry framework. The first group of key stakeholders that may benefit from this study are any leadership, management, or IT personnel within an organization involved in any of the three tiers of the cybersecurity RMF (NIST, 2011; 2018). At the organizational and business process levels, organizational leaders and managers make strategic and process-oriented decisions that guide the organization and its activities. Leadership and management may use this study's results to create new organizational goals and processes more aligned to greater cybersecurity. The results may give IT professionals a better idea of the types of cybersecurity training and education that would be most effective in mitigating insider threat.

The second group of key stakeholders that may benefit from this study are any organizations and scholars that are involved in provision, research, and/or development

of ex ante cybersecurity products, governance, networking, resources, or services (Kuerbis & Badiei, 2017). The stakeholders might be anyone within or without an organization that is hired to preempt cybersecurity incidents before they occur, to prevent breaches, or to establish processes for mitigating their effects. This may include cybersecurity service providers, IT consultancies, IT-related agencies, governing bodies, internal IT personnel, and organizational leadership. This study is targeted, by nature, more toward audiences interested in cybersecurity prevention because ISPs, ISPC, and cyber hygiene are measures that are implemented as preventative and mitigatory types of risk management (Nord et al., 2019). Partially due to the rigorous nature of the 2021 CSBS dataset, the results provide insight that might be used to increase demand in ex ante cybersecurity efforts. The results also provide insights that may help governing bodies develop more effective ex ante networks and governance structures.

Research Question

What is the relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence?

Hypotheses

Null hypothesis (H_0): There is no statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence.

Alternative hypothesis (H_1): There is a statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence.

Significance of the Study

Top management commitment and structured security processes such as ISPs are critical in increasing the cybersecurity within organizations (Daud et al., 2018). Increased cybersecurity can positively impact businesses by minimizing potential financial and data loss from security breaches (Daud et al., 2018). The importance of leadership involvement in increasing organizational cybersecurity is paramount (Pullin, 2018). Yet most investigations involved organizational personnel rather than leaders (Angraini et al., 2019; Cram et al., 2019). Organizational leaders are considered key decision-makers in both first- and second-tier cybersecurity risk management efforts (NIST, 2011; 2018) and play a major role in ISPC throughout the organizations they manage (Caratas et al., 2019; Daud et al., 2018; Hu et al., 2012; Pullin, 2018). This study is an attempt to help address this gap in research, such that scholars and professionals may have access to more information regarding how leaders' perspectives of ISPC and cyber hygiene affect cyberattack vulnerability. Organizational leaders may be able to take advantage of these insights to augment their actions, involvement, decisions, and goal setting to more effectively address emerging cybersecurity threats. If they possess more accurate management-level information, improved leadership efforts may result in greater security and the prevention of capital loss associated with security breaches.

Regarding the implications of this study for positive social change, cybersecurity vulnerability does not only affect organizations, but any human being that is involved in any online or networked transaction or that stores private information within any online or networked system. Insider threat—caused by employees who do not comply to information security policies due to ignorance, lack of cybersecurity knowledge, or lack of cyber hygiene—has been repeatedly found to be the most significant threat to organizational security (Daud et al., 2018). Security vulnerabilities put sensitive data at risk for security breaches, such as confidential personal information of stakeholders such as clients, customers, or anyone who interacts with IT-connected organization using their private data (Such et al., 2019). As a result, this study contributes to the protection and security of private information. By adding to ISPC, cyber hygiene, and organizational cybersecurity research, this study contributes to positive social change by increasing the potential of organizations to protect the right of privacy to any people that engage in networked or online activities.

Theoretical Framework

This study's theoretical framework is protection motivation theory (PMT). PMT was proposed by Rogers in 1975 to explicate behaviors that are protective to the agent of action according to internal and environmental conditions. According to PMT, individuals have the tendency to act protectively in response to threats or fear appeals in both emotional and rational ways (Herath & Rao, 2009). Coping with threats or fear appeals occur via two distinct processes: (a) threat appraisal and (b) coping appraisal (Herath & Rao, 2009). Threat appraisal involves an individual's subjective assessment

regarding the severity and probability of the threat, as well as how vulnerable the individual is to the threat (Rajab & Eydgahi, 2019). Coping appraisal involves an individual's assessment regarding the capacity to adapt to the threat, as well as self-assessments regarding the individual's competence, response ability, and self-efficacy in the process of coping with the threat (Rajab & Eydgahi, 2019). When these two factors are taken together, PMT can be used as a framework to describe the primary and secondary processes by which organizational leaders understand and mediate ISPC, cyber hygiene, and cybersecurity vulnerability.

As this study is predicated on the identification of individual and institutional factors that can determine the cybersecurity vulnerability of an organization, the theoretical framework on which it is constructed must be validated for these variables. There is a great deal of precedent for using PMT for this type of inquiry, largely because the theory integrates both internal cognitive-emotive factors—such as individual beliefs, knowledge, and assessments—and external institutional factors—such as consequences and probability of harm (Rajab & Eydgahi, 2019). Choi et al. (2018) discovered a qualitative link between the insider beliefs and organizational cybersecurity using PMT, thereby confirming the framework's utility in investigating individual factors of compliance. Hina et al. (2019) verified qualitative links between institutional governance and ISPC, thereby confirming the framework's utility in investigating external factors of compliance. In summary, cybersecurity and ISPC research using PMT supports the tenability of the study's alternative hypothesis.

Review of the Professional and Academic Literature

The strategy for searching the literature revolved around focused Boolean keyword research strictly for peer-reviewed scholarly journal articles. The two most consistently used keywords were “information technology” and “cybersecurity”; I always used one of these two keywords in the “Subject” element of the database search function. Using one of these two keywords as a foundational boundary to limit studies to the most relevant, I placed topical keywords in the second and/or third rows following the “AND” Boolean function in the “Abstract” element of the database search function. These secondary keywords included “information security policy”, “information security policy compliance”, “insider threat”, “protection motivation theory”, “cyber hygiene”, and “Industry 4.0”. These topical keywords were first input two at a time, for a total of three rows of Boolean inputs connected by the “AND” function, to make sure that the first set of studies had a high level of specificity to the topic. I input these topical keywords manually, noting each the various possible combinations of keywords that were attempted, to ensure that studies were not missed.

The strategy for choosing articles was also systematic in nature. I reviewed the search results according to a planned method of detecting relevance to this study, first according to the title. If the title was relevant to the topic of this study during the initial review of the search results, I opened a tab to the respective study. The abstracts of the studies for each open tab were subsequently reviewed to determine relevance. If the contents of the abstract had relevance to this study, the respective journal article was downloaded and the citation was saved in a reference document to organize references by

topic, to identify any duplicate articles, and in case the article would be cited in this study.

The sources cited in this study were not limited purely to scholarly articles from current peer-reviewed journals, but also included publications, professional and government reports, seminal works, older scholarly articles, and references books. While reviewing the peer-reviewed articles yielded from the Boolean searches, I found it necessary to review sources that were cited in the current scholarly articles I had found during my initial search of the literature. Of the 85 total sources cited in this study, 74 (87.1%) were published in the last five years and 74 (87.2%) were peer-reviewed. Of the 74 sources published in the last five years, a total of 51 sources (71.8%) were peer-reviewed scholarly journal articles, six sources (8.1%) were reference publications related to research methodology and design, four sources (5.4%) were from government reports, and three sources (4.1%) were from private-sector auditing reports commonly cited in scholarly literature. Four sources were peer-reviewed articles published in 2016 or earlier, which I included because they featured research designs and results not found in other more current articles. Another three sources were also articles published in 2016 or earlier, which I included because they contained literature reviews that provided significant insight into the topic. Finally, two older sources were seminal works related to the theoretical framework.

This section contains a review of the literature critical in understanding the issues inherent in addressing the problems and research questions of the present study. It begins with a review of protection motivation theory, the foundational theoretical framework

structuring this study, along with why it was chosen, how it has been used in research, and how it fits into the context of ISPC research. Then follows a discussion of the consequences of Industry 4.0 on cybersecurity, in which the increased relevance of ISPC in organizational and business research and practice is fully explained. Next are reviews of insider threat and cyber hygiene, to further contextualize and demonstrate the critical roles organizational personnel play in cybersecurity. Finally, the section closes with an in-depth review of the many factors that mediate ISPC and a discussion of ISPC models and frameworks.

Protection Motivation Theory

Rationale

As PMT is one of many theories that are regularly used in ISPC research, the rationale for choosing this framework must be discussed. According to Cram et al.'s (2019) meta-analysis, ISPC research is characterized by as many as 17 distinct theoretical frameworks. Some, such as Moody et al. (2018) and Koohang et al. (2021), have begun to develop, validate, and revise a unified theory specifically for the context of organizational information security policy compliance. Among the many potential theoretical frameworks, I chose PMT as this study's primary theoretical framework for two fundamental reasons.

First, PMT is a highly prominent theory in ISPC research that directly pertains to this study's topic. The theory has had its validity and appropriateness confirmed by multiple peer-reviewed research articles (Cram et al., 2019; Koohang et al., 2021; Moody et al., 2018). The prominence of PMT is in a large part due to the granularity of analysis

possible in the subfactors associated with threat appraisal and coping appraisal, which allows for detailed analyses of the affective and cognitive antecedents of risk management behaviors (Choi et al., 2018; Herath & Rao, 2009; Rajab & Eydgahi, 2019). PMT has been tested extensively for predictive power (Moody et al., 2018) and its two constructs, threat appraisal and coping appraisal, accommodate the present study's variables. PMT is also ideal in addressing this study's research question and alternative hypotheses because it is predicated on an inherent relationship existing between cybersecurity beliefs, organizational constraints, and actual cybersecurity behavior (Herath & Rao, 2009). PMT, then, is used by researchers when it is necessary to investigate how an organization's current cybersecurity is influenced by insiders, organizational governance, or a combination of the two (Choi et al., 2018; Hina et al., 2019). As such, PMT was highly appropriate for this study because it involved inquiring about the effects of insider cognitions, knowledge, and actions on organizational cybersecurity.

Second, a comparison of the four most prominent ISPC theoretical frameworks indicated that PMT had the most predictive power to determine compliance outcomes (Rajab & Eydgahi, 2019). Rajab and Eydgahi tested and compared the efficacy of four different theoretical frameworks in determining employee intent to comply to organizational information security policies: (a) the theory of planned behavior (TPB), (b) general deterrence theory (GDT), (c) organizational theory (OT), and (d) protection motivation theory (PMT). The researchers constructed a detailed quantitative survey instrument that included all four models, surveyed higher education staff and faculty, and

tested for the predictive power of each with reference to participants' intent to comply. Results indicated that three factors—perceived threat vulnerability, efficacy of threat response, and cost of response—were the most predictive of intent to comply to security policy, each of which were PMT variables (Rajab & Eydgahi, 2019). The findings are quite significant, as they contradict the many researchers who utilized TPB, GDT, and OT as the primary theoretical constructs to investigate intent to comply (Moody et al., 2018). However, even as Moody et al. and Koohang et al. (2021) demonstrated, this is not to say that the other three theories are inapplicable to the investigation of ISPC. Yet Rajab and Eydgahi's findings support the use of PMT in measure intent to comply. In contrast, the other three theories may be predictive of other ISPC effects, such as compliance behavior, attitudes, or beliefs (Rajab & Eydgahi, 2019).

This is not to state, however, that PMT is the single most applicable theory in ISPC research. Some researchers, such as Moody et al. (2018) and Cram (2019), view PMT as just another theory among a framework of theories that can be better used to characterize how ISPC manifests within the organizational context. Regardless of the push toward more comprehensive frameworks, PMT remains a validated theory in ISPC research.

Use of PMT in ISPC Research

These justifications for choosing the theoretical framework are not to say that research using PMT does not have its share of potential shortcomings. There exist cases in which data gathered using PMT constructs yielded conflicting quantitative results. Pahnila et al. (2007), one of the first groups of researchers to empirically validate PMT in

the ISPC context, investigated the role of threat appraisal and coping in employee attitudes toward ISPC. The researchers measured the relationship between threat appraisal and attitude toward ISPC, as well as between coping appraisal and attitude (Pahnila et al., 2007). Threat appraisal was found to have a significant effect on ISPC attitudes, which implied that there is value in having employees be highly aware of the severity of potential cybersecurity threats (Pahnila et al., 2007). Coping appraisal, however, did not have such a significant effect, implying that employee beliefs that they could adequately respond to cybersecurity threats had little to no bearing on their attitudes to comply (Pahnila et al., 2007). Yet the researchers did not fully investigate the role of coping on compliance, but only intent to comply. In contrast to Pahnila et al.'s findings, Rajab and Eydgahi's (2019) study confirmed that coping appraisal did have a statistically significant relationship to compliance, thereby providing conflicting evidence. Such contradictions in results need not invalidate PMT itself but may be a result of any number of factors, such as non-rigorous research methodologies, inconsistent operationalization of key concepts, or differences in research conditions.

Other inconsistencies have been evident in quantitative research results. Herath and Rao's (2009) early ISPC research into PMT indicated that not all of the constructs that comprise the theory may be predictive. The researchers investigated the predictiveness of PMT constructs in terms of whether the premises of the theory can mediate two major ISPC factors, including participant concern of security risk and attitudes toward ISPs. They found that just two PMT constructs, efficacy of response and self-efficacy, were significant mediators of intent to comply with ISPs while two other

PMT constructs, cost of response and concern regarding security, were not (Herath & Rao, 2009). Yet Rajab and Eydgahi (2019) reported conflicting results, finding that response cost and perceived vulnerability were two of the three strongest predictors of intent to comply with ISPs. Again, these conflicting findings may indicate a lack of consistency in research, a lack of methodological rigor, or a lack of overarching context into which such discrepancies can be understood.

This is not to demonstrate that PMT cannot be predictive across all of its constructs. Consider Addae et al.'s (2019) application of PMT into the Ghanaian banking sector, which mostly confirmed the statistical viability of the theory to predict for compliance. The researchers used both primary PMT constructs, threat appraisal and coping appraisal, as well as compliance intention to create a quantitative instrument. Participants were mid- to high-level information technology (IT) managers in five Ghanaian banks. Significant predictors included perceived threat severity, perceived vulnerability, response efficacy, and compliance intention. Self-efficacy did not have a significant relationship with compliance. Response cost had a negative relationship with compliance (Addae et al., 2019). Compared to either Herath and Rao (2009) or Rajab and Eydgahi's (2019) findings, Addae et al.'s results were more consistent. Yet it must be noted that researchers have not yet performed systematic reviews or meta-analyses that aim at explicating the reasons for these differences in results.

PMT has not been limited to quantitative inquiries but has also been used to frame qualitative investigations. Posey et al. (2014), for example, used the theory to create a qualitative comparative research design, in which the differences in the thinking of

various participants, particularly between IS personnel and non-IS insiders, were compared to one another. Open-ended interview questions were created using PMT according to three constructs (i.e., vulnerability to threat, severity of threat, and result of maladaptive behavior) that comprise threat appraisal and three constructs (i.e., efficacy to respond to threat, self-efficacy, and cost of response) that comprise coping appraisal (Posey et al., 2014). Note that the rigid characterization of the theory was just as systematic as the quantitative inquiries of Herath and Rao (2009) and Addae et al. (2019), though data collected in qualitative study is inherently not numerically measurable. Through analysis of interview data, the researchers found notable discrepancies between the two participant groups, including the propensity of insiders to identify external threats rather than internal and the propensity of IS professionals to cite lack of education as the most serious vulnerability (Posey et al., 2014). The many consistencies and inconsistencies between the beliefs in the two groups revealed that ISPC is not just a technical concern to be addressed only through quantitative inquiry (i.e., Addae et al., 2019), but can also be addressed through more qualitative means such as organizational culture (Posey et al., 2014). Indeed, whereas Herath and Rao quantified the statistical predictiveness of PMT constructs and ISPC, Posey et al. confirmed the exploratory and explanatory viability of PMT in explicating ISPC cognitions, beliefs, and intent, namely the human-focused internal factors that mediate compliance. PMT's qualitative utility extends further.

PMT has been used to gain qualitative insight into external, organizational factors that mediate ISPC. Hina et al. (2019) used PMT as its predominant theoretical framework

due to the theory's effectiveness in predicting for protective behavior in many domains. Instead of using PMT to investigate ISPC phenomena, the researchers departed from the norm by investigating how institutional governance can affect PMT factors that, in turn, mediate ISPC outcomes. The researchers used the model to conduct interviews for the purpose of creating a questionnaire that would measure this relationship, though the subsequent steps were quantitative due to the need to validate the questionnaire. Note that qualitative studies are often used to build a foundation upon which quantitative instruments can be created (Creswell & Creswell, 2018). Though limited in scope, Hina et al. found that institutional governance can positively affect PMT factors in educators, which can lead to positive ISPC outcomes. Though not as statistically significant as Addae et al.'s (2019) findings, Hina et al.'s results provided insight into individual elements that may mediate the human response to governance. Through this qualitative inquiry, it is possible to confirm how organizational governance can mediate threat appraisal and coping appraisal which together mediate overall ISPC. This insight, in turn, can be used to propel further qualitative or quantitative investigations.

Contextualizing PMT and Addressing the Trend toward a Unified Theory of ISPC

The use of PMT in IS research, as well as the examination of its weaknesses as an ISPC framework, represents a major paradigm shift in research in which scholars have begun integrating the study of human behavior in cybersecurity. As Choi et al. (2018) stated, IS research has largely been lacking in the development of theories that directly pertain to cybersecurity, ISPs, cyber hygiene, and ISPC, instead relying upon existing constructs in fields such as psychology, criminology, and economics. The adoption of

interdisciplinary constructs was rooted in the lack of study into the human antecedents of security breaches, which finally changed due to highly public incidents like the Target and Home Depot security breaches (Such et al., 2019). This trend has largely been positive because it demonstrates that scholars and practitioners have acknowledged the critical importance of insider cognitions and behaviors on organizational cybersecurity, which lead to the study of insider threat, ISPC, and cyber hygiene (Choi et al., 2018). The central role of the insider in IS has been fully validated across the many behavioral science theories, such as the 17 identified by Cram et al., (2019) and the 11 specified by Moody et al. (2018), leading to a multitude of empirically confirmed cognitive and behavioral antecedents to organizational IS breaches. This validation has allowed for a maturing of ISPC research toward more holistic directions.

Despite their yet widespread use in IS research and my decision to use one as the primary theoretical framework, researchers have begun to move away from theories such as PMT in preference of frameworks that consolidate multiple theories relevant to ISPC (Choi et al., 2018; Cram et al., 2019; Koohang et al., 2021; Moody et al., 2018). This shift toward a consolidated theory, however, has not gained substantial momentum and represents an overall minority of ISPC research. The shift has been motivated by concerns that the large number of interdisciplinary frameworks being used in ISPC research has led to conflicting theoretical approaches and inconsistent findings, leading to difficulties in gaining clear and cohesive insights into the true cognitive and behavioral antecedents to cybersecurity breaches (Cram et al., 2019). The use of so many disparate theories has also contributed to the general lack of standard operationalizations of terms,

constructs, and instruments (Moody et al., 2018). Regardless of the abundance of information security research, this lack of operationalization has made conflicting findings difficult, if not impossible to resolve (Cram et al., 2019; Moody et al., 2018). Yet this same, albeit disparate, proliferation of research has allowed systematic researchers to begin to examine higher-order patterns above that of currently accepted theories.

The validation of so many existing theories and constructs in IS research has made it possible to begin consolidating and constructing unified theoretical frameworks that more directly pertain to ISPC as a whole and more accurately contextualize how cybersecurity functions in organizations (Cram et al., 2019; Moody et al., 2018). Moody et al. (2018) made the ambitious attempt to consolidate the relevant theoretical frameworks and constructs into a unified model of information security policy compliance (UMISPC). The researchers empirically refined the many validated antecedents to ISPC, then operationalized them into a single theory, the UMISPC, comprised of eight constructs: response efficacy, threat, habit, role values, fear, intention, neutralization, and reactance (Moody et al., 2018). Koohang et al., (2021) confirmed the reliability and validity of the UMISPC, though the researchers found that habit and fear were not significantly related to intent to comply. But Koohang et al. did not recommend that scholars and practitioners redact the two constructs, because the UMISPC is still a new construct and prior studies suggest that further testing be performed to confirm these findings. Although the UMISPC does not directly pertain to the focused nature of this

study, understanding the gradual paradigm shift in IS research informs where PMT lies in the field.

Though more holistic and unified frameworks of ISPC are emerging, they are not yet ready for use in a nonexploratory setting. Because of the inherent complexity of the UMISPC, it is largely only appropriate for in-depth, highly detailed, and multi-factor analyses of ISPC. The need for further validation in more rigorous settings (Koohang et al., 2021; Moody et al., 2018) also precluded using this framework for this study. Like the current trend toward cybersecurity integrations throughout all aspects of organizations beyond that of organizational governance (Choi et al., 2018), the UMISPC marks a trend toward a more integrated, comprehensive, and sophisticated approach to ISPC theory which is characteristic of the Industry 4.0 paradigm shift. As Industry 4.0 has not yet reached its apex, so the holistic and consolidated ISPC frameworks have yet to reach maturity.

Industry 4.0 and the Consequences of Increased ICT Integration

As this study's problem is predicated upon the increased implementation of technology, it will be important to review the basis for this shift. Industry 4.0 refers to the overarching paradigm shift toward the integration of information and communication technologies (ICTs) throughout all industrial processes in which such implementations are possible (Aceto et al., 2019; Núñez-Merino et al., 2020). Such integration necessarily involves the integration of collaborative information networks throughout an organization which allows for information gathering and exchange throughout all connected components of an organization (Mon & Giorgio, 2021). The Industry 4.0 movement is

characterized by the increasing adoption of many lesser technological paradigm shifts, including but not limited to cyber physical systems, blockchain, automation, additive manufacturing, the internet-of-things (IoT), artificial intelligence (AI), machine learning, cloud computing, virtual environments, augmented reality, and big data analytics (Aceto et al., 2019; Kiss et al., 2019; Mon & Giorgio, 2021; Núñez-Merino et al., 2020; Zhang et al., 2019). Apart from these revolutionary technological integrations, a key defining factor of Industry 4.0 is the inextricable integration of physical processes and ICTs, leading to an unprecedented dependence on information technology in all organizations undergoing this major industrial paradigm shift (Kiss et al., 2019). A large quantity of research exists that indicates the advantages of IT innovation rooted in Industry 4.0, including the ability to overhaul existing organizational structures (Nimawat & Gidwani, 2021; Wilkesmann & Wilkesmann, 2018), to gain competitive advantage through business model innovation (Moellers et al., 2019; Singh et al., 2020) while leveraging customer involvement (Saldanha et al., 2017). Less studied are the cases in which increased implementation of technologies throughout organizational structures can have distinctly negative consequences, including increased stress on personnel (Atanasoff & Venable, 2017), increased vulnerability to cyberattack (Zhang et al., 2019), and the increased need for novel communication structures (Rudramuniyaiah et al., 2020). These relatively unexamined negative consequences are the primary subject of this study.

Scholars have traditionally focused on the advantages of using IT implementations to increase innovation. Scholars studying the relationship between IT and innovation have confirmed multiple IT factors and outcomes that improve

organizational innovation and competitiveness, so the positive effects of IT innovation are not in doubt (Trantopoulos et al., 2017). However, researchers have also found distinct negative outcomes stemming from IT implementations that should be addressed to ensure continual success (Atanasoff & Venable, 2017). As such, there must be a balanced focus in research regarding both the potential positive and negative consequences of such innovations to organizational health that can be mediated through innovation management. Despite the fact that IT implementations can help organizations innovate and generate competitive advantage, the same implementations can also introduce fundamental and structural disadvantages to firms that may not yet have been adequately addressed (Kiss et al., 2019; Kondiloglu et al., 2017). This has led to a rapidly shifting risk landscape that must be addressed.

