2023

Cyber Risk Management from a Resource Advantage Perspective

Komlan Seyram Ahavi

CYBER RISK MANAGEMENT FROM A RESOURCE ADVANTAGE PERSPECTIVE

By

Komlan Seyram Ahavi

A Dissertation

Presented in Partial Fulfillment of Requirements for the

Degree of

Executive Doctor of Business Administration

in the

Crummer Graduate School of Business, Rollins College

2023

Acknowledgments

I would like to first thank God for the health and strength received throughout these last three years. I thank my wife for her unconditional support during the entire process, and my daughter who took it upon herself to remind me often if I did my homework. I am grateful for their sacrifice and enduring the countless family times that I missed.

Thank you, Dr. Marshall, for giving me the opportunity to pursue this program and supporting my passion for strategic risk management throughout the program. Thank you, Dr. Walkup, Dr. Yoho, and Dr. Hair, for your support and great insights. You challenged my thought processes and shared your experience with me, which I value dearly. I cannot thank you enough, Dr. Kizer, for the inspiration you have been and your engagement in my development as an engaged scholar.

Abstract

The cyber risk management system has become a top priority for organizations in the global economy, and the internet and digitalization have changed how people work and live, making it essential to manage cyber risks effectively. However, many organizations find it difficult to establish an optimal cyber risk management system due to a lack of a clear understanding of their current level of security, insufficient budget, limited skills, and knowledge, and/or lack of technical expertise. Importantly, risk management is a complex process that requires an organization to establish a comprehensive risk management system to manage its cyber risks. Identifying the right framework and achieving an optimal return on investment in their cyber risk management system is a key challenge for organizations today. Managing cyber risks requires substantial resources of the firm and resource allocation could affect cybersecurity readiness. The research will use a survey to measure the risk appetite, risk tolerance, resource allocation, company size, technology wariness level, and cyber security readiness of respondents' organizations to understand each construct's relationship with resource allocation and cyber security readiness. Targeted respondents are risk management, internal audit, and information technology governance seniors. Using cross-sectional regression, this paper finds that all variables, but company size have significant effects on resource allocation and its effect on cybersecurity readiness.

Keywords: Risk management, risk management system, optimal return on investment, cyber risk management system, and risk appetite.

Table of Contents

Copyright Page ii

Acknowledgements iii

Abstract iv

Table of Contents v

List of Tables vii

List of Figures ix

CHAPTER 1 – INTRODUCTION 1

Background of Study 1

CHAPTER 2 – LITERATURE REVIEW 5

Resource Advantage Theory (RAT) 5

Cyber Risk Management System 8

Technology Acceptance Model (TAM) 8

Dynamic Risk Management (DRM) 12

Research Hypotheses 14

Conceptual Model 19

CHAPTER 3 – METHODOLOGY 20

Study Design 20

Participants 21

Survey Design 21

Survey Administration Procedures 23

Analytics Procedures 23

CHAPTER 4 – RESULTS, DATA ANALYSIS, AND FINDINGS 27

Participant Demographics 27
Company Demographics 30
Factor Analysis Results 33
Resource Allocation 33
Cybersecurity Readiness 34
Technology Wariness 34
Hypothesis 1 35
Hypothesis 2 37
Hypothesis 3 40
Hypothesis 4 43
Hypothesis 5 48
Hypothesis 6 52
CHAPTER 5 – CONCLUSIONS, LIMITATIONS, AND FUTURE RESEARCH 54
References 63
Appendix A 70
Appendix B 71

List of Tables

Table Page

1. Codification Framework Process 22
2. Regression Equations 25
3. Participant Familiarity with their Company's IT Security Technologies and Services 27
4. Department 28
5. Role 29
6. Position 30
7. Company Size 31
8. Industry 32
9. Model Summary – Risk Appetite as a Predictor for Cybersecurity Readiness 36
10. Statistical Significance – Risk Appetite as a Predictor for Cybersecurity Readiness 37
11. Coefficients – Risk Appetite as a Predictor for Cybersecurity Readiness 37
12. Model Summary – Risk Appetite as a Predictor for Resource Allocation 39
13. Statistical Significance – Risk Appetite as a Predictor for Resource Allocation 39
14. Coefficients – Risk Appetite as a Predictor for Resource Allocation 39
15. Model Summary – Resource Allocation as a Predictor for Cybersecurity Readiness 42
16. Statistical Significance – Resource Allocation as a Predictor for Cybersecurity Readiness 42
17. Coefficients – Resource Allocation as a Predictor for Cybersecurity Readiness 43
18. Model Summary – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness 44

19. Statistical Significance – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness 44
20. Coefficients – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness 45
21. Percentile Groups – Technological Wariness 45
22. Model Summary – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation 48
23. Statistical Significance – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation 49
24. Coefficients – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation 49
25. Percentile Groups – Risk Tolerance 50
26. Model Summary – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness 52
27. Statistical Significance – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness 53
28. Coefficients – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness 53

List of Figures

Figure Page

1. Conceptual Model for Study 20
2. Normal P-P Plot of Regression Standardized Residual Dependent Variable: Cybersecurity Readiness; Independent Variable: Risk Appetite 36
3. Normal P-P Plot of Regression Standardized Residual Dependent Variable: Resource Allocation 38
4. Normal P-P Plot of Regression Standardized Residual Dependent Variable: Cybersecurity Readiness; Independent Variable: Resource Allocation 41
5. Cybersecurity Readiness by Resource Allocation by Technology Wariness 47
6. Resource Allocation by Risk Appetite by Risk Tolerance 51

CHAPTER 1 — INTRODUCTION

Background to the Study

The cyber threat landscape is changing rapidly, and organizations worldwide are investing in cyber risk management to provide the best coverage against cyber threats. A threat is an entity whose activities can cause harm to a person or organization (Mateski et al., 2012). Companies in countries such as the United States, Ireland, France, Germany, Spain, Belgium, the Netherlands, and the UK spent as much as 24% of their information technology budget on cyber security investment in 2022, which was as low as 12% in 2020 (Statista, 2022). In the United States, there were 817 cybercrime incidents in 2022, which impacted over 53 million people, and the data shows that California, where most technology companies are concentrated, was the subject of the largest number of cyber-attacks (Johnson, 2021; Statista, 2022). Data breaches expose the personal information of millions of customers. For example, the data breach of CAM4 in March 2020 exposed nearly 11 million consumer records (Johnson, 2021). The CAM4 data breach exposed information such as full names, email addresses, sexual orientation, address IP, email correspondence transcripts, payment logs and password hashes (Tunggal, 2023). Additionally, the financial sector's informatic systems are the most targeted by phishing attacks with 23.6% of global incidents in the first quarter of 2022 (Statista, 2022). Cyber-attacks aim to gain access to organizations or individuals information systems to either steal information and/or

harm the system itself. They are reputational risks and can cause financial loss due to lawsuits, loss of confidence from investors and consumers, and damage control (Havakhor et al., 2020). They can also disrupt operations and cause further financial loss or threaten the survival of the firm (Havakhor et al., 2020).

Cyber security readiness involves planning and preparing for cyber risk events. It involves identifying specific risks, determining their impact on the organization, and finding ways to reduce or eliminate those risks. Cyber security readiness also includes developing a process that allows the organization to respond quickly and effectively if an incident occurs. It must be integrated into every aspect of a business and handled by everyone, from everyday business staff to information technology (IT) professionals to senior executives.

Cyber risk management is challenging for organizations because it requires understanding their business processes, value chains and information flows, and operating environment. Good cyber risk management requires up-to-date knowledge about the latest attacks and vulnerabilities and understanding the impact of those attacks on different aspects of the business. The increasing number of cyber security incidents and their high costs have compelled organizations to take cyber risks seriously. Organizations have started investing in cyber risk management solutions to mitigate these risks and improve their security posture. They do so by adopting cyber security frameworks and investing in technology that protects their information assets. However, it has been found that most of these solutions or frameworks are not designed to support an optimal cyber risk management process. The lack of insight into cyber threat metrics and the lack of maturity in the adoption of the cyber security frameworks can reduce the effectiveness of the cyber risk management program (Armenia et al., 2021). The continuous evolution of technology and the rapid growth of the internet, mobile devices, and

social media have created an increasingly connected world and an environment where cyber-attacks are becoming more sophisticated and damaging, causing firms to constantly improve their security, technology, and train staff members, which can create the scarcity of appropriate resources including knowledgeable staff, budget, and time to implement a comprehensive cyber risk management program (Kraaijenbrink et al., 2010). Organizations often cannot accurately assess their current level of risk exposure due to a lack of visibility into their networks and systems. Tohidi (2011) states that cyber security is often seen as a technical issue and, therefore, deferred to operational levels. As such, there is often little, or no attention paid to it at the highest levels of an organization to ensure that cyber risks are adequately integrated with the organization's business strategy. Many organizations do not allocate sufficient resources towards managing their cyber risks properly because they set their business goals and let IT professionals find ways to align with them. Significantly, organizations often struggle to accurately assess their overall exposure and determine how much cyber security investment they need. This often results in inadequate budgets for this purpose by these organizations (Armenia et al., 2021).

Importantly, a lack of training can be one of the major challenges organizations face when trying to implement a cyber risk management system, and this is because many companies do not have dedicated teams for cyber security and are forced to work with existing employees who may not be properly trained or equipped for such tasks. As such, it can be difficult for these employees to manage security risks effectively and efficiently, especially if they do not possess adequate knowledge about computer systems and networks (Armenia et al., 2021; Servaes & Tamayo, 2021).

With the increasing use of mobile devices and cloud services by employees, there is an increased risk of information leakage and data loss due to human error. This results in inadequate protection against these threats, leading to serious consequences if hackers penetrate the organization's network (Tohidi, 2011). This is exacerbated by the fact that many organizations have multiple IT systems that are integrated or linked, making it difficult for them to see how all these systems interact with each other or depend on one another for functionality (Akinwumi et al., 2017).

Although the literature points to several factors causing organizations' shortcomings in their cyber security readiness objectives, it fails to propose solutions to help organizations navigate their risk environment from a resource allocation perspective. It is important to note that the challenges listed above are all related to an organization’s resources and resource management. The literature does not link resource allocation to risk appetite and risk tolerance, which are all strategy-level concepts, and their effects on cyber security readiness. Cyber risk being from the domain of technology, the literature does not link technology wariness and company size (reflecting the resource capacity of the organization) to resource allocation and its effect on cyber security readiness.