The topic and discipline of organizational risk management has become a major issue in business research and practice. As informational assets and organizational processes become increasingly digitized, the structure of security risk changes, which increases overall risk throughout organizations as they have not fully prepared for this major paradigm shift (Caratas et al., 2019). This is particularly important because many businesses necessarily hold private and confidential client information which, for the purposes of achieving competitive advantage to some degree, the firms have digitized and made more vulnerable to hacking. This opens a large risk for companies' reputations if their systems are breached, such as in the 2017 Equifax data breach. By not establishing proper risk management protocols, companies are opening themselves up to major ethical violations. The Cambridge Analytica and Facebook breaches were clear

examples of the consequences of inadequate cybersecurity risk management (Caratas et al., 2019). To add to Caratas et al.'s mostly digital concerns, the Target and Home Depot breaches, as well as the Chicago Federal Aviation Administration fire, highlight the need for physical IS measures and increased cyber hygienic behaviors on the part of all organizational personnel (Branker et al., 2016; Dawson et al., 2018; Such et al., 2019). Increased digitization of organizational processes may also increase the physical methods by which hackers may successfully breach systems, such as through the theft of physical electronic credentials (Branker et al., 2016; Such et al, 2019). To address these increased digital risks, it is necessary for researchers and practitioners to identify the emergent loci of vulnerabilities.

Researchers have only recently begun to identify the domains of Industry 4.0 in which the negative consequences of ICT implementation have not yet been fully attenuated. The constantly evolving digital supply chain—currently making the transition from IoT to cloud computing to blockchain—has exhibited a bevy of emerging vulnerabilities that has had to be continually addressed, any of which have the potential to halt operations (Zhang et al., 2019). IoT and big data are being used to streamline various analytic processes in production and retail industries (Alferidah & Jhanjhi, 2020). Yet a single vulnerability in the very technological implementations that are designed to increase productivity, if breached, can lead to the disruption of the entire organization (Alferidah & Jhanjhi, 2020). In agriculture, IoT and big data are being used for soil monitoring, irrigation management and yield estimation (Bolek et al., 2016). If critical information about crop health is deleted, that season's yield may be dramatically harmed

(Bolek et al., 2016). IoT and Big Data are increasingly being used in physical retail, through the use of RFID technology to greatly streamline inventory management and to innovate the entire shopping experience (Alferidah & Jhanjhi, 2020). These new retail applications, however, are vulnerable to a wide variety of possible cyberattack methods and vectors (Alferidah & Jhanjhi, 2020). Despite the large amount of knowledge available and being applied regarding the tremendous operational advantages that Industry 4.0 technologies offer, neither large-scale organizations nor small- to medium-sized enterprises (SME) have adequately addressed the many risks inherent in increased IT implementation.

A nontechnical organizational vulnerability common to IT implementations is, incidentally, unaddressed consumer trust issues which stem from increased potential for cybersecurity vulnerability (Núñez-Merino et al, 2020; Zhang et al., 2019). Núñez-Merino et al. stated that the dramatic shift in flexibility that new ICT implementations contribute to organizations may also lead to factors that might inhibit or even degrade the organizational processes they augment. In a surface-level analysis, it may seem that the increased dependence on technology of this paradigm shift may reduce the importance of the human element as a security concern (Kiss et al., 2019). In fact, the single most common and difficult to address vulnerability in Industry 4.0 is insider threat (Bhaharin et al., 2019). Industry 4.0 is largely predicated on cyber physical systems, namely a more seamless integration between humans and ICTs. The human threat remains because the increased technological implementations only increase the probability that human errors will introduce vulnerabilities to organizational systems and processes (Kiss et al., 2019).

As a result, this human threat is a critical known vulnerability that must be addressed to help attenuate IS risk.

Insider Threat and Information Security Policies

The cost of a successful cybersecurity breach can be substantial. Globally, most firms report at least a single IS breach per year (Addae et al., 2019). In the United States healthcare industry alone, security breaches led to a total financial loss of $6 billion per year. According to PricewaterhouseCoopers (2018), a single data breach on average can cause 40% of operational distortion, 39% of either data loss or dilution, 32% loss of product efficacy, 29% harm to a firm's physical property, and 22% stakeholder harm to livelihood. Lowry et al. (2015) found that as many as 91% of organizational employees fail to comply to ISPs. The financial and operational costs may not be enough of an impetus for top-level management to prioritize IS in their organizations, which has led to further research into the significant degree of risk that employees can represent.

Empirical research has consistently supported the assertion that employees are the single greatest cause of IS breaches in firms of all industries and sectors (Addae et al., 2019; Bhaharin et al., 2019). Many cybersecurity weaknesses can only be taken advantage of through the exploitation of the individuals employed within the organization (Bhaharin et al., 2019; Branker et al., 2016; Choi et al., 2018; Daud et al., 2018; Neigel et al., 2020; PricewaterhouseCoopers, 2021). Insider threat refers to the continual threat that organizational insiders of all levels pose to organizational cybersecurity (Bhaharin et al., 2019; Choi et al., 2018). Insider threat is considered the single most substantial danger to organizational cybersecurity by far (Daud et al., 2018; Koohang et al., 2021; Moody et

al., 2018). The most fundamental way in which organizations address cyberthreats is through the implementation and enforcement of information security policies (Angraini et al., 2019). Investigating how organizational personnel can be encouraged to comply with ISP, thereby strengthening the organization's overall cybersecurity, has become a primary topic in the study of the role of human behavior in cybersecurity (Alzahrani et al., 2018). This has led to the investigation of the various factors that may mediate employee compliance to mitigate this human threat.

Insider threat cannot be quantified or qualified without accounting for the information security policies to which organizational personnel are required to adhere. ISPs define the security standards, behavioral boundaries, and personal responsibilities of all personnel that use technology within an organization, for all leadership and employees (Angraini et al., 2019). ISPs are documents that provide the guidelines, rules, and regulations to which all personnel within the organization must adhere to ensure that information technology assets and data stored within the assets remain secure when they are accessed and used (Angraini et al., 2019). ISPs are the primary means by which organizations control for information security behaviors, which can include ethics of computer usage, policies governing internet use, IT use policies, and use of social media (Bhaharin et al., 2019; Choi et al., 2018; PricewaterhouseCoopers, 2021; NIST, 2018). In research and practice, insider threat is operationalized as intentional or unintentional human errors that stem from ignorance, neglect, and failure to comply to ISPs (Angraini et al., 2019; Bhaharin et at., 2019). As such, it becomes clear why the field of ISPC involves the inextricable relationship between ISPs and human factors, perhaps

particularly in matters of technical IT implementation and management-oriented organizational governance (Bhaharin et al., 2019). As ISPs are the most widely used institutionalized means of enforcing employee compliance and reducing insider threat, it is also clear why these policies have been and continue to be one of the primary topics in cybersecurity research and practice.

To better contextualize the role of ISPs in organizations, it is necessary to detail how organizations typically manage cybersecurity risk. According to Caratas et al. (2019), organizations typically use some form of the Three Lines of Defense Model for managing cybersecurity risks. The first line of defense involves the point where risks are identified and managed, namely through top management controls and through internal organizational measures of control. This first line of defense represents operational management: all of the risk assessment, response, and management operations that are operated by the relevant management personnel. The second line of defense involves organizational risk management and compliance functions, namely the risk management apparatus and environment within firms. This also involves senior management but also includes the organizational components of financial controls, risk management, organizational security, intraorganizational inspection, quality management, and ISPC. It is this level at which top management is supported by technical expertise and expert monitoring so that the ground-level response to the identified threats is satisfactory. The third line of defense involves independent internal audits of the organization, which is reported to some committee or governing body (Caratas et al., 2019). Note the overall integration of ex ante and ex post risk management efforts at the organizational level,

such that capacities for both breach prevention and response are maintained (Kuerbis & Badiei, 2017). ISPs, then, exist within the border of the first and second lines of defense, being organizational mandates developed at first line management, but implemented and refined at the second line prevention functions, thus contextualizing where ISPs and insider threat lie within IS risk management.

In order to provide further insight into the risk landscape of increased IT implementation, Bolek et al. (2016) enumerated a number of internal and external factors by which IT can contribute to cybersecurity risk, then investigated their relationship to IS risk. Internal factors included employee ignorance, employee behaviors, absence of IT department, lack of support by senior management, insufficient hardware, hardware or software faults, insufficient software, lack of standards or guidelines, and lack of financial resources for IT or IS. External factors included IT certification, governmental IS legislation, governmental IS support, technological progress, risk of natural disaster, and failure of third-party services. The most statistically significant IS risk factor was employee behavior, which is to say insider threat. The other statistically significant factors were related to insider threat and ISPC, including absence of IT department, lack of management support, absence of internal standards and guidelines, certification, lack of government support, technological progress, and failure of third-party service (Bolek et al., 2016). It is critical to note the common denominator in Bolek et al.'s findings that align with those of other ISPC researchers: each of these IS risk factors involve organizational insiders as a primary agent (Angraini et al., 2019; Daud et al., 2018; Koohang et al., 2019). This further confirms the centrality of human affect, cognition,

and behaviors when examining organizational cybersecurity and ISPC, namely the importance of the human element.

The significance of the human element is confirmed by real world examples of successful security breaches. Researchers have repeatedly stated that a significant number, if not a majority, of cybersecurity breaches can be traced back into human noncompliance to ISPs and lack of cyber hygiene. The more public of these include the "Wannacry" ransomware event, the Target breach, the Home Depot breach, and Chicago's Federal Aviation Administration fire (Branker et al., 2015; Daud et al., 2018; Hummer et al., 2016; Such et al., 2019). Such breaches cost organizations significant human and financial capital, making security noncompliance a persistent risk to organizational health and security (Ponemon Institute, 2018). Researchers have repeatedly pointed out the gap in IT security research and practice regarding the behaviors, attitudes, beliefs, and knowledge that contribute to security policy compliance or noncompliance (Angraini et al., 2019; Branker et al., 2016; Daud et al., 2018). These incidents serve as proof that employee and management ignorance of organizational ISPs are greatly exacerbating the risk of security breach (Daud et al., 2018). The logical next step is determining the factors that mediate employee and management understanding of and compliance with ISPs.

In the realm of organizational IS, the proper management of employee access to secured networks remains a significant problem. The problem continues despite the implementation of identity access and management systems (Hummer et al., 2016; PricewaterhouseCoopers, 2021). This employee-centered problem persists because

employee access management dictates the personnel that can interface physically with IT/IS implementations (Hummer et al., 2016). Many security breaches are caused by ineffective user management, which leads to overprivileged users that unknowingly have the permissions to compromise an organization's security (Hummer et al., 2016). Consider the 2014 Target breach, which was only possible because hackers had gained access to an employee's credentials which were not physically secured as per proper ISP protocols (Such et al., 2019). Organizations have turned to implementing identity access and management technologies in order to better manage employee access to information systems (Hummer et al., 2016; Khansa & Liginlal, 2012). However, employee compliance to new identity access management policies remains a problem, as researchers have consistently found that information systems security professionals most often cite employees as one of the greatest sources of security incidents (PricewaterhouseCoopers, 2021). As these examples demonstrate, factors that mediate ISP awareness and compliance are quite complex, which has led a set of researchers to focus purely upon the potential of cyber hygiene to mitigate organizational cybersecurity risk.

Cyber Hygiene

Prior to an in-depth discussion on information security policy compliance, it will be important to distinguish this topic from cyber hygiene, a newly emergent topic related to ISPC but more general in scope. Cyber hygiene largely refers to the establishment and maintenance of behaviors associated with a healthy cyber environment (Cain et al., 2018; Neigel et al., 2020). Cyber hygiene is characterized according to three dimensions: (a)

awareness and knowledge of cybersecurity, (b) attitudes toward cybersecurity, and (c) behaviors directly or indirectly pertaining to cybersecurity. As with ISPC, cyber hygiene is not only associated with IT personnel, but all individuals within an organization that interact in any way with IT hardware and software (Neigel et al., 2020). Cyber hygienic behaviors include regularly checking one's hardware and software for signs of hacking or potential threats, routinely revising passwords without recycling old passwords, keeping software updated, and other actions that are designed to maintain cybersecurity at the personnel level of an organization (Neigel et al., 2020). Cyber hygiene does not pertain specifically to how organizational actions affect ISPC, but instead pertains to more generalized patterns of behavior and how they mediate an organization's cybersecurity (Such et al., 2019; Vishwanath et al., 2020). Though cyber hygiene does not yet have a large academic or empirical foundation of literature, existing research into this topic may provide insight into ISPC-related issues. Likewise, because of the relative newness of cyber hygiene, research into this topic tends to be more practical in nature which can provide real-world insight into ISPC. In all, cyber hygiene studies tend to focus upon general individual antecedents to cybersecurity knowledge, attitudes, and behaviors, thereby providing a potentially useful independent variable in the present study.

The primary issue of using cyber hygiene as a research construct is due to its newness as an IS concept relative to other constructs. Despite the increased interest, there is yet no academic or industry consensus on the definition or operationalization of cyber hygiene (Vishwanath et al., 2020). Furthermore, there exist no accepted holistic measures of cyber hygiene (Vishwanath et al., 2020). Although many researchers have focused on

specific user behaviors (Egelman & Peer, 2015), such measures assume that participants are aware of such behaviors, thereby limiting measurements to actions that are potentially widely known to personnel (Vishwanath et al., 2020). However, researchers have begun to operationalize cyber hygiene for future research.

Although cyber hygiene has not yet been fully operationalized in a manner accepted throughout IT, researchers have begun to frame the concept. According to Vishwanath et al. (2020), there are three aspects of cyber hygiene that are important when constructing a definition. First, cyber hygiene is complex and multidimensional; each relevant dimension contains multiple factors and subfactors that contribute to the understanding of what comprises hygiene (Vishwanath et al., 2020). Second, cyber hygiene is a collection of guidelines regarding blanket actions which personnel should follow and build a subconscious vigilance for, akin to physical hygiene habits like handwashing (Vishwanath et al., 2020). Third, hygiene can only have a general definition because practices occur in different contexts and cultures (Vishwanath et al., 2020). These three elements contextualize cyber hygiene as all actions pertaining to protecting one's information when interacting with technology (Cain et al., 2018; Neigel et al., 2020; Such et al., 2019; Vishwanath et al., 2020). Unlike Moody et al.'s (2018) attempt at refining a holistic model for ISPC, researchers have not yet holistically modeled the complexities inherent in cyber hygiene. As a result, cyber hygiene can refer to any number of factors and variables by which human cognition and behavior mediates cybersecurity outcomes.

The premise for cyber hygiene research is much akin to that for other cybersecurity topics. Like scholars investigating insider threat and ISPC, cyber hygiene researchers contend that novel cybersecurity threats continue to emerge despite increased expenditures and improved technology because human error introduces vulnerabilities that can be taken advantage of regardless of the security of an organization's IT systems (Dupuis, 2017; Neigel et al., 2020; Sawyer & Hancock, 2018). The billions that are spent annually, with expenditures only increasing each year, have by no means eliminated cyberattacks nor have they attenuated the emergence of newer and more serious threats (Neigel et al., 2020). Unlike conventional insider threat and ISPC research, however, cyber hygiene researchers focus primarily upon the individual as the primary cause of cyberattacks, data leaks, and successful scams—whether in private or within their professional context (Neigel et al., 2020). As such, cyber hygiene is not specific to the organizational context, but pertains to any individual whose private, financial, and social information is at risk from cyberattack (Cain et al., 2018; Such et al., 2019; Vishwanath et al., 2020). This is not to say that there is no overlap between cyber hygiene and ISPC research, but that their contexts differ.

Many factors can potentially mediate cyber hygiene in individuals. Cybersecurity awareness and knowledge are primary antecedents to cyber hygiene behaviors (Dupuis, 2017). But more specific, trait-level, and behavioral antecedents to cyber hygiene exist. Using a number of validated measures of cybersecurity knowledge, computer self-efficacy, trust in technology, and locus of motivation, Neigel et al. (2020) investigated the statistical significance of various potential behavioral and trait-level antecedents to

cyber hygiene in university students. Use of the internet, handling of digital information, and use of social media were predictive of cyber hygiene knowledge, while handling of digital information, use of social media, smartphone use, and password management were predictive of positive attitudes toward cyber hygiene. Handling of digital information, past incidents of reporting cybersecurity incidents, regular use of email, use of the internet, and password management were significantly related to cyber hygienic behaviors. Neigel et al. also uncovered unique gender-specific predictors of cyber hygiene behaviors, attitudes, and knowledge. The researchers identified a number of potential traits that made participants vulnerable to social engineering attacks, such as through the male propensity to trust in technology or the role of intrinsic motivation in predicting female cybersecurity attitudes (Neigel et al., 2020). These behavioral and trait-level factors reveal the complexity involved in understanding insider threat, which is demonstrated in Moody et al.'s (2018) large-scale UMISPC. Neigel et al. also stated that adequate cyber hygiene education is lacking in the modern educational system, with many participants lacking in cybersecurity knowledge and highly vulnerable to many different types of cybersecurity attack vectors. These findings likewise confirm similar statements made by ISPC researcher regarding the failings of cybersecurity education (Addae et al., 2019; Alshaikh, 2020; Angraini et al., 2019; Dawson, 2018). Cyber hygiene, then, confirms ISPC research regarding the centrality of cybersecurity awareness, knowledge, and education in the mitigation of insider threat.

Demographics can also provide insights into cybersecurity knowledge and behaviors. Cain et al. (2018) engaged in a study of a diverse set of participants,

investigating their knowledge of cybersecurity threats, knowledge of cybersecurity concepts, and cyber hygiene behavioral patterns, while using descriptive statistics rooted in demographical antecedents. Particularly insightful were differences in demographic effects. The youngest and oldest cohorts tended to share too much information through insecure social media platforms, while the majority of all cohorts did not check their privacy settings. Counter to common assumptions, those from older cohorts tended to behave in a more cyber hygienic manner, while no significant difference in knowledge of cyber hygiene was found between any cohorts. Though males had more cyber hygiene knowledge than females, both genders had comparable levels of hygienic behaviors. Surprisingly, experience with prior cybersecurity incidents did not increase cyber hygiene. Likewise, self-identification as cybersecurity experts were correlated with less hygienic behaviors and less cybersecurity knowledge. Finally, although the majority (81%) of all participants reported some cybersecurity training, this education was not related to any increase in either cyber hygienic knowledge or behaviors (Cain et al., 2018). Both Neigel et al. (2020) and Cain et al.'s studies provide a general profile of the knowledge, attitudes, and actions of individuals regarding cybersecurity which can be used to better promote actions that promote rather than harm organizational cybersecurity. Though these studies do not apply directly to the organizational setting, for example, the findings reveal the inherent threats to cybersecurity that a typical insider poses for an organization. Both studies uncover the possibility of gender- or age-specific social engineering opportunities to leverage insiders' demographics as a potential cyberattack vector. Both studies' findings on the ineffectiveness of cybersecurity training

also reveals a potentially critical issue, that schools and organizations may need to develop IS education regimes that are more effective in mediating actual cyber hygiene behaviors.

Researchers have been investigating generalized cyber-hygiene-based implementations for small- to medium-sized enterprises (SME) that do not yet have sophisticated IT departments to systematically formulate and deploy organization-specific ISPs, cybersecurity training, and IT management. Such et al. (2019) investigated the effectiveness of a specific low-cost cybersecurity scheme, the United Kingdom's Cyber Essentials, in such SMEs. These protocols are a marked contrast to market offerings in which third-party cybersecurity firms external to the business in question offers services to organizations without ISPs or full IT departments (Kuerbis & Badiei, 2017). Though not as comprehensive as ISPs, these low-cost cyber hygiene focused security protocols are increasingly being required from SMEs by organizations that contract their services, namely government agencies and companies with large supply chains (Mon & Giorgio, 2021; Such et al., 2019). Through case studies of multiple different types of SMEs—finance, specialist scientific services, web development and online services, and hospitality—Such et al. investigated a wide range of organizations to determine the efficacy of Cyber Essentials in increasing the cyber hygiene of organizations. Significant observations included: (a) that vulnerabilities are not just a function of network and service complexity, (b) that Cyber Essentials mitigated most threats as long as basic measures were strictly adhered to, (c) that routine maintenance on IT implementations are critical, and (d) that third party software can circumvent the

Cyber Essentials scheme. Like other researchers, Such et al. found that the majority of the most severe vulnerabilities were centered around either organizational insiders or guest privileges. Attenuating this insider threat, however, was the fact that many of these vulnerabilities could be addressed by simple measures that were relatively easy to enforce (Such et al., 2019). Though these low-cost bare minimum cybersecurity standards can be effective to a certain degree, they do not directly address insider threat, which remains the largest cybersecurity vulnerability.

Information Security Policy Compliance

In both research and practice, information security policy compliance (ISPC) is the principal topic that must be examined when addressing how insiders affect cybersecurity. ISPC remains the single greatest issue that must be addressed when considering ISP implementation, insider threat, and organizational cybersecurity (Angraini et al., 2019; Cain et al., 2018). The main problem with ISP implementation is not the accuracy of the policy documents themselves, which are usually developed from the technical perspective, but that of noncompliance to ISPs on the part of organizational personnel at all levels (Angraini et al., 2019; Daud et al., 2018). As presented above, human beings remain the largest threat to organizational cybersecurity.

To better understand organizational ISPCs, researchers have used varying methodologies to determine statistically significant factors that mediate compliance. Sommestad et al. (2014), for example, engaged in a systematic literature review to identify the factors that mediate compliance and to determine each factor's importance in mediating compliance. The researchers identified 61 distinct and statistically significant

predictors of ISPC. Sommestad et al. were able to organize these factors into six categories: (a) individual attitudes toward compliance behaviors, (b) intent to comply with ISPs, (c) actual compliance behaviors, (d) individual attitudes toward misuse of IT, (e) intent to misuse organizational technology, and (f) actual misuse behaviors. A notable aspect of this study was the lack of categories regarding cybersecurity knowledge, awareness, or education. Sommestad et al. were not able to find variables that were clearly more significant than the others. Although it is unfortunate that no key factors were found, this is likely due to the disparate findings from the reviewed studies. The results are likely a sign of the relative newness and perhaps a lack of accountability in compliance research (Hina & Dominic, 2017; Indu et al., 2018). But as Moody et al. (2018), Rajab and Eydgahi (2019), Koohang et al. (2021), and Choi et al.'s (2018) studies demonstrated, scholars have begun to consolidate cybersecurity research and the cybersecurity field as a whole. This section will include a survey of the major predictive factors of ISPC, each of which will feature various subfactors, including intent to comply, awareness, communication, culture, affect, norms, habits, deterrence, and organizational governance.

Intent to Comply

Though seemingly self-evident, intent to comply remains a highly validated ISPC factor. As Sommestad et al. (2014) confirmed, intent to comply is a popular antecedent in research. Alzahrani et al. (2018) investigated the intent of employees to comply to ISPs using self-determination theory as the theoretical framework. Investigating mediators and factors that influence employees' compliance to ISP and intent to comply have become

increasingly important (Alzahrani et al., 2018) as researchers have begun to argue that prior research, what can be called traditional ISPC research, has put too much focus onto technological measures that do not account for the vulnerabilities that are characterized by the actions of organizational personnel (Elifoglu et al., 2018; Luo et al., 2020). Alzahrani et al. examined the roles that the subfactors of intent to comply—including autonomy, competence, relatedness, perceived legitimacy, and perceived value congruence—can play in influencing employee intent to comply to organizational ISP. Having controlled for age, education, experience, and sample size, the researchers found that autonomy, competence, and relatedness are positively correlated with compliance intent (Alzahrani et al., 2018). Perceived value congruence, which is the degree to which an employee's values are congruent with that of their organization, was negatively correlated with compliance intent and perceived legitimacy had no significant correlation to compliance intent (Alzahrani et al., 2018). The use of compliance intent to predict for ISPC has remained statistically significant (Koohang et al., 2019; 2021), and is included in Moody et al.'s (2018) UMISPC as an integral factor. Though a simplistic factor relative to others, intent continues to prove its utility in predicting for ISPC.

Awareness and Knowledge

Awareness and knowledge have recently emerged as key factors in predicting for ISPC. The potential for cybersecurity and cyber hygiene knowledge to directly influence compliance behaviors has been repeatedly acknowledged and confirmed (Cain et al., 2018; Kuerbis & Badiei, 2017; Neigel et al., 2020; Such et al., 2019). Koohang et al. (2019) integrated multiple "sociological, psychological, and organizational behavior" (p.

231) constructs and theories—including organizational leadership, trust in leadership, self-efficacy, and employee intent to comply—into ISPC research, arguing that they can have a mediating influence upon employee compliance. Competent leadership and greater employee trust, which are frameworks rooted in organizational psychology, have been found to positively influence employees, which can increase ISPC. Self-efficacy is a psychological measure of an individual's belief in one's ability to accomplish an objective or task, which multiple researchers found can be a direct mediator of ISPC. Using these existing frameworks, Koohang et al. created a quantitative survey instrument to investigate the importance of awareness in compliance. In analyzing the survey results, the researchers found that awareness toward security polices is positively related to leadership competence and employee trust toward the organization (Koohang et al., 2019). These findings align with the inherent predictiveness Cain et al. and Neigel et al. found that knowledge had regarding cyber hygiene, as well as the significant role that high-level leadership can have on overall awareness and compliance (Daud et al., 2018). Cybersecurity awareness and knowledge, then, may be direct predictors of organizational vulnerability to cyberattack.

Affect

ISP compliance researchers have tended to focus upon cognitive theories and processes that may mediate compliance behaviors in personnel. Others have more recently chosen to investigate affective theories and processes that can lead to noncompliance (Koohang et al., 2021; Moody et al., 2018; Ormond et al., 2019). Ormond et al. stated that affective factors may have a significant impact upon ISPC behaviors in a

manner distinct from cognitive factors, with a potential to be strong indicators for predicting employee actions that can either weaken or strengthen an organization's security against cyberattack. The notion of using affect to predict for behaviors is rooted in Triandis' (1977) theory of interpersonal behavior. Affect involves emotional processes, including antecedents to emotions, the emotions themselves, and the consequences of the emotions that arise in response to stimuli (Moody et al., 2018; Ormond et al., 2019; Triandis, 1977). In short, affect can be considered the overall emotional climate and attitudinal inclinations toward target phenomena, in this case toward organizational cybersecurity and ISPC, which can then mediate compliance behaviors and an organization's vulnerability to cyberattack (Moody et al., 2018; Ormond et al., 2019). Like intent, affect is an internal psychological factor that is proving to be a mediator of compliance.

Though affect has been investigated less than other ISPC factors, it has been quantified in more general and specific contexts. Moody et al. (2018), in a general validation of compliance factors in developing the UMISPC, found affect to be statistically significant, though the researchers ultimately chose to subsume the concept into a more comprehensive factor titled role values (Koohang et al., 2021). Ormond et al. (2019), in contrast, advocated a more in-depth examination of affect. The researchers considered affect in terms of two factors. Affective absorption refers to an individual personality trait regarding the degree to which the individual allows emotions to drive their decision-making processes. Affective flow refers to individuals' state of immersion with their emotions. Results indicated that work-related frustration led to negative affect

flow, which resulted in ISP noncompliance. The researchers also found that perceptions of organizational injustice made negative affect flow increase (Ormond et al., 2019). Regardless of specificity, these findings confirm the effect that affective processes have on ISP compliance, and the need for information security researchers to pursue more holistic approaches to compliance research that include emotive and attitudinal factors.

Habits

ISPC is not only a function of affective or cognitive factors, but can also be mediated by the behavioral habits that insiders have accumulated over time. Nord et al. (2020) focused specifically on investigating habit as a factor rooted in the theory of interpersonal behavior. Habits were defined as (a) automatic reactions in response to specific events or situations, (b) automatic tendencies of behaviors, and (c) behaviors that are enacted due to a degree of practice or repetition. Nord et al. investigated ISP habits using the independent variables age, gender, IT knowledge, and IT awareness. The researchers found that differences in the independent variables—that is, differences in age, gender, knowledge, and awareness—were linked to significant mean differences in IT habit scores. ISP awareness and IT knowledge in particular exhibited significant mean differences in how they mediate ISP habits. The findings indicated that habits that are conducive to ISPC tend to be strengthened and reinforced through greater awareness and knowledge of organizational ISP. In summary, the study supports the importance of fostering ISP attentiveness and ISP knowledge to cultivate employee habits that lead to secure behavioral habits (Nord et al., 2020). Indeed, ISPC researchers must not limit themselves to purely cognitive factors, but make sure to investigate behavioral mediators.

Communication

Individual factors are not the only mediators of ISPC; there exist organizational and governance-related factors that can predict for how employees and managers adhere to ISPs. Communication refers to the flow of information throughout an organization, particularly information that is critical to organizational health, such as that pertaining to cybersecurity. Rantao and Njenga (2020) investigated how compliance behaviors can be affected by how ISPs are communicated throughout a firm, interpreted by stakeholders, and implemented by the firm. The authors found that research regarding the role of communication in ISP compliance is lacking. The researchers proposed that how ISPs are communicated can be a significant factor in compliance. Rantao and Njenga combined media synchronicity theory, communication theory, and media richness theory to construct what they termed the miscellany of perception and determination (MPD) framework to test communication in firms. Rantao and Njenga ultimately rejected and confirmed a number of factors within the MPD framework as communication-oriented predictors of ISPC. Factors with no statistically significant predictiveness of ISPC included communication media, familiarity with ISPs, quality of information, information processing time, and certainty of communication. Factors that were significantly predictive of ISPC included rationale for communication, appropriateness of medium used to communicate ISP information, nonconflicting interpretation of communication, and personalization of communication (Rantao & Njenga, 2020). Communication, though certain of its subfactors are nonsignificant, is clearly a consequential antecedent of ISPC.

A more technical term related to communication is knowledge sharing, which refers more to technical communication between professionals within an organization (Rudramuniyaiah et al., 2020). Reviewing ISPC literature, Rudramuniyaiah et al. found that there is a gap in the research regarding the influence that emotions can have on knowledge sharing behaviors, specifically among IT professionals. The researchers surveyed 205 IT professionals throughout the United States regarding the effects of various factors on knowledge sharing behaviors. Four hypotheses were supported: (a) IT specialization is associated with knowledge sharing, (b) organizational culture that promotes sharing is associated with knowledge sharing, (c) increased promotion of sharing strengthens the relationship between specialization and knowledge sharing, and (d) altruism is associated with knowledge sharing. In all, this study demonstrated that insider threat and lack of communication does not only exist in non-technical insiders, but can be an issue in IT personnel as well (Rudramuniyaiah et al., 2020). The validation of knowledge sharing as a factor also proves the existence of complex interpersonal and environmental factors that can have powerful mediative effects on compliance behavior.

Norms

Related to organizational culture are organizational norms which, like individual habits, accumulate within any established body of business. Wiafe et al. (2020) investigated how factors governing personal, subjective, and descriptive norms can influence ISP compliance. The authors found that much research indicates that punishments and sanctions are not necessary to enforce ISP compliance. Many researchers have found the application of criminology to ISPC unsatisfactory in

explaining influences to compliance. Because current research on the role of norms is lacking, Wiafe et al. proposed the use of the theory of panned behavior to identify the role of social norms in ISPC. Social norms are defined as informal guidelines or rules that guide behaviors in social contexts. Descriptive norms are norms that use the actions of others as a gauge for an individual's own behavioral patterns. Injunctive norms involve the collective moral rules shared within a group of individuals. Subjective norms involve an individual's perspective on how other people view a behavior. Personal norms involve an individual's personal beliefs, principles, and values concerning behavioral patterns. Using a survey research design, the authors collected data regarding ISPC and the various different types of norms that may mediate compliance. Personal norms and intent to comply were significantly related to each other. Results indicated that the relationship between personal norms and intent to comply is mediated by attitudes toward ISPC. Subjective norms and predictive norms both exhibited significant predictive relationships with personal norms. This study provides evidence for the use of norms in assessing ISPC behaviors. A major limitation of this study is that the actual compliance behaviors were not being objectively recorded, but rather attitudinal data that is highly subject to participant bias (Wiafe et al., 2020). Nevertheless, the concept of norms introduces another complex interpersonal and environmental mediator of ISPC.

Deterrence

Enforcing ISP compliance can also involve the use of deterrents to discourage personnel from violating policies. Jaeger et al. (2020) approached the topic of deterrence from a new, multidimensional perspective in evaluating the effectiveness of sanctions.

Using findings in criminology, the researchers proposed that such discrepancies might be addressed by more closely examining the potential moderating role of employee expectations, as well as accounting for the possibility that employee deterrability can play a major role in successful deterrence. In criminology, deterrence is defined as the process by which an individual assesses the risks and rewards before deciding to violate a policy. Deterrability is defined as the willingness of an individual to engage in the deterrence calculation (Jaeger et al., 2020). This is akin to threat appraisal (Rajab & Eydgahi, 2019), though focused singularly upon deterrents. The concept of deterrence, however, involves making cognitive and environmental characterizations distinct from PMT.

Deterrence is not only a function of environmental threats, but also the cognitive and affective disposition of individuals toward these threats. Jaeger et al. (2020) introduced a key distinction not found in other theories: inclined compliers and disinclined compliers. Inclined compliers are individuals who comply with ISP due to positive attitudes toward information security. Disinclined compliers are individuals who comply with ISP despite negative attitudes toward the policies, due to potential sanctions. The researchers made a further distinction between externally imposed and internally (i.e., personally) imposed sanctions. Jaeger et al. found that inclined compliers were more motivated by personal norms rather than official or unofficial external sanctions. Inclined compliers were found to be undeterrable by external sanctions, and ISP compliance behavior followed their internal convictions of whether behaviors were reasonable. Disinclined compliers, however, were found to be deterrable by external sanctions, influenced by punishment severity more than certainty of punishment. Furthermore,

disinclined compliers were more inclined to be motivated by potential informal (e.g., social) sanctions rather than formal sanctions (Jaeger et al., 2020). The framework of ISPC deterrence, then, illustrates the complex interactions that can exist among trait-level, cognitive, and environmental factors to mediate compliance.

Sanctions

Sanctions are related to the concept of deterrence, but manifest themselves within a different set of theoretical frameworks. Using justice theory, neutralization theory, and deterrence theory, Alshare et al. (2018) identified seven statistically significant factors related to the potential role of sanctions in ISPC. Celerity of sanctions refers to the speed by which sanctions are enforced, which is an aspect of deterrence theory. Severity of penalty refers to the degree by which corrective measures reflect the severity of the violation in question, another aspect of deterrence theory. Organizational security culture refers to the awareness of all levels of personnel regarding ISPC, sanctions, and security management throughout a firm. Privacy refers to the degree of respect that individuals have for the privacy of their own personal information. Responsibility refers to the degree to which personnel feel an individual responsibility for protecting organizational assets. Organizational justice theory involves procedural justice, interactional justice, and distributive justice. Procedural justice refers to fairness and lack of bias in the decision-making process. Distributive justice refers to how employees compare their reward-contribution ratio with others (Alshare et al., 2018). As this study highlighted, the organization and environment are significant mediators to ISPC.

Culture

Organizational ISPC factors need not directly mediate insider behavior through rewards or consequences. Alshaikh (2020) examined the concept of cybersecurity culture, which is an organization's social context regarding employee compliance. Cybersecurity culture shifts the focus from compelling compliance to creating a sustainable process in which employees will naturally comply. Through an interpretive case study research design, the researcher identified five key initiatives that can transform security education, training, and awareness (SETA) efforts from a compliance focus to a culture focus (Alshaikh, 2020). The initiatives are much like proposed methods by which cyber hygiene could be promoted within organization (see Vishwanath et al., 2020), except more systematic in nature. The first initiative is to simplify the identification of the most important cybersecurity behaviors to increase awareness and to allow for focused effort in changing behaviors rather than beliefs (Alshaikh, 2020). Second, implementing a champion network to better facilitate cybersecurity communication and education. Third, building a hub that can continually provide cybersecurity education and training for key cybersecurity behaviors. Fourth, establishing a brand with which cybersecurity personnel can establish greater credibility and market cybersecurity compliance to personnel. Finally, aligning cybersecurity awareness efforts with internal and external campaigns will allow for more complete integration into all organizational processes (Alshaikh, 2020). Together, these five initiatives contribute an understanding of exactly where researchers, practitioners, and organizational leaders must concentrate their efforts to

construct a culture by which ISPC may occur more naturally than through more conventional methods.

Top Management

Organizational ISPC factors can also include how leadership interacts with and is perceived by insiders. Hu et al. (2012) developed and tested a behavioral model that could improve ISPC by combining theoretical frameworks that contextualize the roles of top management involvement and organizational culture in mediating compliance within an organization. The researchers found that top management involvement and organizational culture can play critical roles in encouraging security compliance in employees. Hu et al.'s study is relevant to the IT field because of the immediate relevancy of their results. It is true that the study is limited in that the researchers were investigating complex factors—top management involvement and organizational culture—which have yet to be fully defined in IT research literature. Yet the inherent complexity only implies that more research may give additional insight into the mediators of employee compliance. Finding that top management is critical to employee compliance may be quite useful in determining more effective security programs. Understanding the role of organizational culture may also help IT researchers and professionals develop organization-wide programs that could improve IT security (Hu et al., 2012). In summary, the study confirms that organizational factors that do not directly mediate employee actions can have powerful effects on ISPC.

Cooperation

Top management commitment and involvement are not the only ways in which organizational leadership can promote compliance. Daud et al. (2018) investigated the effect of organizational practice of cooperation—including top management commitment (TMC), security investment (SI) and structured security processes (SSP)—on employee compliance. The researchers found that TMC and SSP, but not SI, had indirect mediating effects on compliance, relationships not found in prior research. The results imply that security can be improved through cooperation and collaboration throughout an organization, rather than isolating or compartmentalizing information security issues. The findings also confirm that the involvement of top management and organizational security processes are integral to compliance. IT security can be very compartmentalized, which can lead to a lack of knowledge on the part of executives and non-IT personnel. Daud et al. demonstrated that organizations may need to adapt to more holistic and integrated approaches to improving security compliance. Piecemeal implementations may not be the most effective, considering the increasing number of holistic and consolidated models and frameworks currently being developed.

ISPC Models and Frameworks

Much like how researchers have begun to develop more holistic theories of ISPC, scholars, practitioners, and organizational leaders have begun to develop strategies by which the many empirical findings and principles in the body of literature can be applied in organizational practice. As IT research is inextricably rooted in practice, the aim of many researchers has been to create empirically validated frameworks by which ISPs can

be successfully integrated in the organizational setting, ISPC can be promoted, and organizational cybersecurity can be maximized. Many of these ISPC frameworks have not yet been tested in the organizational setting because these are research-based models awaiting actual implementation (Moody et al., 2018; Sharbaf, 2019). The ISPC frameworks presented in this section are distinct from theoretical constructs (such as PMT and UMISPC), in that the former are designed to be applied directly to organizations while the latter are designed to structure theoretical principles. Like emergent cyber hygiene research, ISPC frameworks focus upon practical application over theory. Unlike most cyber hygiene research, in which many constructs are still being confirmed, ISPC frameworks have been constructed using research-based principles and are designed to be understood from the organizational perspective rather than the theoretical. As a result, examining these models can provide insights into the nature of the relationships between insider and cybersecurity from the context of how organizations actually operate while avoiding speculation and retaining methodological rigor.

A Holistic Cybersecurity Framework

Unlike theoretical frameworks, cybersecurity frameworks refer to practical ways that cybersecurity can be systematically applied throughout an organization. Dawson (2018) proposed a holistic cybersecurity framework that accounts the global IT business landscape. In this framework, Dawson integrated three essential cybersecurity topics that are typically examined separately: (a) cybersecurity education for organizational personnel, (b) cybersecurity and the role of technology, and (c) information security

policy. Using specific examples in the education sector, Dawson stated that cybersecurity education will eventually be integrated into current public and private institutions, particularly as Industry 4.0 leads all sectors toward hyperconnectivity. The researcher noted that as more aspects of organizational functioning become connected, cybersecurity knowledge will become a general prerequisite. Next, using the 9/11 event and its aftermath as a key example, the researcher details the importance of public policy for technology implementations. Finally, using existing cybersecurity accreditation and certification, Dawson demonstrated the need for the secure installation of technology and software into existing organizations. In summary, Industry 4.0 is quickly reaching the point where cybersecurity must be addressed at all levels of business, from educating the workforce, to national governance, and to the use of rigorous certification and accreditation processes.

A Security Quality Management Model

Models by which the quality of cybersecurity can be managed are just as necessary as practical frameworks. Sharbaf (2019) presented a 10-part cybersecurity (CS) quality management framework that provides context and insight into how a more secure IT implementation may be executed throughout an organization. First is to develop and maintain an organization-wide CS culture. Second, develop a consistent and persistent purpose within the organization to improve quality. Third, establish CS training, education, and awareness. Fourth, eliminate barriers between IT personnel and other departments while making CS an organization-wide responsibility. Fifth, develop and enforce high-quality information security policies. Sixth, develop and implement a sound

multi-layered CS strategy. Seventh, create and implement a system of monitoring CS quality. Eighth, create a life cycle for CS program which includes risk management, risk and defense measurement, process improvements, and process management. Ninth, establish a holistic approach to CS throughout the organization which integrates personnel, processes, and technology. Finally, align and design CS program to organizational needs and objectives (Sharbaf, 2019). Notable to this model is the importance given to addressing insider threat, intraorganizational communication, constant monitoring and updating, and adapting existing systems to new and emergent threats. Though this model remains yet untested, it illustrates just how many factors a truly effective and self-sustaining ISP implementation must address.

An Integration of Cybersecurity and Corporate Communication Strategy

Corporate communication strategies are yet another way in which organizations may leverage cybersecurity research to improve ISPC. As Rudramuniyaiah et al. (2020) found, improper communication about increasingly inevitable cybersecurity breaches can lead to significant loss in customers and revenues, which necessitate process innovations in corporate cybersecurity communication. Knight and Nurse (2020) investigated how corporations engage in public relations and crisis communication in the event of a cyberattack. The researchers then developed a two-part framework that corporations can use to structure effective communications in cybersecurity breach events. The first part of the framework is ex post crisis preparation for any future response, consisting of five components: establishing the goals of the company after a cybersecurity breach, determining potential security vulnerabilities, creating and maintaining a cybersecurity

knowledge base, integrating cybersecurity preparation with partners and stakeholders, and ensuring that proper cybersecurity basics are in place. The second part consists of a six-step ex ante sequence: (a) deciding whether the breach should be disclosed, (b) establishing exactly what should be disclosed to the public, (c) choosing when the message should be disclosed, (d) selecting how the message is disclosed, (e) preparing for the inevitable reaction, and (f) continuing to deliver the message (Knight & Nurse, 2020). Though this framework must be tested in future research to be validated, this integration of corporate communication strategies and cybersecurity demonstrates that it is possible to take existing organizational standard operating procedures and apply measures that can increase compliance.

Proposal for Performance-Enhancing ISP Implementations

There are instances in which researchers have proposed novel investigations that may result in innovations that may enhance organizational cybersecurity in a synergistic manner. Urhuogo et al. (2014) stated that despite the variety of IS research relating to compliance and ISPs, there has been a general lack of research regarding the effects of organizational IS on individual employees. The researchers proposed a novel approach to addressing this lack: structuring IS and ISP in a way that could actually enhance, rather than impede, individual performance in the workplace, which would not only improve compliance but lead to positive security effects on the organization as a whole, thereby preserving valuable resources and protecting profits. Although the authors did not actually engage in empirical research, but rather only detailed a qualitative research proposal using the system development life cycle as a theoretical framework, Urhuogo et

al.'s paper is of note because the possible variations of cybersecurity implementations have not yet even begun to be exhausted. Regardless of the lack of detail, the possibility of making cybersecurity an integral aspect of the workplace may allow organizations to more effectively secure their information systems.

Top-Management Implementations of Compliance-Centered Cybersecurity Systems

Written accounts of how new cybersecurity systems and ISPs have been implemented within large organizations with a focus on maximizing employee compliance have been nearly nonexistent in the body of research. Pullin (2018), CEO of a large New Jersey health care system, detailed a rare and insightful case study of a complete cybersecurity overhaul of the entire organization. Current scholarly literature and empirical research lack concrete examples of real-world applications of empirically validated ISP principles, instead focusing upon validating theoretical components (Moody et al., 2018). As the head of a health care service provider who noted the importance of ISPC in cybersecurity efforts, Pullin presented a singular write-up of how a revised system and policy of compliance-focused cybersecurity was implemented in a large regional service-based organization. Organization-wide ISP revisions included a board-level committee on IT, the appointment of a Chief Information Security Officer, a revised protocol for vendor management, significant investment into and integration of IS technologies, partnering with a third-party cybersecurity firm, and establishing a consistent employee cybersecurity education protocol. Although Pullin's case study lacks scholarly citations, the overall framework emulates empirically validated cybersecurity principles in a detailed manner and can be assessed accordingly. Most notable in Pullin's

organization-wide cybersecurity implementation, for instance, was the integration of the human element beyond simply mandating all personnel to read and follow ISPs. Rather, Pullin actively promoted cybersecurity awareness and knowledge, a decision confirmed by emerging ISPC models that increasingly emphasize education and awareness over simple directives (Dawson, 2018; Moody et al., 2018). Pullin's implementation strongly resembles Sharbaf's (2019) framework, though the two remain unrelated. An integral aspect of the new system was engaging top-level leadership to be involved throughout many aspects of the cybersecurity effort, an approach validated by multiple studies (Caratas et al., 2019; Daud et al., 2018; Hu et al., 2012). Pullin's top-down approach to governance and risk management has also been confirmed by research (Bhaharin et al., 2019; Hina et al., 2019). In summary, this case study exemplifies how ISPC can be maximized in a systematic, organization-wide manner while putting empirically tested principles into actual practice.

Conclusion

The purpose of this quantitative correlational study was to investigate the relationship between ISPC factors, cyber hygiene factors, and organizational vulnerability to cyberattack. Cybersecurity issues are becoming increasingly difficult for organizations to ignore, with the global average cost of breach having reached $4.24 million in 2021 (Ponemon Institute, 2021). As the paradigm shift toward Industry 4.0 technological implementations becomes even more important to achieving competitive advantage, organizations are introducing ever more unknown and emergent vulnerabilities into their information systems (Bhaharin et al., 2019;

PricewaterhouseCoopers, 2021). All the while, consumer trust has become inextricably linked to organizational cybersecurity capabilities as the public awareness of cybersecurity issues has increased (Kuerbis & Badiei, 2017; PricewaterhouseCoopers, 2021). Implementing cybersecurity measures does not only involve technological interventions, however, as repeated studies have revealed insider threat—the weaknesses introduced by human actors within an organization—as the single greatest and most difficult to address source of vulnerabilities (Bhaharin et al., 2019; Daud et al., 2018; Such et al., 2019). The threat represented by organizational employees, management, and leadership was this study's primary topic of concern.

The theoretical framework underlying the present study was protection motivation theory (PMT). PMT incorporates two affective and cognitive antecedents to risk management actions: threat appraisal and coping appraisal (Choi et al., 2018; Rajab & Eydgahi, 2019). A thorough survey of PMT was presented in the literature review. PMT was chosen because of its alignment with ISPC and the present study's variables. The theory was also chosen because of its strong history of predictive power in cybersecurity research.

Information security policy compliance and related research was reviewed in detail, beginning with a detailed exposition of Industry 4.0 and its consequences for information security. Cyber hygiene, an emergent field focusing upon awareness-based behavioral habits that can reduce cybersecurity vulnerabilities, was also reviewed to context regarding the various behavioral complexities that mediate information security. Then, a thorough survey of the many known factors that have been found to be mediators

of ISPC was presented to contextualize the present study within the body of research. This section closed with a review of holistic ISPC models and frameworks by which research principles could be applied to organizational settings.

Information security policy compliance and cyber hygiene are critical issues that require further research, in a greater effort to formulate practical solutions that can be holistically applied throughout an organization's infrastructure. This study's aim was to address a gap in knowledge regarding top-level management. By investigating the effect of cognitive and organizational factors on cybersecurity breach prevalence, it may be possible to generate significant practical insight into top-level management effect on information security.

Section 2: Project Design and Purpose

The purpose of this quantitative correlational study was to investigate the relationship between ISPC factors, cyber hygiene factors, and organizational vulnerability to cyberattack. In this study, I conducted a quantitative correlational research design using secondary data sourced from the United Kingdom Department for Digital, Culture, Media and Sport's (DCMS) 2021 Cyber Security Breaches Survey (CSBS), which has been subcontracted to the third-party research firm, Ipsos MORI, since 2016 (Ipsos MORI, 2021a; 2021b; 2021c). The independent variables, found in the 2021 CSBS dataset, included: (a) perceived importance of cybersecurity, (b) senior management involvement, (c) use of organizational ISPC, and (d) seeking of information or guidance on cybersecurity. The dependent variable, also found in the 2021 CSBS dataset, was the instances of cybersecurity breach or attack within the organization in question.