This research seeks to understand ways in which resource allocation is linked to an organization’s challenges to establish mature cyber risk management programs by asking the following questions: First, does an organization's risk appetite impact its ability to allocate the right resources to its cyber security readiness? Second, can firms achieve a mature cyber security framework adoption regardless of the resources available to them?

CHAPTER 2 — LITERATURE REVIEW

Resource Advantage Theory (RAT)

One cannot discuss strategy without referring to resource management and vice versa. Organizations globally compete against each other in their respective industries to obtain the largest possible market share and optimize their profits. These companies tend to face the same challenges but possess different resources and capabilities to reach their goal. Each organization uses various strategies to optimize their resources to have an advantage over their competitors. The resources advantage theory derives from the resource-based view of the firm (RBV), which seeks to analyze firms' performances through their resources (Wernerfelt, 1984). Based on the premises of the RBV, firms can achieve a competitive advantage over their competitors by using the resources they have optimally and/or improving them through innovation (Day, 1994; Porter, 1990).

The resource advantage theory (RAT) is a model that attempts to explain the sustainability of competitive advantage and suggests that firms can achieve a sustainable competitive advantage with access to unique resources unavailable to competitors (Hunt, 1999). The first component focuses on creating or capturing resources that can be used to gain a competitive advantage. These resources include technological expertise, skilled employees, patents, and brands that enable organizations to produce superior products and services

compared to their competitors in the market (Malhotra, 2017, pp. 153-154). The next component involves integrating these resources into one system to be combined and aligned for optimal efficiency and effectiveness. This step helps organizations achieve greater productivity through better resource utilization and increase their competitive edge over other players in the market by establishing a competitive advantage through increased quality standards and higher levels of customer satisfaction due to better service delivery systems. This final step involves deploying these integrated resources across all aspects of an organization's operations, including marketing, sales, and logistics (Thoeni et al., 2016).

The RAT argues that firms compete based on managing resources effectively (Malhotra, 2017). This includes managing tangible resources such as money and people, and intangible factors such as information and reputation. It also emphasizes that firms will use these resources differently depending on their situation. Some firms may focus on investment in human capital, while others may focus on investment in physical or financial capital. The RAT defines an organization's competitive advantage in terms of its ability to gain access to scarce resources at lower costs than its competitors (Armenia et al., 2021).

According to the RAT, firms gain a competitive advantage by strategically allocating their available resources in ways that create value for customers and allow them to capture that value through increased revenues or reduced costs (Thoeni et al., 2016). The theory may be applied to a business's cyber risk management system. As modern business requires a certain level of technology use, cyber risk management becomes part of the business function and is necessary to protect the firm’s technology assets. As a business function, organizations will dedicate resources to their cyber security effort. Such resources should be managed optimally to ensure the effectiveness of cyber risk management (Srinidhi et al., 2015).

The RAT views organizational resources as important for understanding why some people in organizations are more effective than others. According to Thoeni et al. (2016), a person's ability to lead comes from their ability to use the various resources available within the organization. If someone can use these resources effectively, they will be a good leader. However, if someone does not have access to these resources, they will not be able to demonstrate leadership abilities. According to this theory, there are several types of resources: informational, financial, physical, legal, organizational, human, and relational (Malhotra, 2017). Informational resources include data about the organization's goals and problems and knowledge about how to achieve them efficiently; financial resources refer to money available for use within an organization; human resources include employees' skills and competencies required for performing tasks successfully; physical refers to infrastructures; legal refers to the organization's intellectual property; relational refers to customers and suppliers; and organizational refers to culture and policies (Malhotra, 2017).

Organizations implement their cyber risk management programs based on several frameworks internationally recognized and approved in the business, technology, and risk management fields (Armenia et al., 2021). Such frameworks include policies, procedures, training, and awareness programs, as well as tools that can help assess, monitor, and improve the effectiveness of existing systems (Armenia et al., 2021; Candell et al., 2015). These frameworks also help organizations manage their risks by identifying areas where they need improvement and provide them with guidance on how best to proceed with these improvements. This paper discusses some of the implications for organizations, focusing on using RAT to develop a better understanding of what drives an organization's decision-making in cyber security resource allocation, and shows how resource allocation affects cyber security readiness.

Cyber Risk Management

The cyber risk management system is a multifaceted, complex, and dynamic system (Akinwumi et al., 2018). The cyber risk management system comprises three components: the cyber risk management framework, the organizational culture, and the human resources (Armenia et al., 2021). The cyber risk management framework comprises policies, processes, and procedures designed to structure and guide the organization's actions in managing its risks (Armenia et al., 2021). Several cyber security frameworks such as the US National Institute of Standards and Technology (NIST) framework are internationally recognized by firms and regulatory agencies and are used by organizations to manage their risks; however, the existing cyber security frameworks are rather static and do not propose a dynamic approach to cyber threat (Armenia et al., 2021). That is not to discount the importance of existing frameworks, but to insist on the need for each organization to use the resources they must adapt to their dynamic cyber threat environment. Companies should not adopt a reactive approach focusing on mitigation and recovery after an attack but seek to anticipate and prevent cyber-attacks (Mateski et al., 2012).

Dynamic Risk Management (DRM)

The constantly changing nature of a company environment introduces the theory of dynamic risk management (DRM). DRM is a theory for understanding the evolution of macroeconomic risks and how they impact financial markets (Fehle & Tsyplakov, 2005). Data reveals that systemic risk increased significantly before the global financial crisis, but it also indicates that certain types of systemic risk were more important than others in predicting financial crises (Servaes et al., 2009). In particular, the combination of credit market conditions and liquidity conditions strongly predicted financial crises during this period. DRM is a new

approach to managing risks in turbulent times (Fehle & Tsyplakov, 2005). It aims to help decision-makers deal with high uncertainty by providing them with tools to understand the sources of uncertainty and helping them manage it effectively. The importance of DRM is not restricted to banks; it has become an essential tool for any organization that operates in a turbulent environment. There is increasing evidence that companies that adopt an effective DRM strategy are better able to survive economic downturns than those that do not. Moreover, its framework allows companies to adjust their risk exposure as they learn more about their business environment (Armenia et al., 2021).

Significantly, many companies use static financial planning models that assume the future will look like the past. These models are useful for various tasks such as budgeting, financial statement analysis, and internal rate of return calculations (Purnanandam, 2008). However, they do not allow managers to adjust their risk exposure as they learn more about their business environment or strategy changes over time. Dynamic financial planning models allow managers to make these adjustments by incorporating real options theory into their modeling frameworks. Many businesses are often faced with challenges that can be addressed by investing in corporate governance risk management. The insurance industry is one such industry facing challenges in managing its corporate governance risks (Servaes et al., 2009). They must invest in corporate governance risk management systems to ensure they can meet the challenges (Servaes et al., 2009). Regulation has always been a concern for the insurance industry. Risk management has become paramount for insurers as technology advances and compliance regulations become more stringent (Servaes et al., 2009). The insurance industry faces many challenges, like fraud, bribery, and corruption (Ganapathy, 2021). In addition to these challenges, insurers are also dealing with a rapidly changing regulatory landscape that is

constantly evolving to meet new requirements (Ganapathy, 2021). Corporate governance risk management is one of the key areas that insurers need to focus on as it helps them manage their risks better and prevents them from falling prey to fraudulent activities perpetrated by their employees or third parties who work on behalf of their organizations (Aven, 2013).

The increasing level of regulation has increased compliance costs which have been passed on to customers in the form of higher premiums. In addition, many insurers have not been able to generate enough profits from their investments to meet their claims obligations and pay dividends to shareholders. This has increased pressure on corporate governance standards within the insurance industry as shareholders seek adequate investment returns while maintaining adequate capital levels (Aven, 2013). DRM does not only apply to the corporate finance functions, but it also applies to the cyber risk management function as well.

The increasing rate of cybercrime and the rising costs of cyber-attacks make it imperative for organizations to implement effective cyber risk management (Hasan et al., 2021). Challenges that organizations face when implementing cyber risk management could be alleviated if they can holistically understand factors that impact cyber security readiness (Hasan et al., 2021). First, organizations should understand their risk environment based on the business they are conducting and map/model potential threats to their businesses (Mateski et al., 2012). There are several threat modeling frameworks such as the operational threat assessment (OTA), which was developed by the Department of Homeland Security (DHS) to help federal and civilian agencies profile and anticipate threats to their security as well as developing a response model to potential threats (Mateski et al., 2012). Companies should also understand their risk appetite as it drives the level of risk they are willing to take when doing business. The Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management defines risk appetite

as the “types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value” (Martens & Rittenberg, 2020, p. 1). It is important to note that every business decision or investment carries a certain level of risk that firms should consider *vis-à-vis* of the potential return. Understanding the threat gives business leaders an idea of the risk related to their businesses, but their risk appetite will also drive their decision-making. While risk appetite is closely related to the company’s overall risk behavior, individual processes and their subsequent technology assets risks are measured through the risk rating, which rates the severity of the risk based on impact and likelihood (Boehm et al., 2019). Generally, the risk rating ranges from very high or critical to very low or low depending on the scale the firm is using (Boehm et al., 2019; Hoffmann et al., 2020). The level of controls the firm will put around cyber security will depend on the risk rating. A high-risk environment, process, or asset will require stronger cybersecurity while a low one will require less effort in terms of cybersecurity. Another factor to consider is risk tolerance, which is defined as the degree of uncertainty an organization can tolerate in pursuing its goals (Martens & Rittenberg, 2020). Risk tolerance sets a boundary not only for an organization’s risk appetite but also its overall business functions and it is a measure of the capability of the enterprise.

One of the most important challenges in cyber risk management is ensuring all stakeholders are on board with the organization's cyber risk management strategy. The lack of support from key stakeholders can lead to a failure in achieving an effective cyber risk management system. For example, employees may become complacent or even negligent in their work practices if they do not understand their role in protecting critical information assets (Marangunić & Granić, 2014). The complexity of technology and its rapid development also makes it difficult for organizations to identify the right framework and mature in its adoption

using the resources available to them. For an organization stakeholder to rally behind enhancing cyber security, they must understand the importance of it and be open to accepting the use of technology, which introduces the theory of technology acceptance.