The research question that drove the study was: What is the relationship between ISPC perceptions in employees, employee cyber hygiene behaviors, and prevalence of organizational security breaches? The null hypothesis (H_0) was as follows: There is no statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence. The alternative hypothesis (H_1) was as follows: There is a statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of

organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence.

In this section, I detail the rationale and design for the procedures of this study. First is an overview of the purpose and properties of qualitative, quantitative, and mixed methodologies, along with examples of how each category of research method has been used in cybersecurity and insider threat literature. I discuss the appropriateness of both qualitative and mixed methodologies to this study, as well as justify my choice of the qualitative methodology to address the research problem. Then is a discussion of the purpose and properties of various quantitative research designs, along with a review of how various designs have been used in cybersecurity and insider threat literature. I discuss the appropriateness of each, while justifying my choice of the correlational secondary data analysis research design and providing an overview how I executed the research using the CSBS 2021 dataset. Then is a detailed summary of the population and sampling that characterized the 2021 CSBS, which is followed by a discussion of the ethical implications and provisions for this study. I review the data collection, data analysis, and study validity of the CSBS dataset, closing with a complete summary.

Method

The qualitative methodology was the first category of research method I considered for this study. Qualitative methodologies are broadly defined as a category of research designs characterized by the collection and/or use of data that cannot be measured or quantified mathematically (Cassell et al., 2018; Denzin & Lincoln, 2018; Ghauri et al., 2020). The types of data collected vary, ranging from interviews,

observations, artifacts (such as documents, journals, or videos), questionnaires, focus groups, and recordings (Gronmo, 2020). Due to the nature of the data that is analyzed in these methods, qualitative research focuses on categorizing, interpreting, and constructing meaning from subjective accounts regarding the topics being investigated (Cassell et al., 2018; Erickson, 2018). These modalities of data, along with the type of analysis required to process the data, are what ultimately make up the qualitative aspect of qualitative methodologies.

Qualitative methodologies are used for a variety of purposes. They are most often used for initial, exploratory, and explanatory studies in which researchers aim to discover or elucidate the factors mediate the topic or research question of interest (Hennink et al., 2020). These methods are also used when a theory regarding an emerging topic must be constructed (Holton, 2018; Leedy & Ormrod, 2021). Quite often in qualitative studies, the variables or factors being examined have not yet been clearly defined or operationalized as is required in quantitative methodologies (Ghauri et al., 2019; Gronmo, 2019). Although qualitative methodologies might use subjective data, they are by no means less valuable or less methodologically rigorous than quantitative methods (Cassell et al., 2018; Leedy & Ormrod, 2021). To illustrate, the primary goal of more rigorous systems of inductive (e.g., grounded theory methodology) or deductive (e.g., phenomenology) coding of qualitative data is to develop theories, themes, categories, codes, descriptions, and conclusions that can thereafter be quantified and validated in future research (Brinkmann, 2018; Holton, 2018). Without the description, categorizing, and operationalization that is performed in qualitative studies, it would not be possible to

conduct quantitative research in complex topics (Cassell et al., 2018; Leedy & Ormrod, 2021; Sallis et al., 2021). Qualitative methodologies remain indispensable for nonstatistical, meaning-based investigations into a wide variety of topics.

Qualitative methodologies are common in cybersecurity, cyber hygiene, and ISPC research and are used for a number of different purposes. The widespread use of qualitative research can be attributed to the fact that many researchers and practitioners are yet attempting to understand the complexities inherent in the intersections of insider threat and organizational cybersecurity (Hina et al., 2019; Posey et al., 2014). Cybersecurity researchers such as Choi et al. (2018) choose to use qualitative methodologies to gather data on the perspectives of organizational insiders, which are then coded into more general themes that provide categorical structures that can be tested in future research efforts. Researchers such as Posey et al. use qualitative methodologies to elucidate the differences between conventional personnel and IT professionals, for the purpose of determining the most efficacious factors to be targeted to maximize organizational ISPC. Researchers such as Aceto et al. (2019), in contrast, use case studies and other research designs not involving human participants to conduct detailed analyses on specific sectors of the IT field. Finally, private research organizations such as the Ponemon Institute (2018) and the research divisions of private firms such as PricewaterhouseCoopers (2018, 2021) use qualitative methods annually to collect data that cannot be easily quantified. Qualitative methodologies have been successfully used to establish exploratory and explanatory understandings of many topics in cybersecurity research.

I determined that qualitative methodologies were not appropriate for this study due to the preponderance of extant studies from which to draw operationalized variables. The variables related to the research problem have already been defined and operationalized in prior research. As illustrated in the above literature review, topics directly related to perceived importance of cybersecurity, senior management involvement, organizational ISPC, knowledge of cybersecurity, and cybersecurity breaches feature prior qualitative research that allows for follow-up research via methodologically rigorous quantitative research. If such research was not yet extant, it would not have been possible for the CSBS to have been conducted over half a decade. Considering the extant body of research on the topics of interest regarding the present study, it would not be efficient to conduct yet another qualitative study for the factors in question. Finally, the variables that will be investigated have already been defined and operationalized by the CSBS 2021 dataset, thereby precluding the use of a qualitative methodology.

Quantitative methodology was the second category of research I considered for this study. In direct contrast to qualitative methods, quantitative methodologies are broadly defined as a category of research designs characterized by the collection of data that can be quantified in mathematical terms (Leedy & Ormrod, 2021; Sallis et al., 2021). Data in quantitative studies can be collected through measurement, observation, surveys, questionnaires, interviews with quantitative components, document collection, artifact collection, or the use of existing quantitative datasets (Ghauri et al., 2020; Stockemer, 2019). Data collection in quantitative studies may also involve complex techniques such

as the use of control groups, blinds, and deception (Ghauri et al., 2020). These techniques are employed to attain certain methodological goals such as increased rigor, determining causality, or accommodating specific research goals (Ghauri et al., 2020). Quantifiable data and the many ways quantitative data can be collected are what characterize all quantitative methodologies.

Quantitative methods can vary greatly in complexity depending on the data to be collected and the purpose of the study. Simple quantitative studies involve the collection and analysis of data that can be easily organized, contextualized, and understood using descriptive statistics such as measures of central tendency, percentiles, percentages, distribution, and frequency (Leedy & Ormrod, 2021; Rees, 2019; Stockemer, 2019). More complex quantitative methodologies might involve determining quantifiable relationships between variables through the collection and analysis numerical data, using more sophisticated inferential statistics, or a combination of inferential and descriptive statistics (Ghauri et al., 2020; Sallis et al., 2021). In summary, quantitative methodologies are ideal in studies involving statistical analysis of variables that are measured numerically.

According to my review of literature, most cybersecurity research from 2017 to 2022 involved quantitative methodologies, though in varying degrees of methodological complexity. The popularity of quantitative methods is because much of the exploratory work has already been performed through prior qualitative inquiries, large scale datasets such as the CSBS have become more widely available, and the IT field has an overall bias toward statistical analysis (Angraini et al., 2019; Koohang et al., 2021; Moody et al.,

2018). At the lowest degree of statistical complexity, such as the Angraini et al. study, are studies that analyze unsophisticated, information-rich survey data with descriptive statistics to present and contextualize the quantitative characteristics of the topic in question. The majority of studies congregate around the middle point of complexity, in which correlational or causal relationships between a handful of variables are confirmed or denied using inferential statistics, while being contextualized by descriptive statistics (Daud et al., 2018; Dawson et al., 2018; Jaeger et al., 2020; Ormond et al., 2019). At the highest degrees of complexity are ambitious and large-scale studies, such as those conducted by Moody et al. and Koohang et al., in which researchers employ multiple different modes of inferential statistics in multiple iterative steps in order to engage in a complex research purpose, such as creating or confirming a unified theoretical framework of ISPC. As the most widely used research approach, it is clear that quantitative methods have been fruitful in providing insight into the issues of insider threat and ISPC in the field of cybersecurity.

For this study, I chose to use a quantitative methodology to analyze the secondary dataset. The quantitative approach was most appropriate primarily because the chosen secondary dataset, the 2021 CSBS, featured a large quantitative dataset on information security policy compliance and organizational cybersecurity which had not been fully investigated. Furthermore, the CSBS contained high-quality quantitative data on factors that were directly relevant to the research problems that underly this study. The participant pool through which Ipsos MORI collected the data, consisting of senior cybersecurity management elements of organizations of all sizes, was likewise directly

applicable to this study (Ipsos MORI, 2021a; 2021b; 2021c). The availability of such a rigorous and pertinent set of unused data collected from a relevant representative population was an excellent opportunity to engage in quantitative research.

The quantitative approach was also most appropriate because the characteristics of this study were highly conducive to this methodology. The primary weaknesses of quantitative data analysis include the need for a valid theoretical framework by which hypotheses can be tested, the need for variables that can be measured quantitatively, and the need for a representative sample to ensure the generalizability of the results (Sallis et al., 2021). Yet the use of protection motivation theory and a methodologically sound archival dataset directly addressed these weaknesses while retaining this study's overall rigor. Although there was no guarantee that any statistically significant relationships between variables would be found, that is true of any quantitative study and was not considered a weakness (Leedy & Ormrod, 2021). In summary, quantitative methodology was ideal for analyzing the 2021 CSBS dataset using PMT as the primary theoretical framework.

Mixed methods were the third category of research methodology that I considered for this study. Mixed methods are broadly defined as a category of research design characterized by an integration of both qualitative and quantitative data collection in various different configurations depending upon the nature of inquiry (Molina-Azorin, 2018). The selection of a specific configuration in a mixed methods study is contingent upon the nature of the topic being investigated, the amount of research currently available in the topic in question, the nature of the data being collected, and the purpose of the

study (Gronmo, 2019; Leedy & Ormrod, 2019). A mixed methods configuration can be as simple as combining related qualitative and quantitative studies into a single simultaneous investigation or as complex as integrating and iterating multiple different qualitative and quantitative data collection/analysis modalities (Cuervo-Cazurra et al., 2020; Gronmo, 2019). As such, mixed methods studies can encompass a wide range of complexity that will be highly specific to each study.

Mixed methodologies have four major advantages over the sole use of either qualitative or quantitative methods designs. First, mixed methods allow for researchers to collect and analyze both qualitative information and quantitative data to rigorously integrate these disparate types of data in a meaningful way (Leedy & Ormrod, 2021; Lo et al., 2020). Second, mixed methods allow researchers to operationalize, validate, test, investigate, and elucidate various factors, concepts, or instruments in a single study which would otherwise require two or more separate quantitative and qualitative studies, thereby saving both time and resources (Lo et al., 2020). This can be important in cases in which the researchers are aiming to quantify factors that have not yet been operationalized or if researchers want to use a qualitative inquiry to determine the validity of an existing quantitative instrument (Hina et al., 2019). Third, mixed methods allow for the investigation of complex research questions impossible to answer with even complex qualitative or quantitative research designs, such as if researchers require integrating multiple factors that have not been operationalized uniformly into a single framework (Levine, 2016; Lo et al., 2020). Fourth, mixed methods can give researchers flexibility beyond commonly accepted research designs, allowing them to pursue

unconventional research purposes such as theory generation (Gronmo, 2020; Leedy & Ormrod, 2021). Though mixed methods are not as widely used as qualitative or quantitative methods, these advantages strongly justify the use of this more complex category of research designs for specific ends.

Although uncommon, the use of mixed methods in cybersecurity, ISPC, and insider threat research is not nonexistent. The major way in which this category of research designs has been typically used in cybersecurity and insider threat research is when researchers are interested in investigating quantifiable variables that have not yet been formally defined or operationalized in past research in order to develop an initial survey instrument. Hina et al. (2019), for example, engaged in a preliminary qualitative study in which subject matter experts were first used to construct a survey instrument designed to measure the relationship between institutional governance and ISPC, which was then quantitatively validated. Vishwanath et al. (2020) also used this approach, using an initial qualitative survey of experts to design a cyber hygiene inventory, followed by quantitative testing to refine and validate the instrument. Overall, cybersecurity researchers in the past 5 years have tended to prefer complex quantitative designs such as meta-analyses instead of mixed methodologies, though the latter are no less valid.

Despite the utility of the mixed methods approach, it was not appropriate for this study. Though the use of a secondary quantitative dataset does not preclude a mixed-methods approach, adding a qualitative element to the study would not have contributed to addressing this study's research problems nor would it have fulfilled the research purpose. The purpose of this study was to determine the relationship between four

independent variables—perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, and seeking of cybersecurity information or guidance—and the instance of cybersecurity breach or attack. Each of these variables have already been operationalized in prior literature, as was detailed in the literature review. Adding another component not necessary for addressing the research question would have only diluted the focus of this study while adding no meaningful elements.

Design

The first research design I considered for this study was the quantitative descriptive design. The purpose of the descriptive design is to quantify some well-defined property or properties of a specific subject or subjects in a given topic (Ghauri et al., 2020; Shkoler, 2019). Unlike more complex quantitative designs, descriptive designs involve describing or providing non-inferential data regarding the phenomenon or problem in question (Shkoler, 2019). This design is largely used in studies in which properties can be easily quantified, such as if the variables being investigated are easy to operationalize or have been defined in prior research (Cain et al., 2018). More complex descriptive designs can be comparative in nature, such as through collecting data from a cross-section of multiple different samples that differ along certain variables, such as age, gender, or demographic (Leedy & Ormrod, 2021; Shkoler 2019). Descriptive designs can also be longitudinal, in which descriptive data from a single sample of participants are collected over a long period of time (Leedy & Ormrod, 2021). The single common element among descriptive designs is the primary use of descriptive statistics, such as percentiles, measures of central tendency, distribution, percentages, and frequency

(Leedy & Ormrod, 2021; Rees, 2019; Shkoler, 2019; Stockemer, 2019). The utility of the descriptive design, then, is in quantifying the characteristics of phenomena in question.

Purely descriptive designs are not very common in cybersecurity literature because descriptive statistics are mostly used in conjunction with correlational or experimental designs that use inferential statistics. Although new issues and insights regarding ISPC and insider threat are continually emerging, which necessitates descriptive research to better quantify and understand organizational insiders, the vast majority of studies involve using descriptive statistics as a stepping stone toward quantitative designs involving inferential statistics (Hina & Dominic, 2017; Neigel et al., 2020; Rajab & Eydgahi, 2019; Rantao & Njenga, 2020). Cain et al.'s (2018) study was the sole exception among the reviewed literature, in which the researchers conducted a descriptive cross-sectional study to better understand the knowledge and behaviors regarding the emergent topic of cyber hygiene. Though descriptive statistics are clearly invaluable in cybersecurity research, purely descriptive designs are uncommon due to these statistics being subsumed in the pursuit of more complex qualitative or inferential research endeavors.

Descriptive designs were inappropriate for this study for three reasons. First, the variables that will be investigated have already been operationalized, precluding the need for any preliminary descriptive research. Second, the CSBS 2021 has already quantified the characteristics of the target population, again precluding the need for descriptive efforts. Finally, a descriptive study would simply be unable to address the present study's

research problem, which necessitates inferential statistics to test for relationships between variables. As such, a descriptive design was unsuitable for this study.

The correlational research design was another potential research design for this study. Often considered a type of causal research, though significant correlations do not directly imply causation, this research design involves quantitatively measuring variables then using inferential statistics to calculate the degree to which the variables are statistically associated with each other (Ghauri et al., 2020; Leedy & Ormrod, 2021; Shkoler, 2019). The key element to correlational designs is determining whether or not statistically significant associations exist between variables of interest (Lo et al., 2020; Shkoler, 2019). Potential correlations are investigated for a number of reasons, such as to test hypotheses, replicate prior research, validate theoretical frameworks, determine the nature of certain phenomena, clarify the relationships between the factors that comprise a phenomenon, or validate theoretical frameworks (Ghauri et al., 2020; Leedy & Ormrod, 2021; Shkoler, 2019). There are a wide variety of correlational statistics available for use, which are selected according to the scales of the variables being measured in a given study (Leedy & Ormrod, 2021). As a large number of quantitative research involves investigating relationships between variables of interest, it is clear why correlational studies remain among the most popular research designs.

The correlational design is commonly used in cybersecurity research due to the utility of comparing variables of interest. Within these correlational studies, researchers tend to focus on exploring if and/or how certain factors mediate ISPC or other related independent variables (Addae et al., 2019; Jaeger et al., 2020; Wiafe et al., 2020). Such

studies (a) use one or more existing theoretical frameworks with which to operationalize the variables, (b) either create their own survey instruments or re-validate an existing instrument, (c) and measure the variables using the instrument through participant recruitment (Jaeger et al., 2020; Rantao & Njenga, 2020). They then use inferential statistics to determine relationships between the variables for various purposes, such as testing the validity of some factors against others, determining the effect size of certain mediating variables, or to test proposed relationships (Addae et al., 2019; Rantao & Njenga, 2020; Wiafe et al., 2020). Some researchers, such as Koohang et al. (2021) or Alshare et al. (2018), choose to engage in factor analyses and other statistical methods before using correlational statistics. These preliminary statistical tools were designed to refine and validate theories or surveys that were newly constructed in prior research so that correlations could be tested with a greater degree of confidence (Alshare et al., 2018; Koohang et al., 2021). Despite whatever procedural complexities that may be involved, most quantitative studies involve the use of correlational designs largely due to the need to determine relationships between factors in a given cybersecurity phenomenon.

The correlational design was the most appropriate research design for this study primarily due to the nature of the research problem. The key objective of the present study was to determine the association that exists between a number of independent variables (i.e., perceived importance of cybersecurity, senior management involvement, use of organizational ISP, and seeking information regarding cybersecurity) and organizational vulnerability to cyberattack, which necessitates a research design that allows for the statistical comparison of variables. The correlational design was also

appropriate because it has been used extensively in cybersecurity research to uncover statistically significant results between variables, such as in ISPC (Rajab & Eydgahi, 2019), cyber hygiene (Cain et al., 2018), and security breach (Vishwanath et al., 2020) research. Most importantly, the correlational design was ideal in addressing this study's research questions using the relevant variables available in the 2021 CSBS dataset. No further complexities in data collection or analysis procedures were necessary to optimally address the present study's research questions and purpose.

Experimental and quasi-experimental designs are another type of quantitative study that I considered for this study, though the complexity and specificity of purpose make them less popular than correlational designs. Experimental studies are designed to help determine causality through specific procedures designed to isolate potential changes in dependent variables in response to deliberate changes in independent variables, all of which are quantitatively measured and statistically calculated (Ghauri et al., 2020). In an experiment, the researcher manipulates and measures the conditions of the predictor variable (also called the experimental or independent variables) and measures the outcome variable (also called the dependent variable; Ghauri et al., 2020; Shkoler, 2019). Among the manipulated variables, there will always be at least one control group that receives a placebo or no intervention, whose outcomes will also be measured to serve as a baseline for analysis (Leedy & Ormrod, 2021). In true experimental designs, the experimental and control conditions are distributed randomly and as many confounding variables as possible are held as constantly as possible. In quasi-experimental designs, the distribution of experimental and control conditions is not

random, and the experimenters cannot control for a maximum number of confounding variables (Leedy & Ormrod, 2021). There are many types of experimental and quasi-experimental designs, which are chosen according to the phenomenon being investigated, the number of experimental and control variables, the nature of the participants, the nature of the setting, the experimenter's resources, and other various constraints (Ghauri et al., 2020; Leedy & Ormrod, 2021). Regardless, these designs are indispensable when attempting to determine a degree of causality between variables of interest.

As with the descriptive design, neither experimental or quasi-experimental designs were common in cybersecurity research on insider threat, cyber hygiene, and ISPC. The overwhelming majority of quantitative studies were variations of the correlational design. It might be postulated that this is the case because the factors related to insider threat, cyber hygiene, and ISPC manifest in organizational settings which are not conducive to experimental or quasi-experimental controls. The Ormond et al. (2018) study was the only relevant study conducted in the past 5 years with an experimental design. In this study, participants in the experimental group were assigned decreased levels of reward to increase frustration, to determine the effect of frustration on ISPC. The researchers found that increased frustration led to negative affective flow and increased violations of ISPs (Ormond et al., 2018). Although experimental and quasi-experimental designs are rare in this topic, they can be useful if applied properly.

I did not choose to use either an experimental or quasi-experimental design because these designs are simply not within the scope of this study's research question or purpose. Experimental or quasi-experimental designs were not appropriate because this

study aimed to identify a descriptive model using correlational statistics, rather than a causal model. Introducing a control element, even using a quasi-experimental design due to the use of a secondary dataset, would not have introduced any additional insight for addressing the research question. But more importantly, introducing a control element simply would not have been possible considering the use of secondary data, as well as the scope of the variables that were investigated in the present study.

Population and Sampling

Population

The 2021 CSBS defined the broad scope for this study while this study's research purpose and questions further narrowed the population. The population of the CSBS consisted of non-profit organizations and private companies, which included registered businesses, registered charity organizations, and educational institutions in the United Kingdom (Ipsos MORI, 2021a; 2021b; 2021c). The survey population was meant to represent enterprises across all sectors throughout the UK that have information technology implementations (Ipsos MORI, 2021a; 2021b; 2021c). Leadership with the greatest seniority and responsibility for cybersecurity within all participating organizations were sought after and surveyed. For multinational organizations, individuals with the greatest seniority and responsibility for cybersecurity in the UK arm of the organization were sought after and surveyed. If a multinational organization had a presence in Great Britain and Northern Ireland, both branches were considered separate organizations (Ipsos MORI, 2021a; 2021b; 2021c). It is important to note that, though the total population of the 2021 CSBS was reviewed in this discussion, the scope of the

present study included only one of the three categories of organizations: registered businesses.

In accordance with this broad scope, the total usable population was considerable in number. The original population included 89,372 businesses that were part of the UK's Inter-Departmental Business Register (IDBR), 199,742 registered charities, and 25,283 public and private educational institutions throughout the UK form the primary school to university levels (Ipsos MORI, 2021a; 2021b; 2021c). Once businesses not meeting IT and size criteria were eliminated and after telephone tracing and cleaning were completed, the entire population of organizations that were eligible and useable for the CSBS totaled 29,074 IDBR businesses, 169,476 charities, and 18,307 educational institutions. Businesses were further subcategorized according to number of staff, from micro (1-9 on payroll), small (10-49 on payroll), medium (50-249 on payroll), to large (250+ on payroll). The original population included 314,397 organizations while the eligible and usable population included 216,815 organizations (Ipsos MORI, 2021a; 2021b; 2021c). It is from the usable population that the sample was ultimately drawn.

Sampling

The 2021 CSBS involved a small number of inclusion and exclusion criteria, some of which were specific to the type of organization in question. Only organizations with more than one individual on the payroll were included (Ipsos MORI, 2021a; 2021b; 2021c). Single-person businesses, also called sole proprietorships, were excluded. Only organizations with IT implementations integral to their overall operations with central cybersecurity concerns were included. Within the population of businesses, public-sector

businesses were excluded as they are subject to adhere to government-mandated standards for cybersecurity. Businesses in the fishing, forestry, and agriculture sectors were excluded due to lack of cybersecurity relevance and challenges in gaining authorization (Ipsos MORI, 2021a; 2021b; 2021c). As can be inferred these criteria were designed to facilitate data collection and optimize the relevance of the sample specifically to cybersecurity issues.

The 2021 CSBS researchers fully justified the survey's sampling procedures. A primary goal of the CSBS is to get as close to random sampling of the total population as possible (Ipsos MORI, 2021a; 2021b; 2021c). The total sample of completed quantitative interviews included in the CSBS were 1,419 businesses, 487 charity organizations, and 378 educational institutions, considered more than enough as representative samples (Ipsos MORI, 2021a; 2021b; 2021c). Note again that the scope of the present study only included the 1,419 businesses.

Certain subgroups within the organization types were weighted to ensure representation. For this purpose, the 2021 CSBS did not feature purely simple random sampling but also involved stratified random sampling. Stratified random sampling in businesses and charities was necessary to ensure that outliers were adequately represented in the dataset (Ipsos MORI, 2021a; 2021b; 2021c). Sampling for businesses was stratified proportionally according to region but, as micro-sized businesses greatly outnumbered the other three sizes, was stratified disproportionately according to size (Ipsos MORI, 2021a; 2021b; 2021c). Small, medium, and large business were boosted so that they would not be excluded. Certain sectors were also boosted to mirror samples for

the 2020 CSBS. While Scotland, Wales, and England had comprehensive databases of charity organizations, Northern Ireland did not yet feature a comprehensive database, so the 2021 CSBS does not feature a truly random sample for that region, though this was not considered a major concern. Sampling for charities was stratified proportionally according to region but, as low-income charities greatly outnumbered high-income charities, was stratified disproportionately according to income. High-income charities were boosted so that they would not be excluded in representation. Simple random sampling was used for the population of educational institutions (Ipsos MORI, 2021a; 2021b; 2021c). The 2021 CSBS researchers engaged in highly valid probabilistic sampling methods to either attain a representative sample, representative stratified sample, or, in the case of underrepresented organizations, an overrepresented sample.

Ethics

Data analysis commenced after IRB approval was attained. I completed CITI Training required for doctoral student researchers enrolled in Walden University, with a completion date of February 12, 2022. IRB approval was confirmed on July 6, 2022. The Walden University IRB approval number for this study was 07-06-22-1020148. As the 2021 CSBS dataset was available for public use, there was no need to gain permission to use the data. However, permission was needed to create an account with the UK Data Archive to access the data. As approval was necessary for academics residing outside of the United Kingdom, I applied for a username using my Walden University student credentials and was approved for access. According to the published reports, the data has been anonymized for public use (Ipsos MORI, 2021a; 2021b; 2021c) so there was no

need to further anonymize the data to protect the identities of the respondents and their businesses. As I cleaned and formatted the data specifically for this study, I kept my modified version of the dataset in a password-protected computer, accessible only to me, throughout the study. In case researchers ask for access to this data, I will continue to keep my data within a password-protected USB drive in a locked location accessible only to me. I will delete this data five years after this study's publication date. Upon completion of the five years of storage, I will use secure software to sanitize the USB drive so that the data cannot be retrieved.

Data Collection Instrument

This study used the 2021 CSBS as the source of secondary quantitative data. The 2021 CSBS involved the use of a proprietary quantitative survey questionnaire that was adapted from the survey of the previous year (Ipsos MORI, 2021c). Instrument-creation for the CSBS study has been an annually iterative process from 2016 onward, being revised through pilot study during each wave. The 2021 CSBS questionnaire featured survey items were omitted from or added to the 2020 CSBS questionnaire to increase the efficacy of items, the efficiency of the survey process, and to introduce key cybersecurity factors. The 2021 CSBS survey contained a total of 28 highly structured, multipart items (from a total of 78 proposed items over the 2016 through 2021 years) that that were scripted specifically to optimize the gathering of quantitative data through verbal telephone surveying (Ipsos MORI, 2021c).

The purpose of the 2021 CSBS was to gain information on key cybersecurity factors in organizations across the UK. The specific target population included those in

senior-most information technology or cybersecurity positions within the organizations in question. For the 2,284 total participants, the average length to administer the 28 total questions of each telephone survey was 20 minutes. As the survey instrument was meant to represent a scale, no scoring protocol was required or necessary.

Survey items were not always simple questions but were often composed of multi-part scripts. Many items were composed of a combination of subitems (Ipsos MORI, 2021c). The scripts for survey items involved varying how specific questions were presented depending upon the type of organization (i.e., business, charity, or education) or depending on participant responses to prior items or sub-items. Apart from consent and simple follow-up questions, the survey questionnaire consisted of scripted items across 11 different categories of inquiry. The categories included: (a) business profile, (b) perceived importance and preparedness, (c) spending, (d) information sources, (e) policies and procedures, (f) business standards, (g) supplier standards, (h) cloud computing, (i) breaches or attacks, (j) most disruptive breach or attack, and (k) GDPR. All categories except the first pertain directly to the topic of cybersecurity (Ipsos MORI, 2021c). With these categories, the survey encompasses all the primary issues relevant to organizational cybersecurity from the senior information technology perspective.

Ipsos MORI did not provide usable psychometric statistics of the survey instrument, though some validity was addressed in the 2021 CSBS documentation. Psychometric data could not have been reported because CSBS questionnaires are not psychometric in nature but were designed to gather quantitative and qualitative descriptive data representative of a large population of organizations. The internal

consistency reliability measurements, the degree to which items are consistent in their measurement (Hackett, 2019; Stockemer, 2019), of the survey instrument were not provided. The lone reliability measure provided was margins of error, which is not applicable to the present study because it is based on weighted sampling and percentages (Ipsos MORI, 2021b). The content validity, the degree to which an instrument's items are judged to measure the target concepts (Hackett, 2019), of the CSBS is confirmed annually with a group of government, industry, and academic cybersecurity stakeholders (Ipsos MORI, 2021c). Construct validity, a statistical measurement of whether the instrument's items adequately measure the target concepts (Stockemer, 2019), was not computed for the 2021 CSBS (Ipsos MORI, 2021c). Criterion-related validity, which involves the degree to which the results of an instrument are related to target outcomes (Hackett, 2019), was not investigated in the 2021 CSBS as the survey was descriptive in nature with no correlational statistics conducted (Ipsos MORI, 2021b; 2021c). In summary, as the 2021 CSBS was meant to take descriptive measurements of organizations, this lack of psychometric properties was not considered problematic for this study.

Data Collection Technique

This study used secondary data in the form of the public 2021 CSBS dataset. The secondary data analysis is a data collection technique that is highly appropriate in certain situations. Also called the ex post facto (i.e., *after the fact*) or archival research, secondary data analysis refers to studies in which a researcher collects secondary (i.e., archival) data to perform quantitative data analysis to determine statistical relationships

between variables that have already been measured (Leedy & Ormrod, 2021). Secondary data sources can include websites, organizational records, administrative data, government reports, data accessed from authors of specific journal articles, reports from private organizations, historical archives, public statistics, or from many other archival sources (Ghauri et al., 2020; Shkoler, 2019). In practice, the secondary data analysis is typically used because a source of quantitative data is available that has not been used for a specific purpose and that applies to a research problem (Ghauri et al., 2020). Archival research is also popular if a researcher does not have the time or resources to collect quantitative data in a conventional manner (Delios, 2020; Lo et al., 2020). This design is ideal for when relatively pristine datasets are available for use.

The secondary data analysis differs from other quantitative designs only in that the researchers are not manually collecting data themselves. Instead, specific variables that pertain to the research problem of a study are first selected from an existing secondary dataset that the researcher finds in archival form and gains permission to use (Delios, 2020; Sallis et al., 2021; Shkoler, 2019). The researcher then computes inferential statistics from these variables to determine whether significant statistical relationships exist between them, thereby testing the study's hypotheses (Gronmo, 2020; Leedy & Ormrod, 2021). Such studies are highly efficient and effective when performed on existing large-scale surveys, such as those government agencies conduct annually, or if the researcher is able to gain access to organizational data (Lo et al., 2020). The primary weakness of the ex post facto design is the inability to specify the minutiae of the variables and the inability to audit the data-gather process, though this can be largely

mediated through the use of a relevant and high-quality dataset (Gronmo, 2020). Another potential weakness is present if the dataset is a popular source of data for researchers (Lo et al., 2020). The strengths of using secondary data analysis, however, include the free availability of official data, the ability to take advantage of large methodologically rigorous data collection procedures, and the ability to conduct a quantitative study on a representative sample without a large budget (Leedy & Ormrod, 2021).

Archival studies, though common across many academic disciplines, are rare in cybersecurity research on cyber hygiene, ISPC, and insider threat. This is likely because, save for the relatively new CSBS, large-scale datasets are not yet widely available in these topics. Though private organizations that conduct large-scale surveys such as the Ponemon Institute (2018) and PricewaterhouseCoopers (2018; 2021) do publish regular public reports containing the results of statistical analyses, these firms do not release their datasets to researchers. The meta-analysis conducted by Cram et al. (2019) was technically a secondary data analysis, though it involved collecting data from multiple secondary sources (Shkoler, 2019). Despite the relative rarity in the field of cybersecurity, the secondary data analysis remains a highly useful and valid research design.

The secondary data analysis design, in conjunction with a correlational design, was the most appropriate data collection technique, largely due the CSBS 2021 dataset. First and foremost, the ready availability of the largely unused CSBS 2021 data was an opportunity to engage in a study with a greater potential for positive impact using a large-scale dataset compared to any study in which I alone would have had to engage in

quantitative data collection. The many different factors that were investigated in the 2021 CSBS also offset the primary weakness of secondary data analysis, as the dataset contained all of the variables necessary to address the research problem of the present study. Due to the richness of the 2021 CSBS and a lack of studies using the dataset, this data also addressed the second potential weakness of ex post facto designs. Finally, because secondary data analysis is simply a mode of data collection, it was highly compatible with a correlational design (see Ghauri et al., 2020). For these reasons, a secondary data analysis using the 2021 CSBS public data was considered ideal for addressing this study's research problem.

Data Analysis

I cleaned the data, constructed the variables, and used correlational analysis on the secondary quantitative data found in the 2021 CSBS using the SPSS 28 statistical analysis software package (see *Section 3* for specific details of the entire process). Available data was quantitative and qualitative in nature, with the latter consisting of all four scales of measurement—including nominal, ordinal, interval, and ratio (Ipsos MORI, 2021a; 2021b; 2021c). Upon data cleaning, I constructed the dependent variable (DV) and independent variables (IV). Upon considering my options for applying the study's DV and IVs to the 2021 CSBS, I constructed a single DV and four IVs from the survey items. The DV was in the ratio scale, three IVs were ratio, and one IV was nominal. As the DV and most of the IVs were continuous, the Pearson product-moment correlation coefficient, also called Pearson's *r*, was used to determine the association of individual

IVs to individual DVs. Due to the examination of multiple IVs, multiple linear regression was also used to determine the association of the multiple IVs to each individual DV.

Study Validity

As this study involves a nonexperimental research design, threats to internal validity were not applicable. However, threats to statistical conclusion validity remained concerns as the study involved correlational research. These threats included Type I errors and Type II errors. Type I errors are when data analysis leads to accepting a statistically nonsignificant result as significant, causing an inaccurate rejection of the null hypothesis (Hackett, 2019). Type II errors are when data analysis leads to rejecting a statistically significant result as nonsignificant, causing an inaccurate acceptance of the null hypothesis (Hackett, 2019). The 2021 CSBS researchers did not compute standard psychometric reliability measures because the survey itself was not designed to be a scale but a means of measuring descriptive factors related to cybersecurity breaches. However, the researchers deemed that the margins of error found in the results were within the bounds of satisfactory instrument reliability (Ipsos MORI, 2021b). Although inadequate sample size could lead to threats to conclusion validity, this was not a concern for the 2021 CSBS (Ipsos MORI, 2021c). However, a major assumption that could be a threat to internal validity is that participants reported accurate information (Ipsos MORI, 2021b; 2021c). Although the threat of this assumption is mitigated by interviewing only those at the senior-most organizational positions pertaining to information technology or cybersecurity (Ipsos MORI, 2021b; 2021c), the danger of error yet remained throughout the study.

Summary

The purpose of this quantitative correlational study was to investigate the relationship between ISPC, cyber hygiene, and organizational vulnerability to cyberattack. By using the 2021 CSBS dataset, I conducted a unique secondary data analysis with PMT as the primary theoretical framework. The use of this dataset allowed for the minimizing of typical weaknesses of the qualitative methodology while taking advantage of: (a) its methodological rigor, (b) the pre-anonymized data, and (c) a large sample size. Data cleaning, variable construction, and data analysis commenced upon IRB approval. Variables were nearly all of ratio scale, with the exception of a single nominal IV. Due to the continuous nature of most variables and the use of multiple predictors, the Pearson's *r* correlation and multiple linear regression were the primary forms of data analysis. In all, this study has the potential to contribute greater insight into the role insiders play in mediating organizational cybersecurity.

Section 3: Application to Professional Practice and Implications for Change

Executive Summary

The purpose of this study was to use a quantitative correlational design to determine whether seeking of information or guidance on cybersecurity, senior management involvement, use of organizational ISPC, and perceived importance of cybersecurity were predictive of instances of cybersecurity breach or attack. Upon reviewing the 2021 CSBS dataset and comparing the available items and responses with the necessary dependent and independent variables, it was determined that data preparation would involve variable assignment, variable construction, and data cleaning. Attack Rate and Perceived Importance were assigned single items from within the dataset. Seeking Guidance, Management Involvement, and Organizational ISPC were constructed by combining multiple dataset items and/or questions. Data cleaning involved preparing the relevant items for data analysis by reversing scales, quantifying certain responses, and summing items to be used for variable construction. Pre-analysis evaluation revealed that the cleaned dataset was not yet ready for analysis as it violated the assumptions of outliers and normality necessary for multiple linear regression analysis. After eliminating outliers by applying Tukey's method twice, testing the dataset yielded no serious violations of assumptions. The final dataset numbered $N = 469$ total participants. Calculation of the Pearson's r yielded no significant correlations between the dependent variable and independent variables.

Multiple linear regression analysis was used to determine whether seeking of information or guidance on cybersecurity, senior management involvement, use of

organizational ISPC, and perceived importance of cybersecurity were predictive of instances of cybersecurity breach or attack. The multiple regression model was not predictive of instances of cybersecurity breach or attack, so the null hypothesis of this study was accepted. A single significant predictor was found in the multiple linear regression analysis: perceived importance of cybersecurity. The association was such that a lower degree of perceived importance was predictive for higher annual instances of cybersecurity attack or breach.

The results of this study have numerous implications for professional practice, social change, and research. For the professional practice, it is recommended to take focused measures to promote a positive and urgent perception of cybersecurity throughout internet connected organizations, as the results indicate that greater perceived importance is associated with decreased cybersecurity breaches. Those in leadership positions are also recommended to establish a communication-focused framework of research throughout their organizations to gather both internal and external data on potential vulnerabilities. The major social change implication is confirmation that internal and external prioritization of cybersecurity throughout organizations will help preserve the human right to privacy and protect the private financial information of consumers. Recommendations for research include improving on the items collected in the 2021 CSBS dataset and conducting methodologically rigorous investigations of the antecedents of cybersecurity attacks and breaches.

The two groups of stakeholders for this study are leaders and personnel with a stake in organizational cybersecurity and groups who are interested in researching,

developing, or offering ex ante implementations for mitigating cybersecurity attacks and breaches. The overall strategy for disseminating the study will involve two stages in which the research is placed in broadly accessible platforms and two stages in which the research is distributed in highly specific professional and scholarly communities. This will involve adapting this study into a publication intended for the laity, media posts for professional networks, a series of scholarly articles, a series of professional articles, and a several different presentations.

Presentation of Qualitative Data Analysis

In this subheading, I have detailed the preliminary elements of data analysis including, in rough order, data review, variable assignment, data cleaning, and variable construction. I have discussed the elements related directly to assumption testing and data analysis in the following subheading. The preliminary elements of data analysis were completed in SPSS 28, though notes were taken in Excel or Word. Data review involved examining the dataset to prepare for variable construction and data cleaning. Variable assignment involved determining which survey items matched with the appropriate variable. Variable construction, conducted for three variables, involved combining multiple items into a scale that represents a single variable. Data cleaning involved preparing the items the comprise the variables for data analysis. Quantitative analysis involved computing the Pearson's *r* and conducting multiple regression analysis on the cleaned data.

Upon receiving IRB approval, I reviewed the actual dataset to determine which 2021 CSBS items would be relevant to address the research problem, purpose, and

question. I used the 2021 CSBS "Statistical Release" and the 2021 CSBS "Technical Annex" (Ipsos MORI, 2021b; 2021c) to gain an understanding of the dataset for determining the dependent variables (DV) and independent variables (IV). The dataset was far more complex than the "Statistical Release" or the "Technical Annex" indicated.

Upon reviewing the actual dataset, I determined that the data analysis process would not only involve data cleaning and analysis but would also involve variable construction. The survey items were not as simple as the Statistical Release or the Technical Annex indicated, such that not all variables could be assigned a single variable. Only for the DV and a single IV, instances of cybersecurity breach and perceived importance of cybersecurity, was it possible to cleanly assign a single item each. I found, however, that it would be impossible to cleanly match up individual items in the data with the remaining three IVs. For the remaining three IVs—seeking information or guidance on cybersecurity, senior management involvement, and organizational ISPC—it was necessary to construct each according to the multiple survey items that were relevant to the respective variable.

Variable construction was necessary for the three IVs for two reasons. First, some survey items were single questions with multiple possible responses that were represented as separate items within the dataset. For example, one survey item had 63 separate possible responses, each of which were listed as an individual item in the dataset. To properly integrate these types of survey items into a quantifiable variable, it was necessary to first consolidate each of the relevant responses into a single item. Some variables were best represented by combining multiple survey items into a composite

item. In such cases, each relevant item was modified to enable the summing all to create a ratio scale representing the IV in question.

Variable assignment and data cleaning for the DV, "Instances of Cybersecurity Attack or Breach" (referred hereafter as "Attack Rate"), was conducted after the initial review. The dataset item assigned to the DV was "freq", which represented Question 54: "Approximately, how often in the last 12 months did you experience any of the cyber security breaches or attacks you mentioned?" The data for this variable was cleaned because the responses were not optimized for analysis in the dataset. The eight possible responses included "refused", "don't know", "once only", "more than once but less than once a month", "roughly once a month", "roughly once a week", "roughly once a day", and "several times a day". Two responses, refused and don't know, were excluded from the study due to being incompatible with quantitative correlational data analysis. The participants who responded with the two excluded responses were also excluded from the study as it was not possible to conduct the study with no DV. As a result, not all 1,419 businesses surveyed in the 2021 CSBS dataset were included in the final data analysis. Data cleaning further involved adapting the nominal variables into estimated ratio scales: once only as 1, more than once but less than once a month as 6, roughly once a month as 12, roughly once a week as 52, roughly once a day as 365, and several times a day as 1460. Although it was possible to represent the choices as ordinal variables, I determined that assigning actual values in the DV would be more rigorous and representative of the actual data despite the irregular intervals.

One IV, “Perceived Importance of Cybersecurity” (referred hereafter as “Perceived Importance”), was assigned a single survey item as it was the only survey question that directly pertained to the operationalization of this variable. The name of the item was “barrier6”, which was one of eight possible responses for Question 45: “Which of the following have made it difficult for your organisation to manage any cyber security risks from your supply chain or partners?” Barrier6 represented the response “It's not a priority when working with suppliers or partners.” Among the survey items and responses, barrier6 was the only response with direct applicability to perceived importance of cybersecurity. This variable was also the only variable measured in the nominal scale, with only two potential responses. Response chosen indicated low perceived importance of cybersecurity and response not chosen indicated high perceived importance of cybersecurity. No data cleaning was necessary for this variable.

Constructing the IV “Seeking of Information or Guidance on Cybersecurity” (referred hereafter as “Seeking Guidance”) involved consolidating a single item with multiple possible and overlapping responses. The item in question involved Question 24: “In the last 12 months, from where, if anywhere, have you sought information, advice or guidance on the cyber security threats that your organisation faces?” In the dataset, there were 63 total responses to this question (i.e., the various different sources of information, advice, or guidance) listed as individual variables, ranging “info1” to “info31” and “info36” to “info67”. Constructing the variable in SPSS 28 involved summing across the multiple responses to create a scale that represented the number of sources participants

sought after for guidance. As a result, Seeking Guidance was constructed as a continuous variable in the ratio scale.

Constructing the IV “Senior Management Involvement” (referred hereafter as “Management Involvement”) involved summing seven items into a single ratio scale. A higher sum would represent a greater degree of senior management involvement. The first item was “priority”, which represented Question 9_1: “How high or low a priority is cyber security to your organisation's [directors/trustees] or senior management?”. This item was a scale, which was reverse coded such that “high priority” received the highest response score. The remaining six items were nominal with two potential responses, with “no” coded as zero and “yes” coded as one. The second item was “govtact8”, which represented a single response, “Increased senior management oversight/involvement”, for Question 24E: “What, if anything, have you changed or implemented at your organisation after seeing or hearing any government campaigns or guidance on cyber security?” The third item was “boardrep”, which represented Question 75G: “Were your organisation's [directors/ trustees/ governors] or senior management made aware of this breach, or not?” The fourth item was “info19”, which represented a single response, “Within your organisation - senior management/board”, for Question 24: “In the last 12 months, from where, if anywhere, have you sought information, advice or guidance on the cyber security threats that your organisation faces?” The fifth item was “manage1”, which represented a single response, “Board members/trustees/a governor or senior manager with responsibility for cyber security”, for Question 29: “Which of the following governance or risk management arrangements, if any, do you have in place?” The sixth

item was “reportb19”, which represented a single response, “Internal/head office/board of directors etc.”, for Question 77: “Who was this breach or attack reported to?” The seventh item was “prevent40”, which represented a single response, “Increased senior management oversight/involvement”, for Question 78: “What, if anything, have you done since this breach or attack to prevent or protect your organisation from further breaches like this?”

Constructing the IV “Organizational ISPC” involved summing nine separate questions into a single ratio scale. As most of the nine questions had multiple items to integrate, “Organizational ISPC” was a composite scale, with a higher score indicating more complete organizational ISPC measures. The first set of items was “manage1” to “manage4”, which were responses to Question 29: “Which of the following governance or risk management arrangements, if any, do you have in place?” The second set of items was “comply1” to comply5”, which were responses to Question 29A: “Which of the following standards or accreditations, if any, does your organisation adhere to?” The third set was “ident4”, “ident5”, and “ident11” to “ident14”, which were responses to Question 30: “And which of the following, if any, have you done over the last 12 months to identify cyber security risks to your organisation?” The fourth item was “audit”, which was Question 30A: “Were any cyber security audits carried out internally by staff, by an external contractor, or both?” The fifth set of items was “rules1” to “rules9” and “rules13” to “rules19”, which were responses to Question 31: “And which of the following rules or controls, if any, do you have in place?” The sixth set of items was “policy1” to ‘policy5” and “policy10” to “policy12”, which were responses to Question

32: “Which of the following aspects, if any, are covered within your cyber security-related policy, or policies?” The seventh set of items was “incidcontent1” to “incidcontent6” and “incidcontent9”, which were responses for Question 63A: “Which of the following, if any, do you do, or have in place, for when you experience a cyber security incident?” The eighth set of items was “prevent1” to “prevent24” and “prevent36” to “prevent56”, which were responses to Question 78: “What, if anything, have you done since this breach or attack to prevent or protect your organisation from further breaches like this?” The ninth set of items was “Step1” to “Step10”, which were derived from the responses pertaining to the UK’s 10 Steps to Cyber Security standards.

As the variables were assigned and constructed, I engaged in data cleaning of items that required modification to allow for quantitative analysis. Several variables—including “income”, “income2”, “sizeb”, “update”, “review”, “freq”, “restore”, “damagedirsx_bands”, “damagedirlx_bands”, “damagestaffx_bands”, “damageindx_bands”, and “cost_bands”—required the changing of measurement scales (e.g., from nominal to ordinal or from nominal to ratio), as the survey was interview-based and was not optimized for quantitative analysis. Several variables that were represented as ordinal scales (e.g., an item on a 5-point scale)—including "priority”, “covpri”, “review”, and “restore”—were also reverse coded for clarity or to ensure proper variable construction. Note that individual responses for multi-response questions were already in the dataset as either 0 or 1, such that summing responses for variable construction was relatively straightforward in SPSS. Once variable construction and data

cleaning were complete, the data was ready for assumption testing, correlational analysis, and multiple regression analysis.

Results: Presentation of the Findings

In this subheading, I discuss testing of assumptions, detail the reworking of the DV, discuss retesting of assumptions, present the descriptive results, present the inferential results, and give a concluding discussion of the results. Upon variable construction and data cleaning, the number of participants that could be included in the data analysis was $N = 639$. As is discussed below, the total number of participants was reduced to $N = 469$ to ensure that all assumptions necessary for multiple linear regression analysis were met.