Technology Acceptance Model (TAM)

Technology acceptance model (TAM) is a theory that aims to explain how and why people use technology (King & He, 2006). The model was based on the Theory of Reasoned Action, which suggests that an individual's behavioral intention toward using a specific technology is a function of their attitude toward it and their subjective norm (Chau, 1996). The model states that the more positive the attitude toward using the technology, the greater the intention to use it. The greater one's intention to use it, the more likely one will engage in the behavior. The greater one's behavioral intention to use it, the more likely one will use it (Jan & Contreras, 2011). TAM is a widely used model for understanding how users react to new technologies or changes in their environment. TAM assumes that users do not want to be forced into using something they do not like or understand; instead, they want to feel comfortable with, and have control over, their interactions with technology. The model posits that there are two key determinants of IT usage: *perceived usefulness*, which is defined as the extent to which a user believes that using a system will increase their chances of performing a task successfully; and *perceived ease of use*, which is defined as the extent to which a user believes that using a system will be free from effort. Perceived usefulness directly affects the intention to use, while perceived ease of use indirectly affects intention through its impact on attitude towards use. Perceived usefulness and perceived ease of use, directly and indirectly, affect actual behavior.

Although the model states that two factors must be present for an individual to adopt technology, Malhotra and Galletta, (2019) propose that *social influence* should be considered as

another factor important for technology adoption. If users perceive that these factors do not exist, they will not be motivated to learn how to use the technology or they will not continue using it after training is complete. Users need to understand how this new system will fit into their daily lives and make their lives easier, and they must have a reason they want to adopt and integrate it into their daily lives (Marangunić & Granić, 2014).

The first factor, perceived usefulness, entails the extent to which people believe a system will enhance their performance. It is assumed that people will use a product or service if they perceive it as useful and valuable. The second factor, perceived ease of use, refers to how easy people think a system will be to learn and operate. People are more likely to use a system if they think it will be easy to learn and operate rather than difficult or complex. The third factor, social influence, refers to the degree that people believe their friends and colleagues would approve if they used a particular technology or product/service (Jan & Contreras, 2011). Social influence means that the environment of the user is favorable to the use of technology (Marangunić & Granić, 2014). In other words, the use of technology is a culture. Thus, individuals are more likely to perform behaviors that others in their social network expect them to do than those not expected by others in their network. People also consider normative beliefs about how others think about this new technology before deciding whether they should accept or reject it. In addition, past behavior also affects people's decisions (Marangunić & Granić, 2014).

Three additional factors were proposed as part of the TAM: performance expectancy, effort expectancy, and facilitating conditions. Performance expectancy refers to the extent users believe using a particular technology will help them perform tasks more accurately or quickly than they could without it. High performance expectancy means that users expect to use a particular technology to improve their performance at work or school. Low performance

expectancy means that users expect no improvement in their performance when using a particular technology. Effort expectancy refers to the extent users believe using a particular technology will take less time than doing similar tasks without it. High effort expectancy means users expect less time consumption when performing tasks with technologies than without. Low effort expectancy means users expect more time consumption when performing tasks with technologies than without. Finally, facilitating conditions are conditions that make the use of technology easy or effortless (the technology is user friendly) (Marangunić & Granić, 2014).

TAM has been a useful framework for understanding many aspects of technology use and has been applied to many technologies. Importantly, TAM is one of the most widely accepted technology adoption theories and has been used to explain various types of technology user behavior, including acceptance, continuance, and abandonment. It posits that the degree to which a user will accept and use new technology is a function of perceived ease of use and usefulness. However, the model was not studied for resource allocation in its relationship with cyber security readiness. An extension to the study of cyber security will improve the understanding of how behavioral factors impact resource allocation and its effect on cyber security readiness.

Research Hypotheses

Every project a firm undertakes to make a profit carries a certain amount of risk. That profit or return is measured as a function of the risk and is called the rate of return, which helps decide if the project is worth pursuing (Belghitar & Clark, 2012). Firms need a benchmark that they can compare the rate of return to and see if it fits within the range of risk the company is willing to take to pursue a profit. Companies express that risk benchmark as their risk appetite. Risk appetite plays an important role in explaining the performance of organizations. It is

determined by the organization's board, management, and other risk seniors. Belghitar and Clark (2012) reveal that leadership risk appetite is strongly related to return volatility. Note that the return can be considered a performance measure of the firm's activities. In the same dynamic, this paper argues that leadership risk appetite affects cyber security readiness, which is a performance measure of the firm's cyber security management.

A firm with a low level of risk appetite is more likely to operate in a low-risk environment. As such, the risk rating around the company's processes will be low rated and will require only a minimum level of cybersecurity controls. For a risk rating to be low, the likelihood of the risk occurring should be low and the impact on the firm should be low as well (Boehm et al., 2019). Because the risk is likely to not occur, and even if it occurs it will be of little consequence for the firm, managers should not focus much on it. A firm with a high level of risk appetite is more likely to operate in a high risk environment, requiring a high level of controls around its business processes. A risk-seeking firm, to make high returns, will be more likely to accept more risk. However, the likelihood of the risk occurring and the impact on the firm will be high, putting the company in a precarious position, therefore, increasing cyber security controls. Therefore, it is hypothesized that:

H_1: *An elevated risk appetite will positively influence cyber security readiness*.

Risk appetite will define the number of resources leaders are willing to dedicate to cyber risk management. Cyber security readiness is important in determining how prepared an organization is to respond to cyber threats. In risk management, resources refer to staffing, equipment, software, and other intangible capabilities an organization relies on for its functioning (Benaroch et al., 2006). An organization with adequate resources will respond more effectively to a cyber-attack than one without them. A strong risk appetite indicates risk-seeking

behaviors in expectation of a high return, while risk aversion means that an organization will try hard not to lose money or assets in any way possible. In both cases, this paper recognizes that the firms are pursuing a certain level of profit. Based on hypothesis one, companies with low-risk appetite will allocate less resources to cybersecurity management as their environment and processes only require that they have a minimum level of controls. Risk seeking companies will be required to allocate more resources to cybersecurity because their environment and processes require elevated controls over cybersecurity risks. Therefore, it is hypothesized that:

H_2: *An elevated risk appetite will positively influence resource allocation.*

Resources are crucial for an organization's success. They consist of tangible assets such as buildings and equipment, and other infrastructures needed for the production and distribution of goods or services to customers. They also consist of intangible assets such as knowledge, skills, network, and reputation built over time. Day (1994) defined such intangibles as the capabilities of organizations. In a dynamic and competitive market, such capabilities will provide organizations with a competitive advantage as they possess the tools to innovate and differentiate themselves (Day, 1994). In other words, organizations with more capabilities will outperform those with less capabilities through innovation (Porter, 1990). As cyber security readiness is a performance measure of cyber security management, this dissertation argues that resource allocation can be linked directly to cyber security readiness. Cyber security management requires tangible and intangible resources just as any enterprise production unit and it is linked to the overall company performance. Firms need its capabilities not only to mitigate the risks caused by threat environments, but also to outperform competitors by reducing costs related to cyber security incidents. Therefore, it is hypothesized that:

H_3: *An elevated resource allocation will positively influence cyber security readiness.*

Technology acceptance is the degree to which a person accepts and is willing to use technology (Marangunić & Granić, 2014). The higher the technology acceptance, the more likely people will use a new technology. The technology acceptance model has been extensively used in understanding how individuals perceive and respond to new technologies. It represents a good starting point for examining how individuals perceive and respond to cybersecurity programs. Specifically, employees with high technology acceptance are more likely to engage in proactive cyber risk management activities than those with low technology acceptance. Notably, managers with high technology acceptance would allocate more resources toward risk management activities than their less affluent counterparts. As technology acceptance implies a tendency to adopt technology, this paper argues that people who feel a certain level of discomfort or insecurity around technology, technology wariness, will be less inclined to use technology. In that dynamic managers that feel a certain level of technology wariness will allocate less resources to cyber risk management, undermining their company's cybersecurity readiness. Therefore, it is hypothesized that:

H_4: *Technology wariness will weaken the relationship between resource allocation and cyber security readiness*.

Hypothesis 2 posits that an elevated risk appetite will positively influence a firm's resource allocation. In other words, firm leaders with risk-seeking behavior will allocate more resources to risk security management. However, risk appetite alone is not enough to explain this relationship. This paper explored risk tolerance, which is the degree of uncertainty an organization can tolerate in pursuing its goals (Martens & Rittenberg, 2020). In other words, it is the level of loss an organization can take or is willing to take considering that the loss may harm the company. A company needs to understand its risk tolerance level because it will help

establish a range of acceptable risks and provide guidance on how much risk should be taken. The level of risk tolerance will also help determine which tools, techniques, or strategies should be used to minimize the effects of negative outcomes. Risk tolerance was studied by several academics in the domain of individual financial literacy and investment behavior (Dickason et al., 2018). The research shows that aggressive investors have an elevated risk tolerance, while conservative investors have a low risk tolerance. Risk tolerance assumes that companies have limited capital and resources and cannot take risks that may lead to losses in those areas. It means that risk tolerance can limit the risk-seeking behavior of firms as they cannot go over their capabilities in the pursuit of profit. Hence, company risk tolerance moderates the relationship between risk appetite and resource allocation. This paper argues that firm leaders will behave in the same way influencing their companies' risk posture. In other words, a company that has an elevated risk tolerance will have high risk appetite tendencies as well. If risk appetite positively affects resource allocation, risk tolerance will strengthen that relationship. Therefore, it is hypothesized that:

H_5: *An elevated risk tolerance will strengthen the relationship between risk appetite and resource allocation*.

The number of resources available to an organization directly impacts the preparation of an organization and the level of investment it can afford regardless of the activity it is undertaking. The more resources an organization has, such as time and money, human resources, and knowledge, the more likely it is to have cybersecurity readiness programs. The relationship between resource availability and cyber security readiness is moderated by company size. Armenia et al. (2021) state that small- and mid-sized companies struggle to manage their cyber security because they have limited resources. This means that larger companies with more

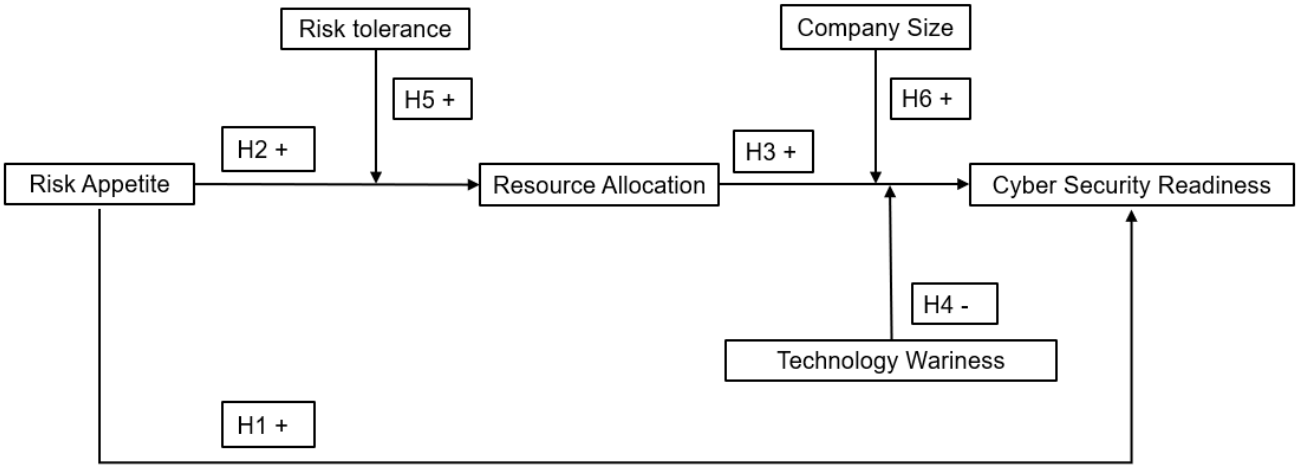
capability will allocate more resources to their cyber security management. It is then hypothesized that:

H_6: *Larger companies will strengthen the relationship between resource allocation and cybersecurity readiness*.