Tests of Assumptions

Multicollinearity was evaluated by determining the correlation coefficients among the four predictor variables. As illustrated in Table 1, most of the bivariate correlations between the IVs were small to moderate in effect size, though they were all significant to $p < .01$. Management Involvement and Organizational ISPC were strongly correlated at $r = .511$, which potentially indicates a multicollinearity problem. According to Sallis et al. (2021), the generally accepted cutoff indicating multicollinearity problems between variables is a correlation value of 0.9. As even the strongest correlation was well under this cutoff, it was determined that there did not exist a problematic degree of multicollinearity between the IVs.

Table 1

Correlations Between Independent Variables

	Seeking Guidance	Management Involvement	Organizational ISPC	Perceived Importance
Seeking Guidance	1	.212**	.347**	.188**
Management Involvement		1	.511**	.251**
Organizational ISPC			1	.427**
Perceived Importance				1

"*" $p < .05$, "**" $p < .01$

Throughout the data cleaning and analysis processes, the assumptions of outliers, normality, linearity, homoscedasticity, and independence of residuals were continually evaluated through the examination of distribution histograms, normal probability (Q-Q) plots, and boxplots of the response (i.e., dependent) variable. The histograms of the distribution were used to visually determine whether the dependent variable exhibited a normal distribution, as normal distribution is a requisite assumption for multiple regression analysis. The normal probability plots of the dependent variable were comprised of scatterplots and best fit lines to help visually determine linearity, homoscedasticity, and independence. The more linear the scatterplot, the better the dataset satisfies these assumptions. Finally, boxplots were used to more accurately ascertain the distribution of the dependent variable and to distinguish the outliers from the rest of the data.

Upon reviewing Figures 1, 2, and 3, I determined that the dataset as it was exhibited major violations of the assumption of normality. The distribution seen in Figure 1 indicated that the distribution of the DV's values were not normal. The overall lack of cohesion among the scatterplots in Figure 2 indicated less than ideal linearity, potential

lack of homoscedasticity, and weak independence. Comparing the deviations represented by the higher-value elements seen in Figure 3 with the distribution seen in Figure 1 clearly favoring the lower-value elements clearly indicated the existence of extreme outliers in the dataset.

Figure 1

Histogram of Distribution of Dependent Variable (N = 638)

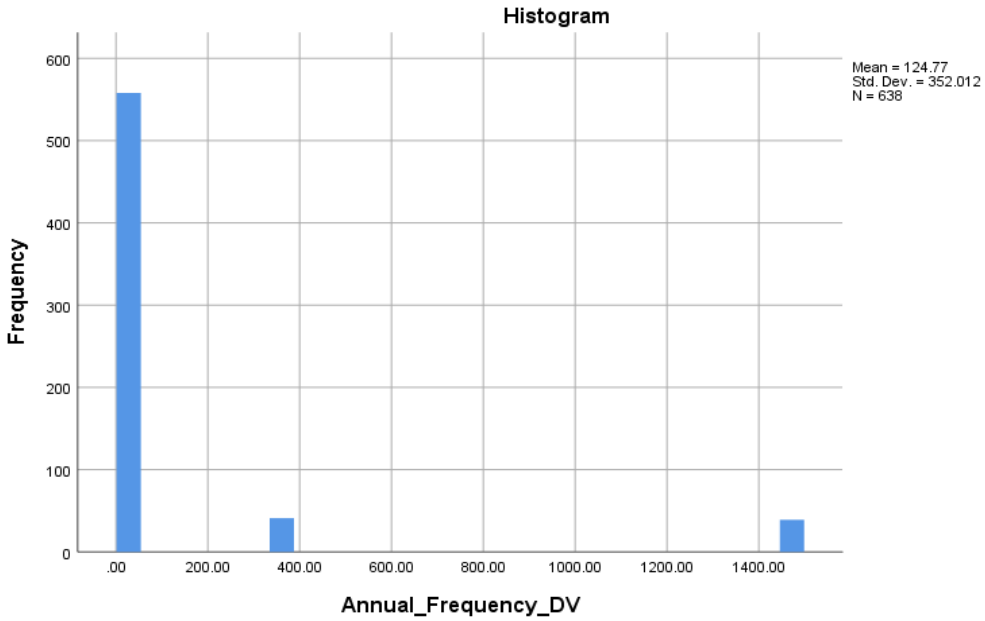


Figure 2

*Normal Probability Plot (Q-Q) of Dependent Variable (*N = *638)*

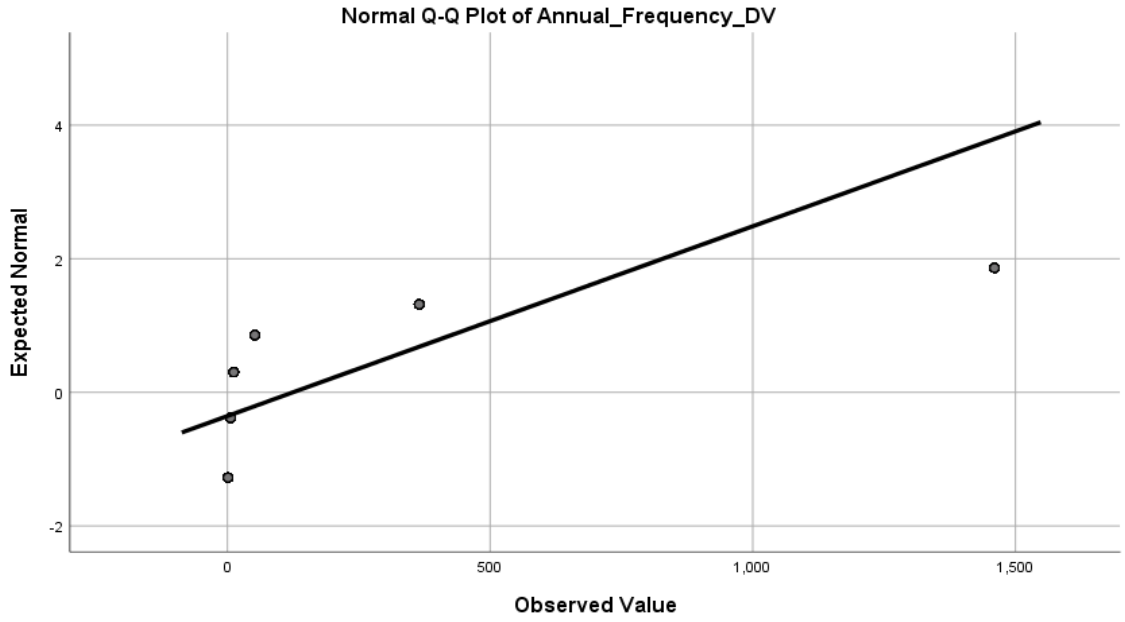
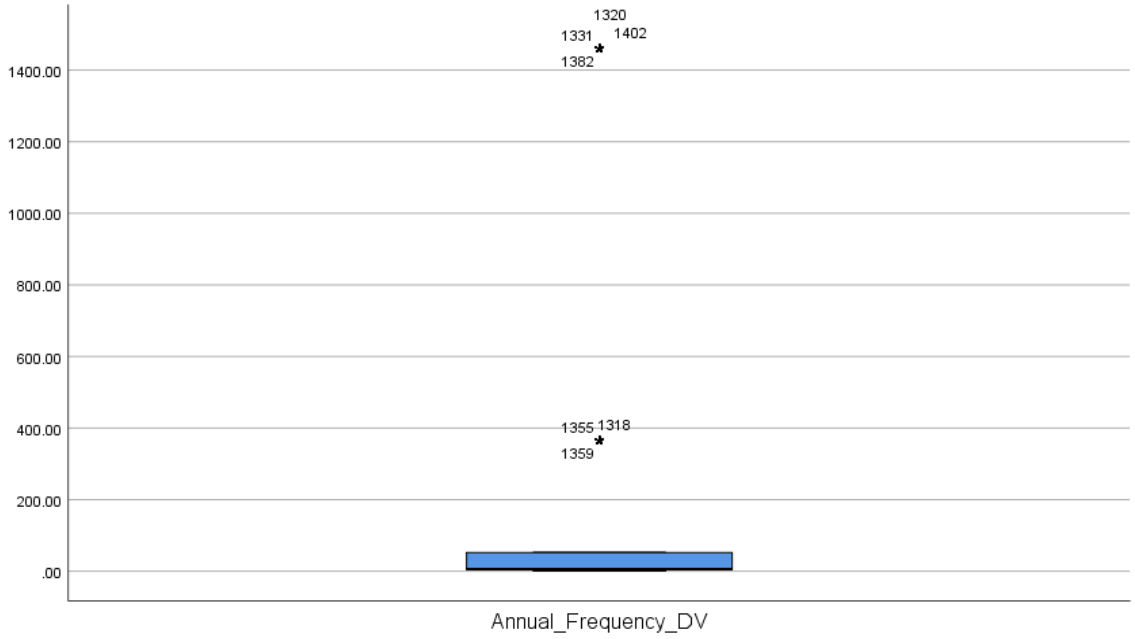


Figure 3

*Boxplot of Distribution of Dependent Variable (*N = *638)*



Note. Tukey's method was used to eliminate outliers (see pp. 92-97).

It was necessary to use a method to systematically cull outliers among the DV in an attempt to achieve a normal distribution (Sallis et al., 2021). I also postulated that culling the outliers might reduce potential violations of linearity, homoscedasticity, and independence (Sallis et al., 2021). For this dataset, I postulated that Tukey's method, also called the boxplot method, of identifying outliers would be the most efficient method of yielding a normal distribution (Kannan et al., 2015). Tukey's method for outlier identification was attempted first due to proven utility and because of its relative simplicity compared to other methods (Kannan et al., 2015).

Tukey's method involves identifying the interquartile range (IQR) of the data for a continuous variable (Kannan et al., 2015). The quartiles of the data are first identified. The IQR is calculated as the difference between the first quartile median (Q1) and the third quartile median (Q3) of the data. Q1 represents the median of the lower half of the variable data and Q3 represents the median of the upper half of the variable data. To find the normal range, IQR*1.5 is calculated, then IQR*1.5 is subtracted from Q1 to determine the lower bound of the normal range and IQR*1.5 is added to Q3 to determine the upper bound of the normal range. Finally, any value less than the lower bound is considered an outlier to be eliminated and any value greater than the upper is considered an outlier to be eliminated.

Tukey's Method was applied to the data to determine the effects on the normal distribution of the DV, as well as the effects on linearity, homoscedasticity, and independence. This led to the elimination of 39 variables, which resulted in a sample size of $N = 599$. Figure 4 indicated that the distribution was not yet normalized. The improved

fit of the points in Figure 5 to the line of best fit indicated that the assumptions of linearity, homoscedasticity, and independence were not grossly violated, and were improved compared to what was seen in Figure 2 when $N = 638$. Again, comparing the high values skewing Figure 4 rightward with the boxplot represented in Figure 6 confirming extreme values, however, indicated that outliers still existed in the DV and must be eliminated.

Figure 4

*Histogram of Distribution of Dependent Variable (*N = *599)*

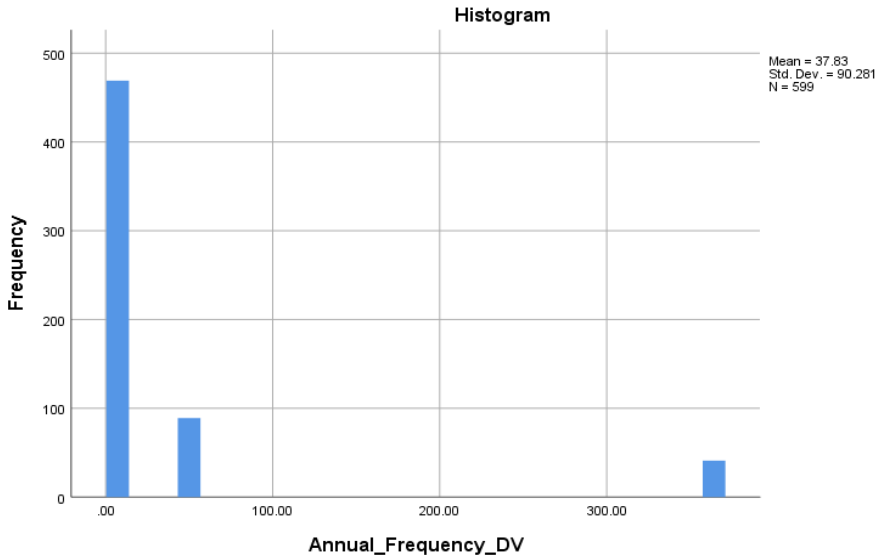


Figure 5

*Normal Probability Plot (Q-Q) of Dependent Variable (*N = *599)*

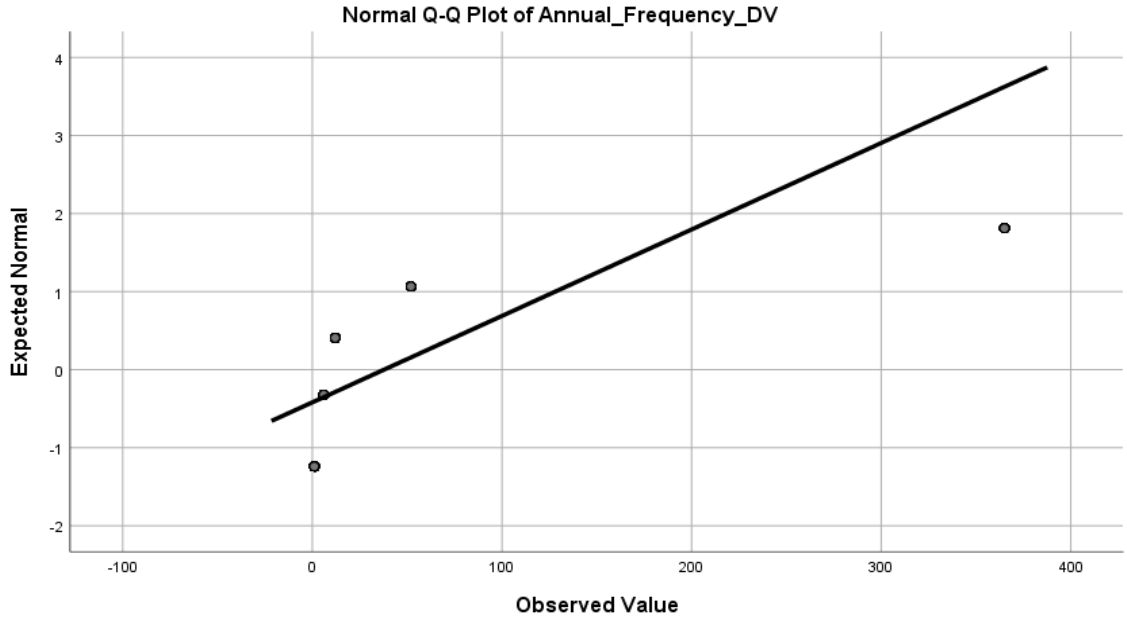
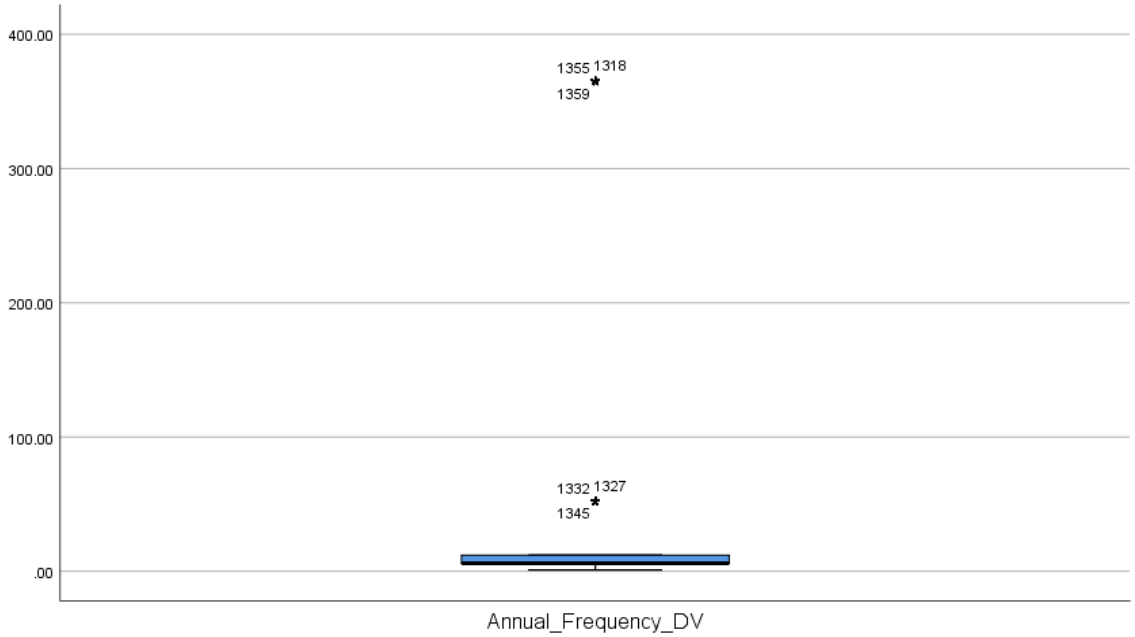


Figure 6

*Boxplot of Distribution of Dependent Variable (*N *= 599)*



I determined that a second application of Tukey's method would be worth testing to confirm whether a normal distribution could be achieved through the elimination of the outliers identified in Figure 6. A total of 130 outliers were calculated then eliminated, resulting in a sample size of $N = 469$. Examinations of the resultant histograms (Figures 7 and 8), normal probability (Q-Q) plot (Figure 9) and boxplot (Figure 10) indicated there were no major violations of normality, linearity, homoscedasticity, or independence of residuals. The distribution of values in Figures 7 and 8 clearly indicates that the $N = 469$ DV dataset has a normal distribution. The distribution of the values in Figure 9 indicates no issues with linearity, homoscedasticity, or independence of residuals, considering the clear linear pattern of the points. Figure 10 confirms the lack of outliers with the potential

to weaken the DV dataset. I concluded that applying Tukey's method twice was the appropriate way to complete final preparations for multiple regression data analysis.

Figure 7

*Histogram of Distribution of Dependent Variable (*N = *469)*

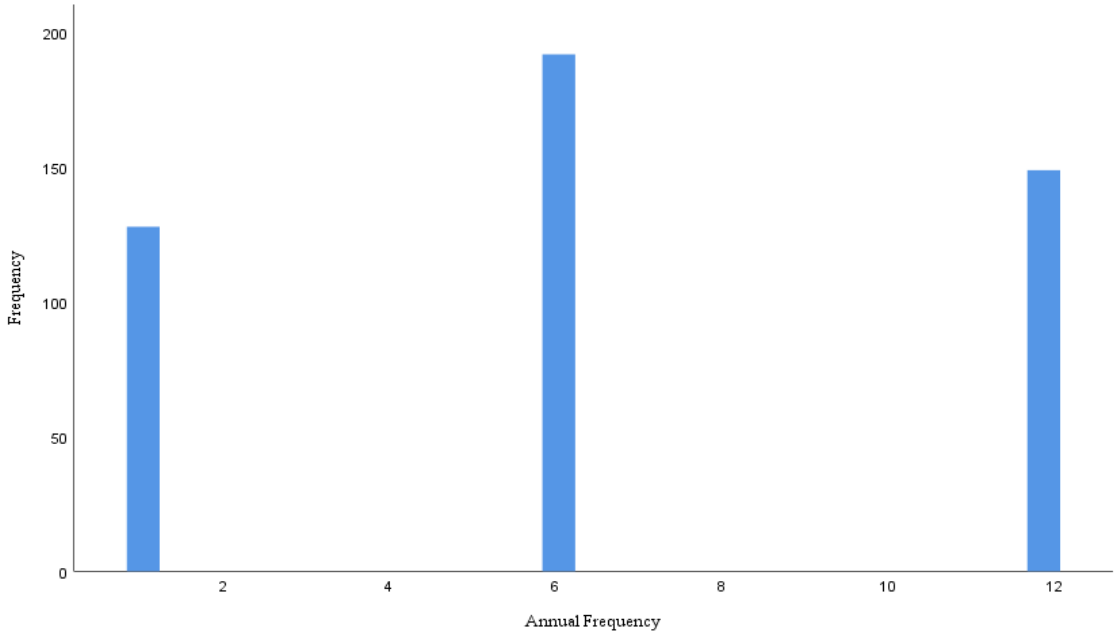


Figure 8

*Regression Standardized Residual Histogram (*N = *469)*

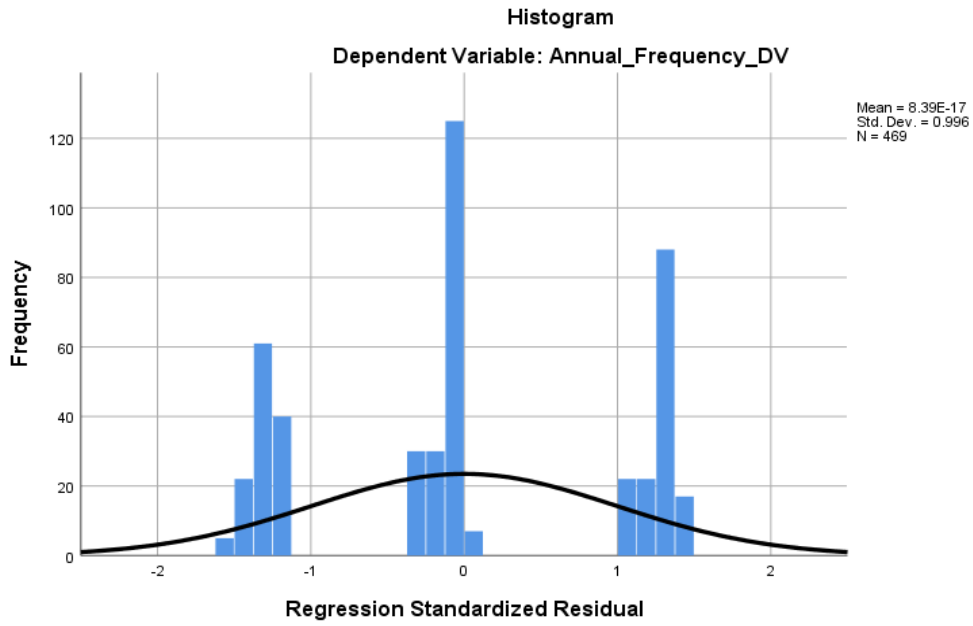


Figure 9

*Normal Probability Plot (Q-Q) of Dependent Variable (*N = *469)*

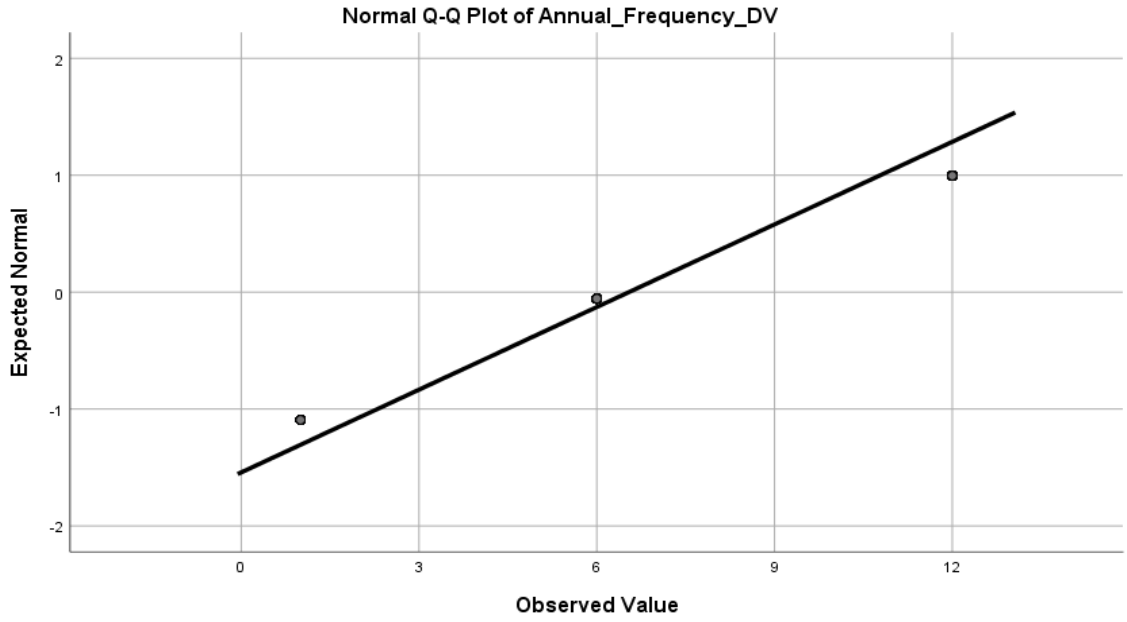


Figure 10

*Boxplot of Distribution of Dependent Variable (*N = *469)*

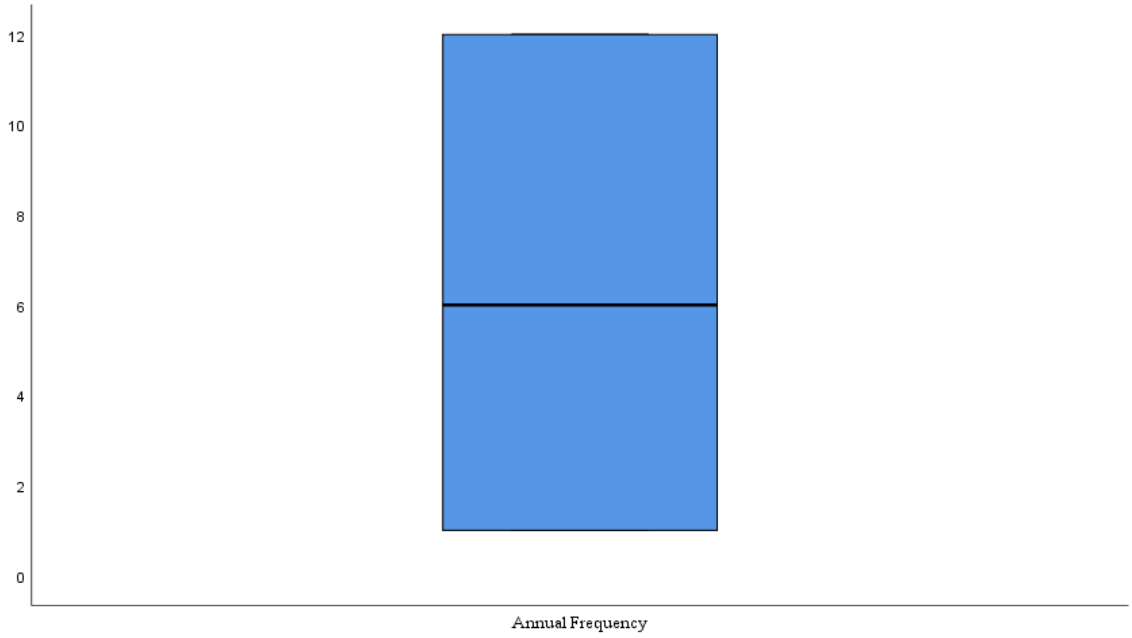


Table 2

Frequency Table for Attack Rate

Attack Rate (Annual)	Frequency	Percent
1	128	27.3
6	192	40.9
12	149	31.8
Total	469	100

Of the N = 469 participants prepared for data analysis at this point, it was not necessary to eliminate any for lack of representation in the IVs. Table 2 contains frequency data for Attack Rate, which was the rate of cybersecurity attacks or breaches participants' organizations had experienced. Note that as the participant pool was reduced so that the response variable would meet the necessary assumptions for multiple regression analysis, the total for each of the frequency tables was likewise limited to 469 total participants. Table 3 contains frequency data for the variable Seeking Guidance, which was the total number of sources from which participants sought information about cybersecurity threats. Table 4 contains frequency data for Management Involvement, which was a scale indicating the degree to which management was involved in organizational cybersecurity efforts. Figure 11 contains a histogram of the frequency distribution of Organizational ISPC. As this variable featured so many possible scores, it was not possible to display their frequencies in the form of a table. A histogram was far more efficient in displaying frequency information for this variable. Finally, Table 5 contains frequency data for Perceived Importance. Perceived Importance was a relatively

simple variable encompassing whether cybersecurity was perceived as a priority with reference to external stakeholders.

Table 3

Frequency Table for Seeking Guidance

Seeking Guidance (Scale)	Frequency	Percent
0	129	27.5
1	172	36.7
2	104	22.2
3	42	9
4	16	3.4
5	6	1.3
Total	469	100

Table 4

Frequency Table for Management Involvement

Management Involvement (Scale)	Frequency	Percent
2	10	2.1
3	36	7.7
4	116	24.7
5	162	34.5
6	141	30.1
7	4	0.9
Total	469	100

Figure 11

*Frequency Distribution Histogram of Organizational ISPC (*N = *469)*

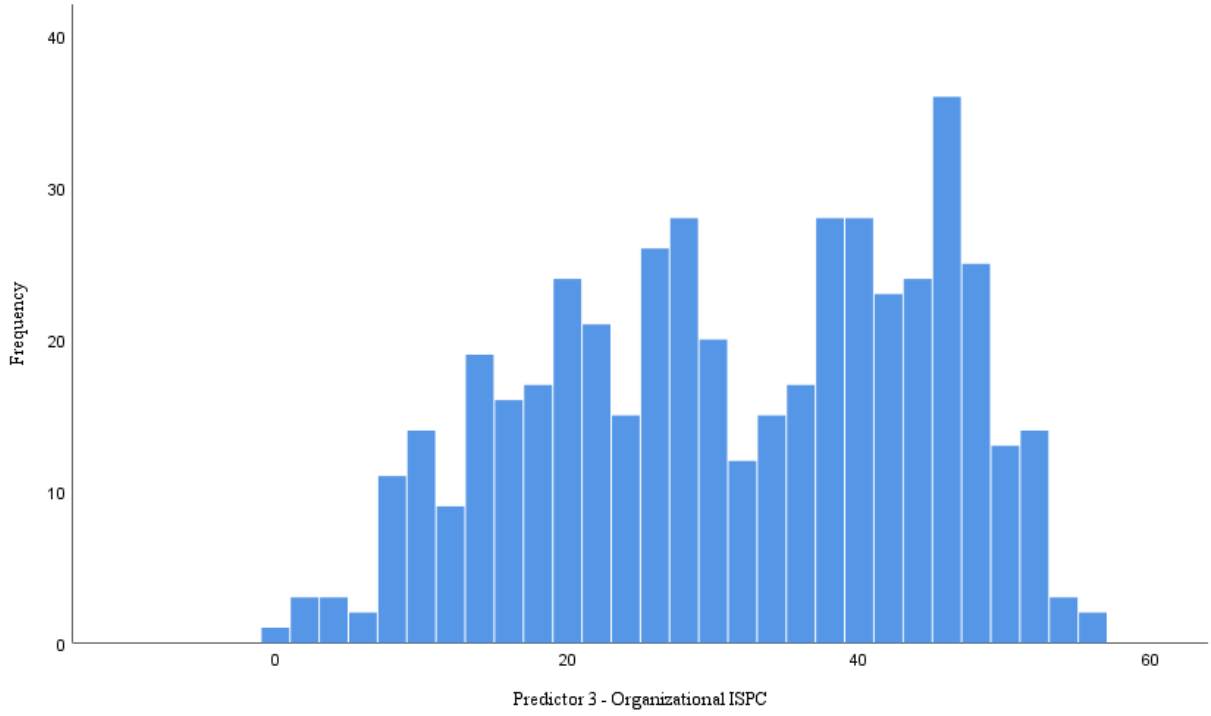


Table 5

Frequency Table for Perceived Importance

Perceived Importance	Frequency	Percent
0 (High Importance)	364	77.6
1 (Low Importance)	105	22.4
Total	469	100

Descriptive Results

Of the 1,419 total surveyed, 469 businesses were part of this study's final data analysis. Variable construction and data cleaning led to the elimination of 781 participants. Applying Tukey method twice resulted in the elimination of 169 additional participants. Table 6 contains descriptive statistics of the study variables. Table 7 contains the descriptive statistics of the regions of businesses surveyed in the UK for the 2021 CSBS within the participant data used for this study. This data was presented to demonstrate to future potential researchers that it is possible to further analyze the CSBS data using location data to determine patterns in cybersecurity behavior. Scholars may also attempt to determine the geographic representativeness of the dataset, though this was beyond the scope of the present study.

Table 6

Means and Standard Deviations for Quantitative Study Variables

Variable	M	SD	95% C.I.
Attack Rate (DV)	6.54	4.24	[6.16,6.93]
Seeking Guidance	1.28	1.14	[1.18,1.38]
Management Involvement	4.85	1.03	[4.76,4.95]
Organizational ISPC	31	13.1	[29.82,32.19]
Perceived Importance	0.22	0.42	[0.19,0.26]

Note. $N = 469$

Table 7

Frequency of Regions of Businesses Surveyed in 2021 CSBS in Percentage

Region	Frequency	Percent
Midlands	77	16.4
South of England	179	38.2
North of England	85	18.1
London	73	15.6
Scotland	32	6.8
Northern Ireland	8	1.7
Wales	15	3.2
Total	469	100.0

Table 8 contains the descriptive statistics of the business sectors of the organizations surveyed for the 2021 CSBS within the participant data used for this study. Future cybersecurity researchers may choose to use this type of information to determine the relative strengths of cybersecurity preparation, differences in attack rates, and other potential differentials that may exist between business sectors. This may also aid cybersecurity providers and other stakeholders target specific sectors in need of specific cybersecurity risk management products and services.

Table 9 contains the descriptive statistics of the size classifications of the participating businesses. Researchers may choose to determine whether size is a factor in a diverse number of cybersecurity outcomes, such as attack rate, cost of breach, or prioritization of information security. Combined with revenue information, this may help cybersecurity providers more optimally target products and services to potentially untapped market potential.

Table 8

Frequency of Sectors in Businesses Surveyed in 2021 CSBS in Percentage

Sectors	Frequency	Percent
Administration or real estate	81	17.3
Construction	39	8.3
Education	4	0.9
Entertainment, service or membership organisations	29	6.2
Finance or insurance	29	6.2
Food or hospitality	24	5.1
Health, social care or social work	31	6.6
Information or communication	34	7.2
Professional, scientific or technical	51	10.9
Retail or wholesale (including vehicle sales and repairs)	78	16.6
Transport or storage	18	3.8
Utilities or production	51	10.9
Total	469	100.0

Table 9

Size Classifications of Businesses Surveyed in the 2021 CSBS

Size Classification	Frequency	Percent
Micro (1 to 9)	188	40.1
Small (10 to 49)	84	17.9
Medium (50 to 249)	95	20.3
Large (250+)	102	21.7
Total	469	100.0

Inferential Results

The first inferential calculation was the Pearson product-moment coefficient between all variables for the purpose of testing the validity of statistical assumptions and to determine whether bivariate relationships exist between the DV and any of the IVs. Table 1 contains the Pearson's *r* results between the IVs, demonstrating that the predictor

variables exhibited no major signs of multicollinearity. Table 10 contains the Pearson's *r* results between the DV and the IVs. No significant correlations were found between the DV and any of the IVs.

Standard multiple linear regression, $\alpha = .05$ (two-tailed), was used to determine whether the variables Seeking Guidance, Management Involvement, Organizational ISPC, and/or Perceived Importance were predictive of job satisfaction. The full names of the independent variables were seeking of information or guidance on cybersecurity, senior management involvement, use of organizational ISPC, and perceived importance of cybersecurity. The full name of the dependent variable was organizational security breach incidence. The full name of the dependent variable was instances of cybersecurity breach or attack. The null hypothesis (H_0) was: There is no statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence. The alternative hypothesis (H_1) was: There is a statistically significant relationship between perceived importance of cybersecurity, senior management involvement, use of organizational ISPC, seeking of information or guidance on cybersecurity, and organizational security breach incidence.

Table 10

Correlations Between Dependent Variable and All Independent Variables

	Attack Rate	Seeking Guidance	Management Involvement	Organizational ISPC	Perceived Importance
Attack Rate	1	0.013	0.027	0.008	0.087

Notes. $N = 469$, "*" $p < .05$, "**" $p < .01$

Table 11

Regression Analysis Summary for Predictor Variables

Independent Variable	*B*	*SE B*	*β*	*t*	*p*	95% C.I.
Seeking Guidance	0.022	0.184	0.006	0.121	0.904	[-0.339, 0.385]
Management Involvement	0.106	0.222	0.026	0.479	0.632	[-0.329, 0.542]
Organizational ISPC	-0.016	0.019	-0.051	-0.849	0.396	[-0.054, 0.022]
Perceived Importance	1.027	0.521	0.101	1.973	0.049	[0.004, 2.050]

Note. $N = 469$

Correlations between variables indicated that the assumption of multicollinearity was not violated. Distribution histograms, normal probability (Q-Q) plots, and boxplots were used to assess whether the assumptions of outliers, normality, linearity, homoscedasticity, and independence of residuals were met. Initial testing indicated violation of the assumptions of outliers and normality. Tukey's method of identifying upper and lower bounds to a dataset was applied twice onto the DV to eliminate outliers. Upon the second application of Tukey's method, the generated histograms, normal probability (Q-Q) plot, and boxplot indicated that the assumptions of outliers, normality, linearity, homoscedasticity, and independence of residuals were met; no serious violations were noted (see *Tests of Assumptions*).

Table 12

Regression Model Summary

Model	*R*	R^2	Adjusted R^2	Std. Error of the Estimate	*F*	df1	df2	*p*
1	0.096	0.009	0.001	4.242	1.072	4	464	0.37

The multiple regression model (Table 12) as a whole was not able to significantly predict for Attack Rate—at F (4, 464) = 1.07, p = .370, R^2 = .02—using unstandardized coefficients. The equation for this model was Pred (Attack Rate) = 6.28 + .022*(Seeking Guidance) + .106*(Management Involvement) - .016*(Organizational ISPC) + 1.03*(Perceived Importance). Most of the independent variables— Seeking Guidance (β = .006, p = .904), Management Involvement (β = .026, p = .632), and Organizational ISPC (β = -.051, p = .396)—were not predictive of Attack Rate. Overall, the inability of the standardized equation for the model to significantly predict for Attack Rate meant that the null hypothesis was supported by the multiple regression analysis.

Perceived Importance

The multiple regression model, however, yielded a single significant standardized predictor: Perceived Importance was weakly but statistically significantly predictive of Attack Rate (β = .10, t (464) = 1.97, p < .05). Perceived Importance refers to the degree to which ISPC is considered important in organizational operations. This IV is represented by a single item, barrier6, which is one of eight possible responses to Question 45: “Which of the following have made it difficult for your organisation to manage any cyber security risks from your supply chain or partners?” Barrier6 represented the response “It's not a priority when working with suppliers or partners.” An affirmative value of barrier6 signified lower Perceived Importance, while a null value of

barrier6 signified higher Perceived Importance. As a result, the positive association signified by the *b* value means that lower Perceived Importance was associated with increased Attack Rate.

Table 13

Summary of Perceived Importance

β	*t*	*p*	95% C.I.	β^2
0.101	1.973	.049*	[0.004, 2.050]	0.008

*$p < .05$

The effect size of Perceived Importance is the square of the semi-partial correlation, .091^2 = 0.008, which is a small, but nevertheless statistically significant effect size (see Keith, 2019). This study was able to confirm that perceived importance of ISPC was positively correlated with incidence of cybersecurity attack or breach. The data indicated that Perceived Importance was weakly associated with Attack Rate, such that lower perceived importance of cybersecurity throughout the organization was associated with increased instances of cybersecurity attack or breach. In summary, despite the acceptance of the null hypothesis, the data indicated that perceived importance of cybersecurity was a significant predictor of annual cybersecurity attack instances.

Conclusions of the Analysis

The purpose of this study was to determine whether seeking of information or guidance on cybersecurity, senior management involvement, use of organizational ISPC, and perceived importance of cybersecurity were predictive of instances of cybersecurity breach or attack. I used standard multiple linear regression analysis to examine the joint ability of the IVs to predict for annual rate of cyberattack. Initial assessments of the

assumptions required for multiple regressions yielded violations and raise some concerns, so Tukey's method was used twice to eliminate outliers and normalize the response variable. After eliminating the outliers, further assessments yielded no serious violations of the assumptions for multiple regression analysis.

The model was not predictive of instances of cybersecurity breach or attack. Due to this finding, the null hypothesis was accepted. However, perceived importance of cybersecurity was found to be predictive of the dependent variable ($b = .10$, $t\ (464) = 1.97$, $p < .05$). Because an affirmative value for the variable Perceived Importance indicates lower degree of perceived importance of cybersecurity, lower perceived importance was associated with increased annual instances of cybersecurity attack or breach. To wit, higher perceived importance was associated with decreased annual instances of cybersecurity attack or breach. The primary conclusion that can be drawn from this analysis is that the standardized regression of perceived importance relative to the other variables is significantly associated with instances of cybersecurity attack or breach.

Applications for Professional Practice

The main conclusion drawn from the results of this study is that the degree to which an organization ascribes importance to cybersecurity will influence the rate at which the organization will be attached or breached annually. It is recommended, then, for business leaders is to prioritize cybersecurity for their respective organizations. The findings imply that emphasizing the importance and centrality of cybersecurity throughout the organization—particularly with processes that involve third-party

stakeholders such as external partners, contractors, distributors, and suppliers—is associated with fewer instances of cybersecurity attack or breach. Many potential methods to emphasize organizational cybersecurity are found in the literature, including increased engagement of highly visible organizational leaders, organization-wide cybersecurity education and awareness programs, ISP revisions, and the promotion of cybersecurity within organizational culture (Alshaikh, 2020; Caratas et al., 2019; Daud et al., 2018; Pullin, 2018; Vishwanath et al., 2020).

Another recommendation for professional practice is for organizations to consider investing resources into ex ante mitigations of cybersecurity threats. As this study confirmed, a before-the-fact factor such as Perceived Importance can be significantly predictive of cybersecurity attack and breach rates. Yet both organizations and information security providers have traditionally focused upon ex post response measures to attacks or breaches that have been discovered after-the-fact (Kuerbis & Badiei, 2017). As multiple frameworks—including NIST's (2011; 2018) cybersecurity risk management framework, Kuerbis and Badiei's cybersecurity industry framework, and Knight and Nurse's (2020) cybersecurity communication framework—suggest, the communication and investigation of the unknowns of cybersecurity threats and risks are key elements to the risk management process. It might behoove organizations to actively invest in auditing potential organizational precursors for insider threat, using the results to create interventions. Over the long term, this may prove to be more efficient than focusing resources solely upon detection and mitigation after the attacks or breaches have already taken place.

A related recommendation is for IT professionals, service providers, and others in the cybersecurity industry to begin developing ex ante solutions for organizational cybersecurity. Although this study was limited to correlational statistics that are unable to determine causation, it is quite possible that addressing significant antecedent factors associated with security breaches may be a cost-efficient method of mitigating emerging cybersecurity threats. These ex ante solutions might be welcome throughout industries involving IT because serious protocols for decreasing insider threat are not yet standard (Addae et al., 2019; Bhaharin et al., 2019; Pullin, 2018). Forward-thinking providers may be able to gain competitive advantage by offering insider threat mitigation before market demand inevitably shifts toward ex ante products and services.

Implications and Impacts for Social Change

The primary implication of the study for positive social change is the confirmation that prioritizing cybersecurity as an important organizational issue is predictive of lower rates of cybersecurity attack and breach. The major aspects of cybersecurity that are key to positive social change include the right to privacy and the protection of personal information, which exist in a state of synergy. The basic human right to privacy is increasingly becoming a major issue of concern for consumers, as more of their private information are placed into internet servers due to IT implementations. The protection of this information is paramount, as a single breach can allow for identity theft, which can have far-reaching financial and lifestyle consequences for victims. Together, the issues of privacy and data security are making it imperative for organizations to actively and publicly address cybersecurity concerns for the sake of

preserving their reputations. As the world becomes more connected, cybersecurity only become more paramount, as online privacy and data protection enters the realm of public safety. The more completely an organization addresses security issues stemming from inside threat, the greater its contribution to public safety becomes.

Recommendations for Further Research

A major recommendation for further research is to improve upon the problematic elements of the 2021 CSBS dataset. An issue with the dataset was the lack of resolution in the dependent variable. As it turned out, though the 2021 CSBS did yield much data that could be easily modified or cleaned to be quantitative, the nature of the telephone survey made it such that data for the DV was unrefined. The survey item for this variable was Question 54, which was: "Approximately, how often in the last 12 months did you experience any of the cyber security breaches or attacks you mentioned?" Instead of asking participants for specific quantitative estimates of how often their organizations experience a cybersecurity attack or breach, however, the survey question for this item gave participants a selection of choices, including "once only", "more than once but less than once a month", "roughly once a month", "roughly once a week", "roughly once a day", and "several times a day". Converting this data into a form conducive to quantitative analysis led to a dataset for the DV ranging from the values of 1 to 1460, but in six total increments rising exponentially in value. The incremental and exponential nature of the DV was the primary reason why the original dataset at $N = 639$ so evidently violated the assumptions of outliers and normality, necessitating the systematic elimination of outliers that ultimately normalized the data. The nature of the DV may

have been a contributing reason why the multiple regression model failed to be predictive. It is recommended for future researchers to use a cybersecurity breach or attack measure with more resolution than was available for this study.

A related recommendation for future research would be the testing of various different combinations of variable assignment and variable construction using the 2021 CSBS data. A major issue with the dataset was the large number of survey items and potential responses to survey items, such as one question featuring 63 total potential responses. This necessitated the combination of multiple items and responses to construct three of the four independent variables operationalized for this study (see *Presentation of Qualitative Data Analysis*). Although the scope of this study limited the investigation to five total variables, a future study need not limit itself when conducting secondary data analysis on CSBS datasets. Researchers willing to take advantage of the CSBS are recommended to investigate various different combinations of variables to determine whether significant inferential conclusions can be drawn. The CSBS datasets are rich resources that may have many insights to be uncovered through judicious variable formation and application of inferential statistics.

A further recommendation is for researchers to continue investigating ex ante predictors of cybersecurity breaches and attacks, particularly those related to insider threat. The current model of ex post attempts to mitigate the consequences of cybersecurity attacks after they occur are not enough considering that insiders remain the greatest threat to information security. As the results of this study demonstrate, an ex ante factor, such as Perceived Importance, can be a significant predictor of cybersecurity

breach rate. It will be important, then, to increase the body of knowledge regarding organizational factors that mediate cybersecurity risk. An ongoing process of research and discovery will be necessary to fully understand the human factors that directly mediate cyberattack risk.

Another major conclusion that can be drawn from this study is the need for methodologically rigorous research with data of sufficient resolution. Although this study's regression model was not predictive of the annual rate of cybersecurity attack or breach, this does not mean that the study as a whole does not have applications for cybersecurity research. As Moody et al.'s (2018) and Koohang et al.'s (2021) attempts to develop a holistic framework of ISPC demonstrated, a complete and comprehensive understanding of insider threat has not even begun to be constructed in detail. This will not only require an understanding of the antecedents of cybersecurity breaches as recommended above, but a concentrated effort of researchers to rigorously operationalize the variables used so that subsequent scholars could better replicate and/or compare findings of different studies. As researchers have observed, the variables found in cybersecurity research often differ considerably, leading to problems in developing holistic hypotheses or drawing comprehensive conclusions (Koohang et al., 2021; Moody et al., 2018). This study itself, as was illustrated in the variable construction process, has demonstrated potential problems related to assigning and constructing variables from existing data. As such, detailed and replicable operationalizations of quantitative variables throughout the discipline would facilitate the rigorous consolidation of cybersecurity research.

Recommendations for Action

The major conclusions that characterize this study are (a) the significance of perceived importance of cybersecurity throughout an organization on rates of cyberattack and cybersecurity breaches, (b) the need for research to be integrated into organizational information security processes, and (c) the need for methodologically rigorous academic research on the antecedents to cybersecurity attack rates. The targets for disseminating the conclusions of present study include two general groups of stakeholders. The first group includes organizational leaders, management, and IT professionals who have any stake within their respective organization's cybersecurity. This would involve leadership at all levels, especially top-level management, due to the key role senior management can play in mitigating cybersecurity risks (Alshaikh, 2020; Daud et al., 2018; Hu et al, 2012; Pullin, 2018). The second group includes organizations and scholars who are researching, developing, and/or providing ex ante cybersecurity implementations designed for mitigating cybersecurity attacks and breaches.