Conceptual Model

Figure 1

Conceptual Model for Study



CHAPTER 3 — METHODOLOGY

This research posits that the cybersecurity readiness of an organization will depend on its resource management or resource allocation. However, the resource allocation itself depends on the risk appetite posture of the firm. This paper also considers various factors that can affect resource allocation and cybersecurity readiness, specifically risk tolerance, company size, and technology wariness. By examining the relationship between cybersecurity readiness and resource allocation and resource management, this study provides insights regarding how companies might better prepare themselves and guard against cybersecurity threats.

Study Design

The current study employed an online survey to collect data measuring risk appetite, risk tolerance, resource allocation, company size, technology wariness, and cyber security readiness. Because this research was aimed at assessing the relationships between a variety of variables and was interested in examining the moderating effects of certain factors, a quantitative-based survey was the best structure for collecting the data. By relying upon quantitative rather than qualitative data, it is reasonable to include a larger number of participants and the significance of relationships within the hypotheses can be assessed statistically. Collecting data through an online survey was determined to be the most effective collection method because internet-based

surveys are more efficient, faster, and less expensive than other alternatives such as phone or mail-based surveys (Schonlau et al., 2002).

Participants

Participants included IT governance, internal audit, and risk management seniors across several industries, with each participant representing a company (n = 200). All participants were screened at the beginning of the survey to ensure that respondents were relevant to the level of decision-making that the research seeks (Appendix A). The questions addressed respondents' experience and familiarity with their company's cybersecurity as well as their position, role, and responsibilities within the organization. The screening questions also gathered information about the company industry and the company's IT budget construction (i.e., whether the IT security budget is separate or contained within the overall IT budget).

Survey Design

As there are several risks involved with the activities of organizations, this paper focuses only on cyber security risks. Several methods are used in finance to measure the risk appetite of organizations through their leaders. For example, a CES's risk appetite is captured through his/her wealth, education, time in the role, board experience, and age (Belghitar & Clark, 2012, p 4). For this research, another method will be used to collect risk appetite data, by assessing the sentiment of risk and technology leaders about the risk posture of their organization using a 9-point Likert scale. The scale ranges from one to nine, with one meaning the organization has a very low risk appetite and nine meaning that it has a high-risk appetite. The same method as risk appetite is used to collect data for risk tolerance. A 9-Point Likert scale, with one meaning the organization has a very low risk tolerance and nine meaning that it has a high-risk tolerance.

Cyber security readiness is measured in terms of the firm cyber security maturity. Cyber security management uses various frameworks individually or combined depending on the firm's resource capacity or cyber security management maturity. The main frameworks used are the NIST and the International Standards Organization 2 7002 (ISO 27002). The research used the Cyber Security Maturity Assessment methodology to measure organizations' cyber security maturity as presented in Table 1 (Sulistyowati et al., 2020). Each item within each framework is rated on a 9-point Likert scale to assess the level of maturity of the organization's use of the cyber security frameworks.

Table 1

Codification Framework Process

No	Model/Categories	ID
	NIST	
1	Asset Management	A1
2	Business Environment	A2
3	Governance	A3
	ISO 27002	
1	Information Security Policies	B1
2	Organization of information security	B2
3	Human resources security	B3

Technology wariness can be measured using two of the national technology readiness survey dimensions, which measures the discomfort, and the insecurity people feel toward technology (Parasuraman, 2000). However, this study focuses on the company. Using the survey

model and adapting it to collect company-level data, this study collected data for each dimension. The participants were asked about the sentiments of their organizations' tendencies toward technology. For each of the four dimensions, a 9-point Likert scale was used.

Company size is often classified as small, medium, or large (Hörisch et al., 2014). The number of employees or revenue is used to make a such classification. This paper used the number of employees classification for this study. Note that small firms consist of less than 50 employees, medium companies consist of 50 to 249 employees, and large firms have more than 250 employees (OECD, 2017). This classification varies per agency and does not fit the purpose of this study. As such this paper used a scale of the number of employees ranging from less than 500 to more than 75,000 to accurately measure the size of firms considering that some multinational companies employ more than 75,000 people.

Survey Administration Procedures

The survey was administered online by *Alchemer*, a third-party research company that maintains a database of participants for studies such as this one. The researcher elected to use a third-party company for data collection because companies such as this have access to populations of respondents that are professionals in relevant fields and, thus, are well-suited for participating in this study.

Analytic Procedures

In total, the survey contained 22 questions aimed at capturing data specific to the hypotheses included in this study (Appendix B). Except for Company Size, all survey questions designed to capture data for the variables included in the model had responses set as a 9-point Likert scale. The Company Size variable gave participants ranges of headcounts from which to choose. All analyses of the above variables were conducted using Statistical Packages for the

Social Sciences (SPSS), which is a commonly relied upon computational program for quantitative data analysis (Okagbue et al., 2021). Two of the questions relating to Technology Wariness were worded negatively in the survey and, prior to analysis, the responses to these two questions were reverse coded to allow for consistent interpretation with the rest of the variables.

The variables Risk Appetite, Risk Tolerance, and Company Size were measured using a single survey question for each topic. For the variables Resource Allocation, Technology Wariness, and Cybersecurity Readiness, respondents were asked to answer multiple questions directed at various components of each of these variables. These were examined using exploratory factor analysis to determine whether the survey questions for each variable were measuring the same construct. Factor analysis is a statistical methodology that can be applied in situations where it is helpful to understand how responses to related survey questions relate to one another. This can be helpful both for consolidating data into a single factor for use in multiple regression or for identifying survey questions that do not provide a clear picture of the data (Shrestha, 2021).

Common factor analysis rather than Principal Components Analysis was used because it is more fitting for identifying a latent factor structure within the variables examined and maximizing the fit of correlations (Fabrigar et al., 1999). An oblique rotation (Jennrich & Sampson, 1966) was used because the intent of the oblique rotation is to simplify the factors and is based on the belief that the factors would be correlated (Child, 2006).

Within a factor analysis, it is important that Bartlett's test of sphericity (Bartlet, 1954) is used to make sure that the correlation matrix was not based on random chance and the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) Statistic (Kaiser, 1974) is confirmed to be

approaching or above 0.50. These assumptions were relied upon for the factor analyses in this research.

In cases where the factor analysis was supportive of combining survey questions for a given variable, the survey responses for each individual respondent were averaged together. Once the factors were analyzed for the three variables with multiple survey questions, the variables were analyzed for skew and kurtosis using a 2.1 cutoff for skew and a 7.1 cutoff for absolute kurtosis (West et al. 1996). No variable exhibited skew or kurtosis outside of normality and no highly deviant cases were flagged through this analysis, so the entirety of the dataset was included in the analysis. Additionally, a z-score was calculated for each variable. No z-scores outside of the standard range of -3.0 and 3.0 emerged, further confirming that the data does not contain outliers.

Once the dataset was determined to not be violating normality, linear regression was used to assess the relationships between variables postulated in each hypothesis. Linear regression was selected as the analysis technique because it is well-suited for assessing the relationships between quantitative dependent and independent variables and can also be used to determine whether mediating or moderating effects are present within the relationships (Berger, 2003).

Regression equations for each hypothesis were developed to test the relationships of the variables postulated within each hypothesis. Table 2 delineates the regression equations for the hypotheses examined in this study.

Table 2

Regression Equations

Hypotheses	Equation
H1	Y_1(Cybersecurity Readiness) = $B_0 + B_1 X_1$(Risk Appetite)
H2	Y_2(Resource Allocation) = $B_0 + B_1 X_1$(Risk Appetite)
H3	Y_1(Cybersecurity Readiness) = $B_0 + B_2 X_2$(Resource Allocation)
H4	Y_1(Cybersecurity Readiness) = $B_0 + B_2 X_2$(Resource Allocation) + $B_3 X_3$(Technology Wariness) + $B_2 X_2 B_3 X_3$ (Resource Allocation x Technology Wariness)
H5	Y_2(Resource Allocation) = $B_0 + B_1 X_1$(Risk Appetite) + $B_4 X_4$(Risk Tolerance) + $B_1 X_1 B_4 X_4$ (Risk Appetite x Risk Tolerance)
H6	Y_1(Cybersecurity Readiness) = $B_0 + B_2 X_2$(Resource Allocation) + $B_5 X_5$(Company Size) + $B_2 X_2 B_5 X_5$ (Resource Allocation x Company Size)

CHAPTER 4 — RESULTS, DATA ANALYSIS, AND FINDINGS

Participant Demographics

The survey included 398 participants of which 182 were disqualified and 15 partially completed the survey. Because the study is focused on cybersecurity management and is targeting risk management seniors, as well as audit and technology seniors, the researcher included the following disqualifying screening questions:

- What organizational level best describes your current position?
- Which department do you primarily work within at your organization?
- How familiar are you with your organization's management of IT security technologies and services?
- Please check one of the activities that you see as part of your job or role.
- Does your job involve securing or overseeing the security of your organization's information systems or IT infrastructure (including auditing)? Please mark yes even if your job is only partially involved in the security function.

Any responses that do not satisfy the parameters set by the researcher will terminate the survey and the participant responses will not be included in the sample. Of the 201 remaining participants, one missed some of the questions and was removed from the data. Finally, there were 200 participants who qualified for and completed all survey questions. All were based in

the United States, and all stated that their jobs involve securing or overseeing the security of their organization's information systems or IT infrastructure (including auditing). When asked about their level of familiarity with their organization's management of IT security technologies and services, nearly all stated that they were either familiar (n = 37) or very familiar (n = 152). Table 3 details the participants' familiarity with their organization's management of IT security technologies and services.