The overall strategy for action commences in four total stages, the first two focusing on a broad and easily accessible distribution of the study then the latter two focusing on distribution to organizational leaders and IT professionals. The first stage of the strategy will hinge upon disseminating the study in as a widely distributed and easily accessible form as possible for the principal investigator for a minimum of monetary investment. Though researchers tend to first disseminate their studies via peer reviewed journals, this strategy involves distributing the findings via self-publishing platforms such as Amazon. The primary advantage of this strategy will be the ability to harness the

search engine of the self-publishing platform itself. As the topic of the paper involves specialized keywords, such as information security policy compliance, the keywords related to this study will have a larger chance of being discovered by potential readers than in more general topics. Online self-publishing has the major advantage of being easy to distribute through many different online media, which will play a role the second stage of this strategy: establishing an online presence in a professional and academic networking platforms such as LinkedIn and ResearchGate. This will enable the principal researcher to connect with the public at large using the topics covered in this study while opening an avenue for networking with interested individuals.

The third and fourth stages of the strategy will hinge upon more specialized distribution within specialized academic and professional communities, such as cybersecurity specialists and business administrators. The third stage will involve applying for publication in both scholarly journals and trade publications. The former will help disseminate the findings and conclusions of this study to promote research in the recommended direction, while the latter will help develop awareness of the insider threat issues in professionals. The primary advantages of this method, if the articles are accepted, are (a) the targeting of a highly focused group of scholars and practitioners with a high chance of being actively interested in the findings and (b) distribution of the articles in academic and professional article databases frequented by scholars and professionals. The fourth stage will be to actively seek out conferences and groups related to cybersecurity, offering to give presentations directly related to the contents and

findings of this study. This will allow for real-time interaction with those interested in the study, as well as opportunities to be published in conference-related publications.

Communication Plan

The communication plan will directly reflect the strategy for disseminating the results and conclusions of the study. To this end, the present study will be modified into four general forms of communication—two forms for broad distribution and two forms for specific distribution. Note that each form will be a specific adaptation of this study's content, to ensure efficiency without the need for extraneous content-creation.

The first form will be as an electronic book formatted for the lay population. An important element of this book will be to craft the title and the description to be optimized for specialized keywords pertaining to ISPC, cyber hygiene, and insider threat. The advantage of this form will be easy accessibility for the public—be it laypeople, scholars, or professionals—through commonly accessed book distributors that will also be automatically compiled into major search engines. Of all forms of communication, this would be the most widely accessible. The second form will be that of a series of short articles to be posted on professional networks to draw attention to this study and the electronic book. The primary purpose of this form would be to adapt short pieces of the study to draw attention to specific cybersecurity topics, and to the study and electronic book, without the need for additional content-creation or research.

The third form will be adaptations of this study into articles that would be submitted for review in scholarly journals covering either cybersecurity or business. The most easily adapted articles would be comprised of complete elements of this study, such

as the literature review and the quantitative correlational design. More work would be involved in using the notes compiled for the study to expand upon a section, such as an article on the historical background of ISPC research. The most work would be using this study and its notes to write novel articles, such as a proposal for increased rigor in insider threat research. Note that the articles may be scholarly or professional in nature. Finally, the fourth form will be the creation of several presentations—in the form of slides or posters—that can be presented in professional and scholarly conferences or organizations. As the content of the presentations would be based on that of the scholarly or professional articles written for stage four, they would be of minimal effort to create.

Skills and Competencies

The first set of competencies I demonstrated was the ability to identify critical gaps in both practice and research in the field of information security, while developing a proposal for a research project. This was not just a matter of reading articles related to cybersecurity. This involved the browsing of academic databases with varied cybersecurity keywords while simultaneously conducting focused research on specific topics that were encountered. It also required the active evaluation of the current state of various topics in cybersecurity research according to criteria such as (a) length of time they have been featured in literature, (b) the general number of articles available about each, (c) which topics have been rich in engagement in the last five years, (d) current gaps being examined, and (e) current gaps that have not yet been addressed. Only after an extensive scrutiny of cybersecurity research was I able to decide upon insider threat as a fruitful topic to pursue for this study. It was also during the initial scrutiny when I

demonstrated my ability to conduct a deep search to find a relatively pristine dataset that matched the purpose I had initially proposed for this study.

Throughout the review of literature in preparation for this study, I demonstrated the ability for focused research into a set of related topics to elucidating a research problem and provide a detailed survey of the context with which the study could be understood. Scholarly literature on topics as potentially broad as ISPC, insider threat, and cyber hygiene are not organized in any meaningful way but are published in many different publications with various different specializations. As the principal researcher, I demonstrated the ability to read a large body of research in the relevant topic and systematically organize it into a form that could be more easily understood by an audience. In the literature review itself, I demonstrated the ability to communicate what I had discovered to document the meaningful structure that contextualized the content of this study.

I demonstrated multiple competencies while designing the quantitative study, preparing a large-scale public dataset for analysis, constructing variables from dataset items, engaging in quantitative research, and interpreting inferential results. In designing a quantitative correlational study, I demonstrated my ability to plan and execute an entire course of empirical investigation tailored to address a specific research question while documenting the process throughout. In cleaning the data and constructing variables, I demonstrated my ability to execute a technically complex task using specialized software of which I had minimal experience, through judicious research, seeking of guidance, documentation, and self-checking. I also demonstrated the ability to test assumptions and

print the relevant figures as proof. Likewise, in analyzing the prepared dataset using multiple linear regression, I demonstrated my ability to execute the final stages of SPSS analysis while printing all of the data relevant to communicating the analysis. Finally, I demonstrated competency in interpreting quantitative outputs, relating it to the context of the literature, and recommending multiple aspects of research and action.

Reflections

My most poignant realization occurred when I first examined the makeup of the survey items, within the actual dataset, that were supposed to comprise the study's five variables. I greatly overestimated the utility of the 2021 CSBS for the type of quantitative study I had designed. I had only reviewed the 2021 CSBS's Statistical Release and the Technical Annex, as I had an understanding that I was not to begin using the actual dataset prior to IRB approval. I had made the mistaken assumption that the data for the DV would only require minimal cleaning to be optimized for correlational research. In reality, the survey item corresponding to the dependent variable was not optimal for quantitative research as the response choices only had a limited number of choices. Having reviewed the questionnaire in the Technical Annex, I had likewise mistakenly assumed that the items related to the IVs could be used for relatively straightforward variable construction. In reality, many survey items were not optimized for variable construction, which led me to decide to construct three survey items in the form of scales, which may not have been optimal. It is distinctly possible that these issues with the dataset may have been why the multiple linear regression model was not significantly predictive of attack rate.

Despite having taken an applied skills course on quantitative data analysis and SPSS, working with the CSBS dataset in SPSS was both far more difficult than I had expected, while simultaneously taking far less time than I had estimated. The difficulties were rooted in using search engines, references, resources, and tutors to learn which SPSS functions I would need to use for constructing the variables and preparing the data for analysis, and how these functions should be executed. As I was using many of these functions for the first time, while teaching myself and seeking minimal guidance, there were many instances in which I was forced to recheck the work multiple times to ensure that various elements of data preparation were completed without issue. Despite these difficulties, there were far less new functions to learn that I had planned for. Likewise, conducting multiple regression analysis on a dataset this size was near instantaneous. I experienced quite an abrupt end to the data analysis process because the interpretation of the data was far more straightforward than the preparatory work. In summary, this project was a challenge that I am glad to have taken up and completed.

Conclusion

The multiple regression model—which integrated the independent variables Seeking Guidance, Management Involvement, Organizational ISPC, and Perceived Importance—was not predictive of annual rates of cyberattack or breach among the participants of the 2021 Cyber Security Breaches Survey that were included in this study. Several reasons for this result were presented, including the nature of the 2021 CSBS, the variable construction process that characterized three of this study's IVs, and data cleaning due to nonnormal distribution of the DV. Although the null hypothesis was

accepted, the analysis did yield a significant result: lower Perceived Importance was predictive of a higher Attack Rate among the participants. In this study, it was again confirmed that insider threat was associated with increase organizational cybersecurity risk. In a cybersecurity marketplace full of after-the-fact fixes to existing attacks or breaches, practitioners are recommended to consider a focus on preventative measures to mitigate insider threat. In a cybersecurity discipline full of conflicting research, scholars are recommended to consider increasing methodological rigor in an attempt to consolidate insider threat research. As Industry 4.0 continues its inevitable rise, the right to privacy and the protection of sensitive personal data will inevitably become matters of public safety. In response, it will be necessary for all stakeholders to prepare diligently for this major shift in paradigm.

References

Aceto, G., Persico, V., & Pescape, A. (2019). A survey on information and communication technologies for Industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges. *IEEE Communications Surveys & Tutorials, 21*, 3467-3501. https://doi.org/10.1109/COMST.2019.2938259

Addae, J. A., Simpson, G., & Ampong, G. O. A. (2019). Factors influencing information security policy compliance behavior. Presented at the *2019 International Conference on Cyber Security and Internet of Things*, 43–47. https://doi.org/10.1109/ICSIoT47925.2019.00015

Alferidah, D. K., & Jhanjhi, N. (2020). Cybersecurity impact over bigdata and IoT growth. *2020 International Conference on Computational Intelligence (ICCI), Computational Intelligence,2020 International Conference On*, 103–108. https://doi.org/10.1109/ICCI51257.2020.9247722

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*. https://doi.org/10.1016/j.cose.2020.102003

Alshare, K. A., Lane, P. L., Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information and Computer Security*, *26*(1), 91-108. https://doi.org/10.1108/ICS-09-2016-0073

Alzahrani, A., Johnson, C., & Altamimi, S. (2018). Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation. Presented at the *2018 4th International*

Conference on Information Management, 125–132. https://doi.org/10.1109/INFOMAN.2018.8392822

Angraini, Alias, R. A., & Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216-224. https://doi.org/10.1016/j.procs.2019.11.235

Atanasoff, L., & Venable, M. A. (2017). Technostress: Implications for adults in the workforce. *Career Development Quarterly*, *65*(4), 326–338. https://doi.org/10.1002/cdq.12111

Baldin, A. (2019). Best practices for fighting the fileless threat. *Network Security*, *2019*(9), 13–15. https://doi.org/10.1016/S1353-4858(19)30108-4

Bhaharin, S. H., Mokhtar, U. A., Sulaiman, R., & Yusof, M. M. (2019). Issues and trends in information security policy compliance. Presented at the *2019 6th International Conference on Research and Innovation in Information Systems*, 1–6. https://doi.org/10.1109/ICRIIS48246.2019.9073645

Brinkmann, S. (2018). The interview. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (5th ed., pp. 984-1026). SAGE Publications.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Carataș, M. A., Spătariu, E. C., & Gheorghiu, G. (2019). Privacy and cybersecurity insights. *Ovidius University Annals, Series Economic Sciences*, *19*(2), 242–246.

Cassell, C., Cunliffe, A. L., & Grandy, G. (2018). Introduction: Qualitative research in business and management. In C. Cassell, A. L. Cunliffe, & G. Grandy (Eds.), *The SAGE handbook of qualitative business and management research methods* (Vol. 1, pp. 1-13). SAGE Publications.

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. *Journal of Information Science*, *44*(6), 752. https://doi.org/10.1177/0165551517748288

Cram, W. A., D'Arcy, A. J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525–554. https://doi.org/10.25300/MISQ/2019/15117

Creswell, J. W. & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). Sage.

Cuervo-Cazurra, A., Andersson, U., Brannen, M. Y., Nielsen, B. B., & Reuber, A. R. (2020). From the editors: Can I trust your findings? Ruling out alternative explanations in international business research. In L. Eden, B. B. Nielsen, & A. Verbeke (Eds.), *Research methods in international business* (pp. 121-157). Palgrave. https://doi.org/10.1007/978-3-030-22113-3

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business and Society, 19*, 161-180. http://www.ijbs.unimas.my/

Dawson, M. (2018). Applying a holistic cybersecurity framework for global IT organizations. *Business Information Review, 35*(2), 60-67. https://doi.org/10.1177/0266382118773624

Delios, A. (2020). Science's reproducibility and replicability crisis: A commentary. In L. Eden, B. B. Nielsen, & A. Verbeke (Eds.), *Research methods in international business* (pp. 67-74). Palgrave. https://doi.org/10.1007/978-3-030-22113-3

Denzin, N. K., & Lincoln, Y. S. (2018). Introduction: The discipline and practice of qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (5th ed., pp. 31-76). SAGE Publications.

Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for nontechnical majors. *Journal of Cybersecurity Education, Research, and Practice, 2017*(1), 1-17. https://digitalcommons.kennesaw.edu/jcerp/vol2017/iss1/3

Elifoglu, I. H., Abel, I., & Taşseven, Ö. (2018). Minimizing insider threat risk with behavioral monitoring. *Review of Business, 38*(2), 61-73. https://www.stjohns.edu/academics/schools/peter-j-tobin-college-business/departments-centers-and-faculty-research/review-business

Erickson, F. (2018). A history of qualitative inquiry in social and educational research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The SAGE handbook of qualitative research* (5th ed., pp. 96-147). SAGE Publications.

Ghauri, P., Gronhaug, K., & Strange, R. (2020). *Research methods in business studies*. Cambridge University Press.

Gronmo, S. (2020). *Social research methods: Qualitative, quantitative, and mixed methods approaches.* SAGE Publications.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods* (2nd ed.). SAGE Publications.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hina, S., & Dominic, D. D. (2017). Need for information security policies compliance: A perspective in higher education institutions. *2017 International Conference on Research and Innovation in Information Systems*, 1–6. https://doi.org/10.1109/ICRIIS.2017.8002439

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security*, *87*. https://doi.org/10.1016/j.cose.2019.101594

Holton, J. A. (2018). From grounded theory to grounded theorizing in qualitative research. In C. Cassell, A. L. Cunliffe, & G. Grandy (Eds.), *The SAGE handbook of qualitative business and management research methods* (Vol. 1, pp. 233-250). SAGE Publications.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and

organizational culture. *Decision Sciences, 43*(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Indu, I., Anand, P. M. R., Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. *Engineering Science and Technology, an International Journal, 21,* 574-588. https://doi.org/10.1016/j.jestch.2018.05.010

Ipsos MORI (2021a). *Cyber Security Breaches Survey 2021*: *Education institutions findings annex*. United Kingdom Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977490/Cyber_Security_Breaches_Survey_2021_Education_Annex.pdf

Ipsos MORI (2021b). *Cyber Security Breaches Survey 2021: Statistical release.* United Kingdom Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/972399/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf

Ipsos MORI (2021c). *Cyber Security Breaches Survey 2021: Technical annex.* United Kingdom Department for Digital, Culture, Media and Sport. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/977491/20-046099-01_CSBS_2021_quant_technical_annex_v2.4__clean__190321.pdf

Jaeger, L., Eckhardt, A., & Kroenung, J. (2020). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. *Information & Management*. https://doi.org/10.1016/j.im.2020.103318

Kannan, K. S., Manoj, K., & Arumugam, S. (2015). Labeling methods for identifying outliers. *International Journal of Statistics and Systems, 10*, 231-238.

Keith, T. Z. (2019). *Multiple regression and beyond* (3rd Ed.). Routledge. https://doi.org/10.4324/9781315162348

Kiss, M., Breda, G., & Muha, L. (2019). Information security aspects of Industry 4.0. *Procedia Manufacturing*, *32*, 848–855. https://doi.org/10.1016/j.promfg.2019.02.293

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security, 99*. https://doi.org/10.1016/j.cose.2020.102036

Kondiloglu, A., Bayer, H., Celik, E. & Atalay, M. (2017). Information security breaches and precautions on Industry 4.0. *Tehnologìčnij Audit Ta Rezervi Virobnictva, 6/4*(38), 58–63. https://doi.org/10.15587/2312-8372.2017.117593

Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2019). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. https://doi.org/10.1108/IMDS-07-2019-0412

Koohang, A., Nord, J. H., Sandoval, Z. V., & Paliszkiewicz, J. (2021). Reliability, validity, and strength of a unified model for information security policy compliance. *Journal of Computer Information Systems, 61*(2), 99–107. https://doi.org/10.1080/08874417.2020.1779151

Kuerbis, B., & Badiei, F. (2017). Mapping the cybersecurity institutional landscape. *Digital Policy, Regulation and Governance, 19*(6), 466-492. https://doi.org/10.1108/DPRG-05-2017-0024

Leedy, P. D., & Ormrod, J. E. (2021). *Practical research: Planning and design* (12th ed.). Pearson Education.

Levine, R. A. (2016). Repairing the fractured social sciences: An introduction from a historical point of view. In M. C. Hay (Ed.), *Methods that matter: Integrating mixed methods for more effective social science research* (pp. 3-12). The University of Chicago Press. https://doi.org/10.7208/chicago/9780226328836.001.0001

Lo, F. Y., Rey-Martí, A., & Botella-Carrubi, D. (2020). Research methods in business: Quantitative and qualitative comparative analysis. *Journal of Business Research, 115*, 221–224. https://doi.org/10.1016/j.jbusres.2020.05.003

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193–273. https://doi.org/10.1111/isj.12063

Luo, X., Li, H., Hu, Q., & Xu, H. (2020). Why individual employees commit malicious computer abuse: A routine activity theory perspective. *Journal of the Association for Information Systems, 21*(6), 5. https://doi.org/10.17705/1jais.00646

Moellers, T., von der Burg, L., Bansemir, B., Pretzl, M., & Gassmann, O. (2019). System dynamics for corporate business model innovation. *Electronic Markets, 29*(3), 387-406. https://doi.org/10.1007/s12525-019-00329-y

Molina-Azorin, J. F. (2018). Mixed methods. In C. Cassell, A. L. Cunliffe, & G. Grandy (Eds.), *The SAGE handbook of qualitative business and management research methods: History and traditions* (Vol. 1, pp. 102-118). SAGE Publications.

Mon, A., & Giorgio, H. R. D. (2021). Evaluation of information and communication technologies towards Industry 4.0. *Procedia Computer Science, 180*, 639-648. https://doi.org/10.1016/j.procs.2021.01.286

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*, 285-311. https://doi.org/10.25300/MISQ/2018/13853

National Institute of Standards and Technology (2011). Managing information security risk: Organization, mission, and information system view (Special Publication 800-39). United States of America Department of Commerce, Computer Security Division. https://doi.org/10.6028/NIST.SP.800-39

National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations: A systems life cycle approach for security and privacy (Special Publication 800-37 Revision 2). United States of America

Department of Commerce, Joint Task Force. https://doi.org/10.6028/NIST.SP.800-37r2

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, *92*. https://doi.org/10.1016/j.cose.2020.101731

Nimawat, D., & Gidwani, B. D. (2021). Identification of cause and effect relationships among barriers of Industry 4.0 using decision-making trial and evaluation laboratory method. *Benchmarking, 28*(8), 2407-2431. https://doi.org/10.1108/BIJ-08-2020-0429

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2020). Impact of habits on information security policy compliance. *Issues in Information Systems*, *21*(3), 217–226. https://doi.org/10.48009/3_iis_2020_217-226

Núñez-Merino, M., Maqueira-Marín, J. M., Moyano-Fuentes, J., & Martínez-Jurado, P. J. (2020). Information and digital technologies of industry 4.0 and lean supply chain management: A systematic literature review. *International Journal of Production Research, 58,* 5034-5061. https://doi.org/10.1080/00207543.2020.1743896

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal of the Association for Information Systems*, *20*(12), 1794–1843. https://doi.org/10.17705/1jais.00586

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards is security policy compliance*. Paper presented at the 2007 40th Annual Hawaii

International Conference on System Sciences (HICSS'07), System Sciences, 2007. https://doi.org/10.1109/HICSS.2007.206

Ponemon Institute (2018). *2018 cost of data breach study: Global overview*. Ponemon Institute, LLC.

Ponemon Institute (2021). *2021 cost of a data breach report.* IBM Security.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management, 51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

PricewaterhouseCoopers (2018). Fighting new tech risk with new tech solutions. *Key findings from The Global State of Information Security Survey 2018*. Retrieved from https://www.pwc.com/us/en/cybersecurity/assets/pwc-gsiss-2018-technology-industry.pdf

PricewaterhouseCoopers (2021). Global digital trust insights survey 2021: Cybersecurity comes of age. https://www.pwc.ch/en/publications/2020/ch-Digital-Trust-Insights-Survey-2021-report.pdf

Pullin, D. W. (2018). Cybersecurity: Positive changes through processes and team culture. *Frontiers of Health Services Management, 35*, 3-12. https://doi.org/10.1097/HAP.0000000000000038

Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher

education. *Computers & Security*, *80*, 211–223. https://doi.org/10.1016/j.cose.2018.09.016

Rantao, T., & Njenga, K. (2020). Predicting communication constructs towards determining information security policies compliance. *South African Journal of Information Management*, *22*(1), e1–e10. https://doi.org/10.4102/sajim.v22i1.1211

Rees, K. (2019). A user-friendly practical guide to preparing data for analysis. In P. M. W. Hackett (Ed.), *Quantitative research methods in consumer psychology: Contemporary and data-driven approaches* (pp. 326-375). Routledge.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*, 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rudramuniyaiah, P. S., Joshi, K., Shah, V., & Ramanujan, S. (2020). Examining cognitive and emotive influences on knowledge sharing behavior among IT professionals: An empirical analysis. *E-Service Journal*, *11*(3), 1–35. https://doi.org/10.2979/eservicej.11.3.01

Saldanha, T. J. V., Mithas, S., & Krishnan, M. S. (2017). Leveraging customer involvement for fueling innovation: The role of relational and analytical information processing capabilities. *MIS Quarterly*, *41*(1), 267-A11. https://doi.org/10.25300/MISQ/2017/41.1.14

Sallis, J. E., Gripsrud, G., Olsson, U. H., & Silkoset, R. (2021). *Research methods and data analysis for business decisions: A primer using SPSS.* Springer.

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 60*(5), 597-609. https://doi.org/10.1177/0018720818780472

Shkoler, O. (2019). Using contemporary quantitative techniques. In P. M. W. Hackett (Ed.), *Quantitative research methods in consumer psychology: Contemporary and data-driven approaches* (pp. 22-58). Routledge.

Singh, A. K., Jyoti, V., & Rajeev, V. (2020). Understanding role of market-orientated IT competence and knowledge sharing mechanism in gaining competitive advantage. *Global Business Review, 21*(2), 418-435. https://doi.org/10.1177/0972150918824949

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security, 22*(1), 42-75. https://doi.org/10.1108/IMCS-08-2012-0045

Stockemer, D. (2019). *Quantitative methods for the social sciences: A practical introduction with examples in SPSS and Strata*. Springer International Publishing.

Such, J., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic cyber hygiene: Does it work? *Computer, 52*(4), 21–31. https://doi.org/10.1109/MC.2018.2888766

Trantopoulos, K., von Krogh, G., Wallin, M. W., & Woerter, M. (2017). External knowledge and information technology: Implications for process innovation

performance. *MIS Quarterly*, *41*(1), 287-A8. https://doi.org/10.25300/MISQ/2017/41.1.15

Triandis, H. (1977). *Interpersonal behavior*. Brooks/Cole Publishing Company.

Urhuogo, I., Addo, A., & Williams, D. (2014). The influence of information systems security on job performance: A proposed research topic. *Journal of Business Studies Quarterly, 6*(1), 191.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. *Decision Support Systems, 128*. https://doi.org/10.1016/j.dss.2019.113160

Wiafe, I., Koranteng, F. N., Wiafe, A., Obeng, E. N., & Yaokumah, W. (2020). The role of norms in information security policy compliance. *Information & Computer Security*, *28*(5), 743–761. https://doi.org/10.1108/ICS-08-2019-0095

Wilkesmann, M., & Wilkesmann, U. (2018). Industry 4.0 – organizing routines or innovations? *VINE Journal of Information and Knowledge Management Systems, 48*(2), 238-254. https://doi.org/10.1108/VJIKMS-04-2017-0019

Zhang, H., Nakamura, T., & Sakurai, K. (2019). Security and trust issues on digital supply chain. Presented at the *2019 IEEE International Conference on Dependable, Autonomic and Secure Computing,* the *International Conference on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing,* and the *International Conference on Cyber Science and Technology Congress*, 338-343. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00069