Table 3

Participant Familiarity with their Company's IT Security Technologies and Services

Response	**Percent**
Not familiar	0% *(n = 0)*
Slightly familiar	2.5% *(n = 5)*
Moderately familiar	3.0% *(n = 6)*
Familiar	18.5% *(n = 37)*
Very familiar	76.0% *(n = 152)*

Respondents were asked to report on the departments in which they work as well as their roles and positions within the organization. Most respondents work within their company's Information Technology department (n = 149) and their specific roles within their department were most commonly IT Management (n = 94) or IT Security (N = 70). Participants' positions

were most often reported to be either Directors (n = 83) or Senior Managers (n = 64). Tables 4, 5, and 6 highlight participants' department, role, and position within the company, respectively.

Table 4

Department

Response	**Percent**
Cybersecurity	25.5% (n = 51)
Information Technology	74.5% (n = 149)

Table 5

Role

Response	**Percent**
Compliance/Audit	0.5% *(n = 1)*
Database Management	1.0% *(n = 2)*
Infrastructure/Application Development	3.0% (n = 6)
Infrastructure/Application Security	3.0% *(n = 7)*
IT Management	47.0% *(n = 94)*
IT Security	35.0% *(n = 70)*
Network Engineering	2.0% *(n = 4)*
Quality Assurance	0.5% *(n = 1)*
Risk Management	1.5% *(n = 3)*
Security Architecture	5.5% *(n = 11)*
Other	0.5% ***(n = 1)***

Table 6

Position

Response	**Percent**
Manager	18.5% *(n = 37)*
Senior Manager	32.0% *(n = 64)*
Director	41.5% *(n = 83)*
Associate Vice President	2.5% *(n = 5)*
Vice President	5.5% *(n = 11)*
Other	0.0% *(n = 0)*

Company Demographics

In addition to identifying characteristics of the participants, details regarding the company for which the participants work were also gathered. The survey asked respondents to identify the size of their company, based on employee headcount. Sixty-three percent of respondents work for companies with a headcount of 5,000 employees or fewer (n = 126). Table 7 outlines their responses in more detail.

Table 7

Company Size

Response	**Percent**
Less than 500	13.0% ***(n = 26)***
500-1000	25.5% ***(n = 51)***
1001-5000	24.4% ***(n = 48)***
5001-10000	15.5% ***(n = 31)***
10001-25000	11.0% ***(n = 22)***
25001-50000	6.5% ***(n = 13)***
50001-75000	2.5% ***(n = 5)***
More than 75000	2.0% ***(n = 4)***

When participants were asked whether their company's IT security budget is a part of or separate from the overall IT budget, 79% respondents indicated that the security budget is part of their overall IT budget (n = 158) with the remaining 21% stating that their company has a

separate budget for their IT security (n = 42). Additionally, when asked about industry, most respondents indicated that the company they work for is in Technology and Software (n = 85) or Industrial and Manufacturing (n = 33). Table 8 shows the breakdown of companies by their industry.

Table 8

Industry

Response	**Percent**
Agriculture & Food Services	0.5% *(n = 1)*
Business Management	0.5% *(n = 1)*
Communications	1.0% *(n = 2)*
Consumer Products	4.0% *(n = 8)*
Defense & Aerospace	1.5% *(n = 3)*
Education & Research	4.0% *(n = 8)*
Energy & Utilities	0.5% *(n = 1)*
Financial Services	5.5% *(n = 11)*

Table 8

Industry

Response	Percent
Health & Pharmaceutical	7.0% *(n = 14)*
Hospitality	1.5% *(n = 3)*
Industrial and Manufacturing	16.5% *(n =33)*
Public Sector	0.5% *(n = 1)*
Retail	7.0% *(n = 14)*
Services	5.0% *(n = 10)*
Technology & Software	42.5% *(n = 85)*
Transportation	2.5% *(n = 5)*

Factor Analysis Results

To consolidate survey questions into easily testable variables for analysis in this research, in cases where participants were asked to respond to more than one survey question related to a single variable, a factor analysis was employed. As aforementioned, three of the variables examined in this study include multiple survey questions aimed at extracting information from participants that is relevant to that variable.

Resource Allocation

The Resource Allocation independent variable included three survey questions. Exploratory factor analysis was used to determine the reasonability of combining all three Resource Allocation survey questions into a single Resource Allocation variable. The factor analysis KMO statistic was calculated to be 0.705, which is well above the 0.50 recommended threshold and the Bartlett's Test of Sphericity yielded a significant result ($\chi^2 = 233.242$, df = 3, $p < 0.01$). These tests indicated that the factor analysis is appropriate for interpretation.

The factor analysis results yielded a single factor that accounts for 74.8% of the variance in the three Resource Allocation survey questions with an Eigenvalue of 2.243. Because all three of the survey questions are appropriate for inclusion in a single factor, the respondents' answers to each survey question were averaged together to create a single variable representing Resource Allocation.

Cybersecurity Readiness

The dependent variable, Cybersecurity Readiness included six survey questions aimed at assessing various components of cybersecurity readiness. With a KMO statistic of 0.888 and a significant Bartlett's Test of Sphericity ($\chi^2 = 631.612$, df = 15, $p < 0.01$), the factor analysis is appropriate for interpretation. The exploratory factor analysis yielded results indicating that a single Cybersecurity Readiness variable is reasonable. All six of the survey questions were found to be significantly correlated at the $p < 0.001$ level. With an Eigenvalue of 3.960, the factor analysis found that 66.008% of the variance in the Cybersecurity Readiness survey questions can be explained in a single factor that combines all six survey questions. As a single factor emerged for this variable, respondents' answers to the six Cybersecurity Readiness

questions were averaged together to create a single Cybersecurity Readiness score for each respondent.

Technology Wariness

The moderating variable, Technology Wariness included two survey questions addressing participants' experience with their company's discomfort and insecurity around technology. The questions focused on discomfort and insecurity in adopting cybersecurity technology. The KMO test yielded a value of 0.500, which is acceptable for this analysis, and the Bartlett's Test of Sphericity is significant ($\chi^2 = 236.943$, df = 1, $p < 0.01$). This indicates that the factor analysis results can be considered and applied to the Technology Wariness survey questions. The factor has an Eigenvalue 1.836, and this single factor can explain 91.795% of the variance within the questions. With this confirmed, respondents' answers to the discomfort and insecurity questions were averaged together to create a Technology Wariness score for each respondent.

Hypothesis 1

***H_1**: An elevated risk appetite will positively influence cybersecurity readiness.*

To assess the relationship between respondents' assessment of their company's risk appetite and their cybersecurity readiness, the researcher conducted a regression analysis. Prior to conducting the multiple regression, the researcher assessed the data to confirm that no assumptions were violated. Figure 2 demonstrates that the data points are arranged within a reasonably straight line, a desired condition for conducting a multiple regression.

The regression analysis examining respondents' assessment of their company's risk appetite and their cybersecurity readiness yielded significant results. As seen in Table 9, 14.6 percent of the variance in cybersecurity readiness can be explained by companies' risk appetite. Additionally, Table 10 demonstrates that the predictive relationship is significant at a level of $p <$

.001. When examining H_1, the data suggests that a company's risk appetite is predictive of their cybersecurity readiness. The data indicates that companies with a higher risk appetite tend to exhibit more advanced cybersecurity preparedness ($r = .382$, $p < .001$), which supports H1. The coefficients in Table 11 demonstrate that for every 1 unit increase in risk appetite, the data shows an increase of .230 in cybersecurity readiness. Companies with higher risk appetite operate in a high-risk environment thus needing stronger controls and focus on cybersecurity readiness to mitigate their risks. The resulting regression equation is:

Cybersecurity Readiness = 5.764 + .230(Risk Appetite)

Figure 2

Normal P-P Plot of Regression Standardized Residual Dependent Variable: Cybersecurity Readiness; Independent Variable: Risk Appetite

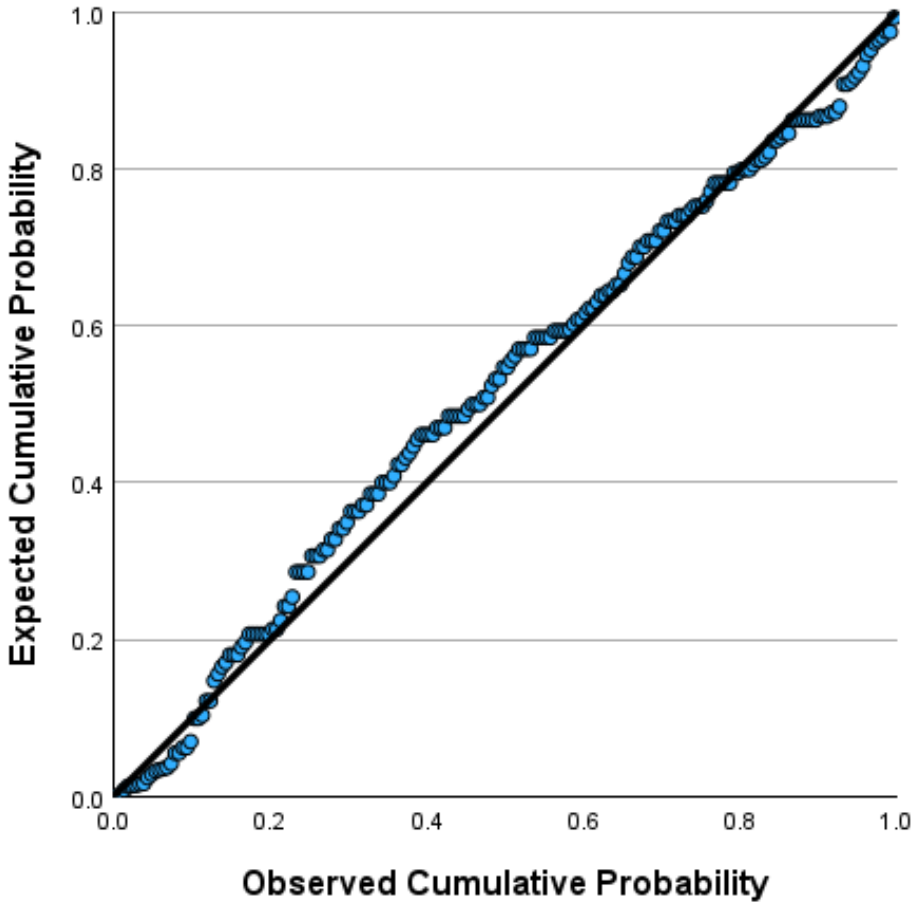


Table 9

Model Summary – Risk Appetite as a Predictor for Cybersecurity Readiness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.382	.146	.141	1.06877	.146	33.770	1	198	<.001

Table 10

Statistical Significance – Risk Appetite as a Predictor for Cybersecurity Readiness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	***Regression***	38.574	1	38.574	33.770	<.001
	Residual	226.169	198	1.142		
	Total	264.743	199			

Table 11

Coefficients – Risk Appetite as a Predictor for Cybersecurity Readiness

		Unstandardized Coefficients		Standardized Coefficients		
Model		**B**	**Standard Error**	**Beta**	**t**	**Significance**
1	***(Constant)***	5.764	.254		22.717	<.001
	Risk Appetite	.230	.040	.382	5.811	<.001

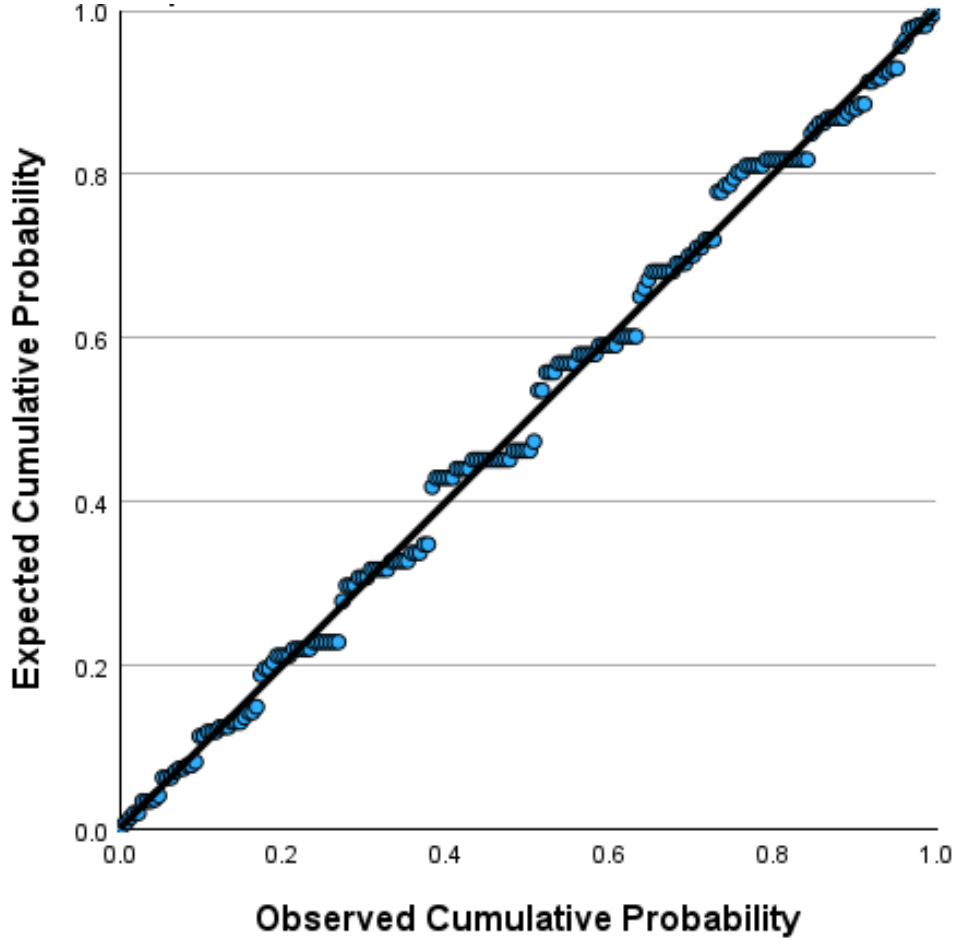
Hypothesis 2

***H_2**: An elevated risk appetite will positively influence resource allocation.*

To examine the connection between respondents' company's resource allocation for technology and their company's tolerance for risk, a regression analysis was carried out by the researcher. Before proceeding with the multiple regression, a careful examination of the data was conducted to ensure that none of the underlying assumptions were violated. As depicted in Figure 3, the data points are reasonably aligned in a straight line, which is a favorable condition for performing a multiple regression analysis.

Figure 3

Normal P-P Plot of Regression Standardized Residual Dependent Variable: Resource Allocation



The regression analysis focused on the relationship between a company's resource allocation and risk appetite for technology yielded noteworthy findings. As presented in Table 12, a considerable 24.5% of the variability in resource allocation can be accounted for by a company's risk appetite. Furthermore, Table 13 highlights the significance of this predictive relationship, with a p-value less than .001. In the context of H_2, the data strongly suggests that a company's risk appetite is indeed a predictive factor for its resource allocation. Based on the regression results, it appears that companies that have an increased appetite for risk also have more resources allocated to technology ($r = 0.495$, $p < .001$). The coefficients in Table 14 further

illustrate that for each incremental unit increase in risk appetite, there is a corresponding 0.305 unit increase in resource allocation. The resulting regression equation is:

Resource Allocation = 5.328 + .305(Risk Appetite)

In this equation, 5.328 is the constant and represents the value of resource allocation if risk appetite was zero. The positive sign of the coefficient .305 indicates a positive slope, which explains the increase in resource allocation when risk appetite increases.

Table 12

Model Summary – Risk Appetite as a Predictor for Resource Allocation

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.495	.245	.241	1.02553	.245	64.308	1	198	<.001

Table 13

Statistical Significance – Risk Appetite as a Predictor for Resource Allocation

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	***Regression***	67.634	1	67.634	64.308	<.001
	Residual	208.241	198	1.052		
	Total	275.875	199			

Table 14

Coefficients – Risk Appetite as a Predictor for Resource Allocation

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Standard Error	Beta	t	Significance
1	***(Constant)***	5.328	.243		21.881	<.001
	Risk Appetite	.305	.038	.495	8.019	<.001

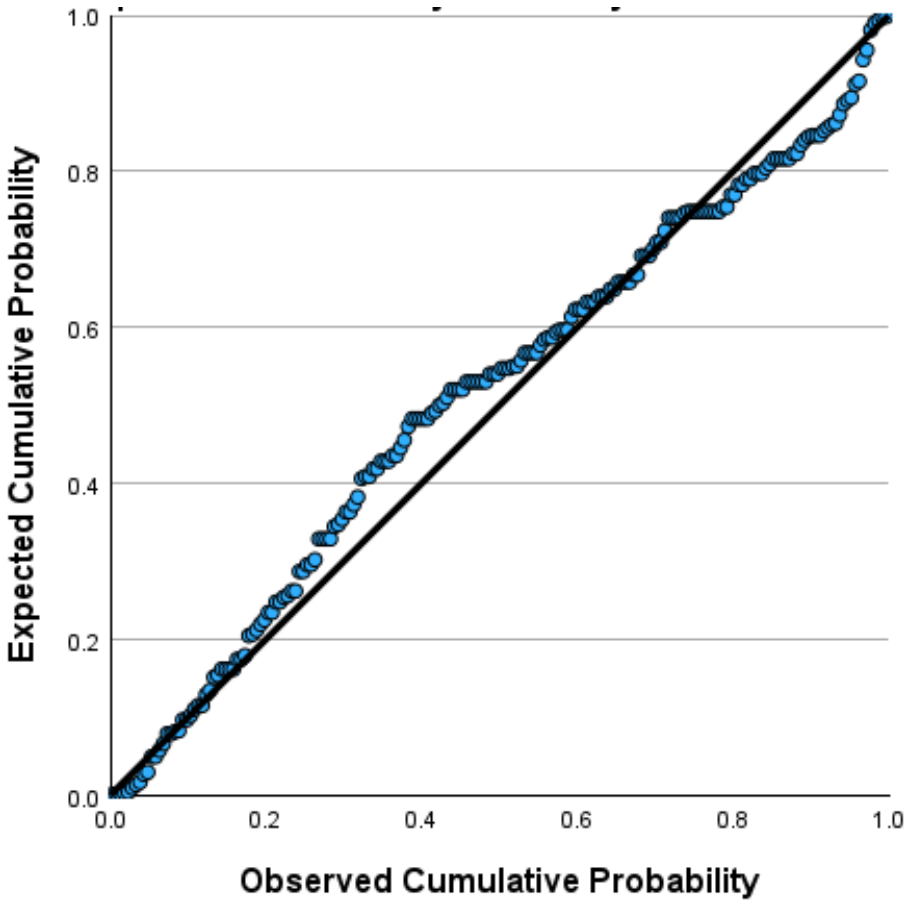
Hypothesis 3

***H_3**: An elevated resource allocation will positively influence cybersecurity readiness.*

To investigate the relationship between the allocation of resources for technology within respondents' companies and their corresponding cybersecurity preparedness, a regression analysis was conducted. As with Hypotheses 1 and 2, prior to proceeding with the multiple regression analysis, a data examination was undertaken to verify that none of the fundamental assumptions had been breached. As illustrated in Figure 4, the data points exhibit a reasonably linear alignment, which confirms the appropriateness of conducting a multiple regression analysis.

Figure 4

Normal P-P Plot of Regression Standardized Residual Dependent Variable: Cybersecurity Readiness; Independent Variable: Resource Allocation



The regression analysis, which focused on the correlation between a company's allocation of resources and its readiness in terms of cybersecurity, has yielded significant findings. As displayed in Table 15, a substantial 54.1% of the variance in cybersecurity readiness can be explained by a company's investment in technology resources. Furthermore, Table 16 underscores the significance of this predictive relationship, with a p-value of less than .001. In relation to H_3, the data strongly suggests that a company's allocation of resources is a predictive factor for cybersecurity readiness. Based on the results of the regression analysis, it becomes

evident that companies with higher resource allocation also exhibit higher scores in terms of cybersecurity readiness ($r = 0.735$, $p < .001$). The coefficients in Table 17 further clarify that for each incremental unit increase in resource allocation, there is a corresponding 0.720 unit increase in cybersecurity readiness. The resulting regression equation is:

Cybersecurity Readiness = 1.991 + .720(Resource Allocation)

Table 15

Model Summary – Resource Allocation as a Predictor for Cybersecurity Readiness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.735	.541	.539	.78353	.541	233.238	1	198	<.001

Table 16

Statistical Significance – Resource Allocation as a Predictor for Cybersecurity Readiness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	*Regression*	143.188	1	143.188	233.238	<.001
	Residual	121.555	198	.614		
	Total	264.743	199			

Table 17

Coefficients – Resource Allocation as a Predictor for Cybersecurity Readiness

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Standard Error	Beta	t	Significance
1	*(Constant)*	1.991	.344		5.792	<.001
	Risk Appetite	.720	.047	.735	15.272	<.001

Hypothesis 4

***H_4**: Technology wariness will weaken the relationship between resource allocation and cyber security readiness.*

To investigate the moderating relationship of attitudes towards technology on the relationship between the allocation of resources for technology within respondents' companies and their corresponding cybersecurity preparedness, a regression analysis was conducted by the researcher. Prior to the regression analysis, the Technology Wariness and Resource Allocation variables were converted to mean-centered z scores to allow for improved interpretation of the results and to avoid creating unnecessary multicollinearity. Once the scores were converted, each participant’s mean centered scores for Technology Wariness and Resource Allocation were multiplied together and the product was relied upon as the moderating variable.

The regression analysis, which focused on how technology wariness moderates the correlation between a company's allocation of resources and its readiness in terms of cybersecurity produced significant results. As highlighted in Table 18, a total of 56.2% of the variance in cybersecurity readiness can be explained by this model. Furthermore, Table 19 underscores the significance of this predictive relationship, with a p-value of less than .001. The

data provides evidence that there is a relationship between cybersecurity readiness, resource allocation, and technology wariness. The coefficients in Table 20 highlight the significance of each portion of the model in the results, yielding the following regression equation:

Cybersecurity Readiness = 3.836 + .507(Resource Allocation) -.366(Tech Wariness) + .042 (Resource Allocation x Tech Wariness)

The coefficient .507 shows a highly significant main effect between resource allocation and cybersecurity readiness ($p<.001$). This relationship is positive as more resources will support the enhancement of cybersecurity. The coefficient -.366 shows a significant effect between technology wariness and cybersecurity readiness ($p\leq0.05$). This relationship is negative as an increase in technology wariness will create a decrease in cybersecurity readiness. Finally, the coefficient .042 shows a significant interaction found by technology wariness on resource allocation and cybersecurity readiness ($p\leq0.05$).

Table 18

Model Summary – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.749	.562	.555	.76961	.562	83.660	3	196	<.001

Table 19

Statistical Significance – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	*Regression*	148.654	3	49.551	83.660	<.001b
	Residual	116.089	196	.592		
	Total	264.743	199			

Table 20

Coefficients – Resource Allocation by Technology Wariness as Predictors for Cybersecurity Readiness

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Standard Error	Beta	t	Significance
1	*(Constant)*	3.836	.882		4.351	<.001
	Resource Allocation	.507	.119	.517	4.256	<.001
	Tech Wariness	-.366	.151	-.834	-2.421	.016
	Tech Wariness Modifier	.042	.020	.818	2.140	.034

To further understand the impact of the Technology Wariness modifier on the relationship between resource allocation and cybersecurity readiness, the research divided the variable, Technological Wariness, into three categories. Table 21 shows the breakdown of respondents in each category and the range of responses that fall into each category.

Table 21

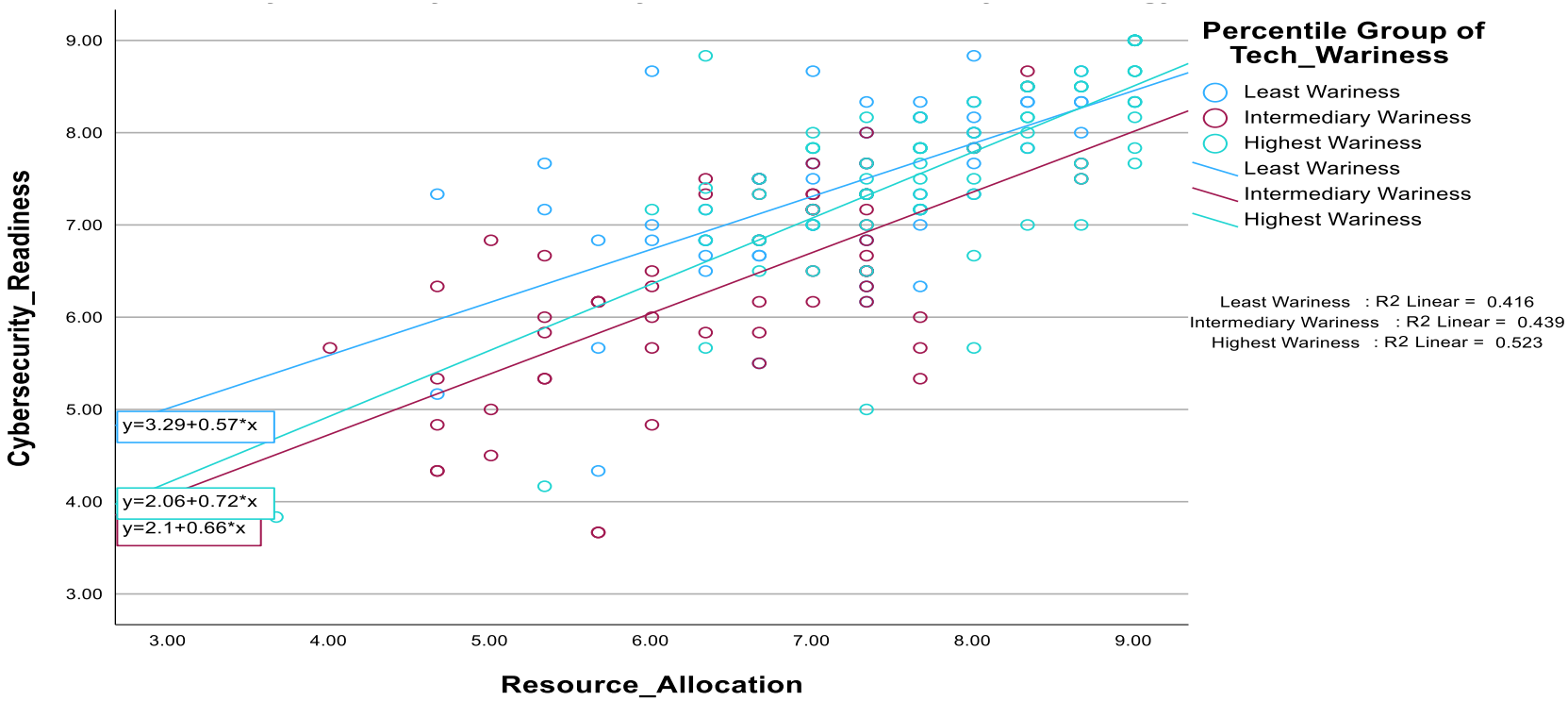
Percentile Groups – Technological Wariness

	N	Minimum	Maximum
Least Wariness	63	1.00	3.50
Intermediary Wariness	62	4.00	7.00
Highest Wariness	75	7.50	9.00
Total	200	1.00	9.00

Finally, the researcher explored the differences in the relationships of each of the three groups. As shown in Figure 5, those in the "highest wariness" group who have a lower resource allocation score are more likely to be similar in cybersecurity readiness to those in the "intermediary wariness" group. However, when those in the "highest wariness" group (green line) have a higher resource allocation score, they are more likely to be similar in cybersecurity readiness to those in the "least wariness" group.

Figure 5

Cybersecurity Readiness by Resource Allocation by Technology Wariness



Hypothesis 5

***H_5**: An elevated risk tolerance will strengthen the relationship between risk appetite and resource allocation.*

To examine how risk tolerance affects the connection between a company's risk appetite and the allocation of resources for technology in respondents' organizations, the researcher conducted a regression analysis. Before conducting the regression analysis, the researcher transformed the Risk Tolerance and Risk Appetite variables into mean-centered z-scores to enhance result interpretation and prevent the introduction of undue multicollinearity. Once these scores were transformed, the researcher multiplied each participant's mean-centered scores for Risk Tolerance and Risk Appetite to create a moderating variable.

The regression analysis yielded noteworthy findings. As depicted in Table 22, this model accounts for 28.7% of the variability in cybersecurity readiness. Additionally, Table 23 underscores the significance of this predictive association, with a p-value of less than .001. The data provides evidence that there is a relationship between cybersecurity readiness, resource allocation, and technology wariness. Interestingly, the coefficients in Table 24 indicate that only the Risk Tolerance Modifier is a significant component of the model. The analysis yields the following equation:

Resource Allocation = 3.836 - .132(Risk Appetite) - .170(Risk Tolerance) + .053 (Risk Appetite x Risk Tolerance)

Table 24 shows that the coefficients -.132 and -.170 are not significant in this model as their p values are respectively .365 and .170, which is greater than 0.05. However, the interaction (risk appetite and risk tolerance) with a coefficient of .053 is significant ($p \leq .010$). This model cannot be partially explained by the main effects, risk appetite and resource allocation and risk

tolerance and resource allocation alone. The analysis shows that risk tolerance moderates the relationship between risk appetite and resource allocation.

Table 22

Model Summary – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.536	.287	.276	1.00175	.287	26.303	3	196	<.001

Table 23

Statistical Significance – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation

Model		Sum of Squares	df	Mean Square	F	Sig.
1	*Regression*	79.187	3	26.396	26.303	<.001b
	Residual	196.688	196	1.004		
	Total	275.875	199			

Table 24

Coefficients – Risk Appetite by Risk Tolerance as Predictors for Resource Allocation

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Standard Error	Beta	t	Significance
1	*(Constant)*	6.891	.728		9.464	<.001
	Risk Appetite	-.132	.145	-.214	-.908	.365
	Risk Tolerance	-.170	.124	-.276	-1.379	.170
	Risk Tolerance Modifier	.053	.020	.978	2.604	.010

To gain deeper insights into how the Risk Tolerance modifier affects the connection between a company's risk appetite and resource allocation, the study divided the Risk Tolerance variable into three distinct categories. Table 25 delineates the division of respondents within each category, as well as the range of responses within these respective categories.

Table 25

Percentile Groups – Risk Tolerance

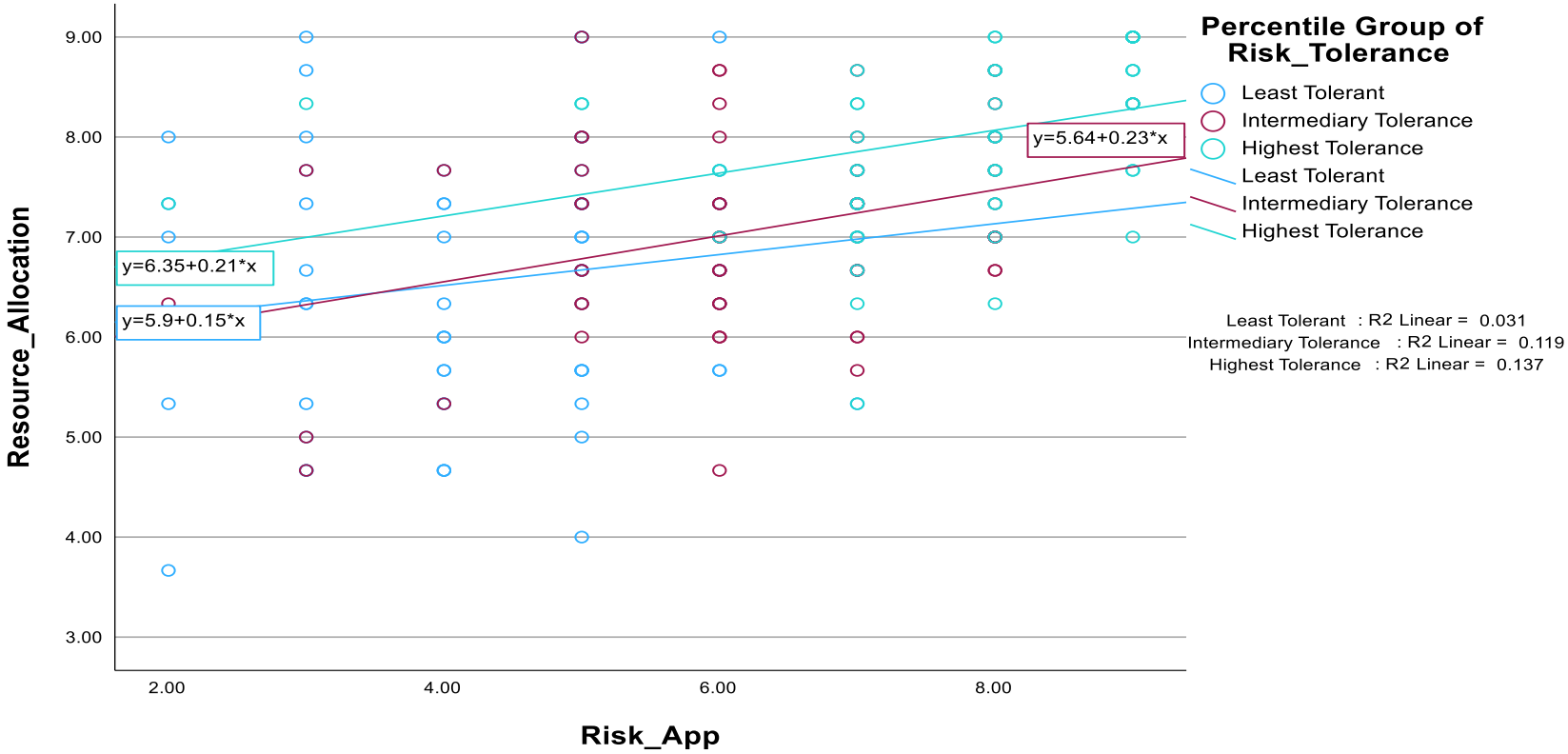
	N	Minimum	Maximum
Least Tolerant	71	1.00	5.00
Intermediary Tolerance	69	6.00	7.00
Highest Tolerance	60	8.00	9.00
Total	200	1.00	9.00

Finally, the researcher explored the differences in the relationships of each of the three groups. As shown in Figure 6, those in the “intermediary tolerance” group who have a lower risk

appetite are more likely to be similar in resource allocation to those in the “least tolerance” group. However, when those in the “intermediary tolerance” group have a higher risk appetite score, they are more likely to be similar in resource allocation to those in the “highest tolerance” group.

Figure 6

Resource Allocation by Risk Appetite by Risk Tolerance



Hypothesis 6

***H_6**: Larger companies will strengthen the relationship between resource allocation and cybersecurity readiness.*

To explore how company size moderates the connection between the allocation of resources for technology within respondents' companies and their corresponding cybersecurity preparedness, the researcher performed a regression analysis. However, this regression analysis did not yield noteworthy results. As shown in Tables 26 and 27, the results indicate that the model predicts cybersecurity readiness. However, upon examination of the coefficients in Table 30, it becomes apparent that the only driver of the model is resource allocation and company size does not have an effect of cybersecurity readiness.

Table 26

Model Summary – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness

Model	R	R Square	Adjusted R Square	Std. Error of the Estimates	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.737	.542	.535	.78616	.542	77.453	3	196	<.001

Table 27

Statistical Significance – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness

Model		Sum of Squares	df	Mean Square	F	Sig.
1	***Regression***	143.607	3	47.869	77.453	<.001
	Residual	121.136	196	.618		
	Total	264.743	199			

Table 28

Coefficients – Company Size as a Moderator on the Relationship between Resource Allocation and Cybersecurity Readiness

		Unstandardized Coefficients		Standardized Coefficients		
Model		**B**	**Standard Error**	**Beta**	**t**	**Significance**
1	*(Constant)*	2.178	.433		5.032	<.001
	Resource Allocation	.692	.060	.707	11.590	<.001
	Company Size	-.496	.718	-.209	-.691	.491
	Company Size Modifier	.074	.098	.231	.754	.452

CHAPTER 5 — DISCUSSION, CONCLUSIONS, LIMITATIONS, AND FUTURE RESEARCH

The research contributes to the field of cybersecurity by showing the importance of the relationship between resource allocation and cybersecurity readiness, and how other factors affect such a relationship. In any investment endeavor, it is important that companies assess their risks and evaluate if the return is worth the risk. As technology is closely related to business processes, companies' risk appetites affect how cybersecurity is managed. In evaluating H_1, which states that companies with elevated risk appetite will have an increased cybersecurity readiness, this paper finds that the hypothesis was supported. This finding outlines the importance of an accurate risk appetite assessment, as a misstatement in a company's risk appetite will affect the risk rating of its processes exposing it to higher risks than expected. As a result, the firm will be unprepared to respond to cyber threats, which can cause significant financial harm. A misstatement in a company's risk appetite may also give stakeholders a false impression that their investment is secure, obscuring their decision-making (Martens & Rittenberg, 2020). If the firm is exposed to a risk, and its impact on the firm is higher than expected resulting in significant financial loss, the firm will lose the trust of current and potential investors as well as customers and business partners. This is why technology and cyber risk management functions within the firm need to work closely with business functions to

understand their business processes and the potential monetary loss associated with those processes (Benz & Chatterjee, 2020). Additionally, cyber risk management will evaluate the cyber risk environment of the firm in combination with the assessment of the frequency of the business process. The risk environment and frequency will help determine the likelihood of a risk occurring, and the potential monetary loss will determine the impact on the firm (Boehm et al., 2019).

Evaluating the impact based on financial loss is not limited to the simple loss of the funds invested. The firm needs to consider other costs related to incident response and recovery. In the case of ransomware, a company will not only lose money due to the disruption to the business, but also the ransom paid, patching of the systems once they are recovered, and investigation of a data breach. If a data breach occurs, the firm will be exposed to reputational risks resulting in regulatory fines, and the loss of investors and business partners. Technology assets that are the pillars of the business, and as a disruption may cause significant damage to the company, they should be considered digital crown jewels and treated as critical risk items.

The empirical support of H_1 serves as a foundation for H_2 and H_3. Although risk appetite plays a crucial role in cybersecurity readiness, its effect is not only direct, but mediated by resource allocation. Cybersecurity does not happen on its own because a firm has identified its risk appetite and rated its risks correctly. There needs to be strategic planning and execution including the resources needed to implement risk management optimal enough to cover the risks identified (Yusif & Hafeez-Baig, 2021). The resources are human, who possess the skill and knowledge at all levels of the firm and are needed in optimal quantity and quality; and technology that is needed to perform the various cybersecurity risk management tasks in an

innovative and effective way; and the budget or funds needed to acquire both the human and technology resources (Day, 1994).

As companies operate in a low-risk environment and require a low level of control over their risks, they will need fewer resources to achieve an optimal cybersecurity readiness. Companies that operate in high-risk environments, on the other hand, will need more resources. This explains the empirical support of H_2, where 24.5% of the variance in Resource Allocation can be explained by Risk Appetite. As companies identify and rate their risk, and state their risk appetite, they need to plan and allocate the resources needed to help them achieve their goals. A strong example supporting H_2 is the segregation of duties of controls in cybersecurity (SoD). SoD is a task that is segmented and allocated to two or more individuals so that one individual cannot complete all of it, concealing fraud, or errors (Kobelsky, 2014). For example, a user requesting access to an application cannot approve the application. Additionally, depending on the risk rating or company practice, the individual approving the access cannot grant the access. As access management can be automated or manual, a firm will need humans, technology, and funds to implement access management controls. Usually, this control is hybrid (partly automated and partly manual). If the control is manual, the company will need more human resources and funds than technology. There will be three levels to the access management control, a requester, an approver, and a fulfiller (Ylonen et al., 2015). If the control is automated, that means the firm has invested in an identity and access management (IAM) tool or technology (Indu et al., 2018). Fewer humans and less manual work will be involved in the process. Once the request is sent, the system will perform checks to ensure that the request is valid and notify the approver. Once the approver validates his/her signature, access will be automatically granted (Ylonen et al., 2015).

The paper posits in H_5 that risk tolerance will strengthen the positive relationship between risk appetite and resource allocation. However, the results show that only the interaction risk tolerance and risk appetite are significant in explaining the model. The hypothesis is supported as risk tolerance strengthen the model. The explanation of the result of H_5 is in the nature and relationship between risk tolerance and risk appetite. Recall that risk tolerance is the level of loss an organization can take or is willing to take considering that the loss may harm the company. As risk tolerance increases, the organization has the possibility to take more risk increasing its risk appetite, prompting the allocation of additional resources to cybersecurity readiness. The paper further investigated the results for H_5 by examining the behavior of resource allocation based on a variation in spectrum of risk tolerance. The paper finds that low tolerance companies with high risk appetites scored lower on resource allocation, while high tolerance companies with high risk appetites scored higher in resource allocation, which further solidifies the initial result.

As illustrated through the access management control, firms that operate in low-risk environments do not need to be strict on SoD. For example, if the process is manual, the approver can also grant access. The risk is minimized if the requester is not approving or granting access. But for high-risk environments or assets, a full SoD is required. The SoD example explains why H_3 is supported as 54% of the variance in cybersecurity readiness is explained by resource allocation. Companies that allocate more resources to cybersecurity management will achieve higher readiness. H_3 results solidify the resource advantage theory and add value to the strategic segmentation theory, as presented by Thoeni et al. (2016). Strategic segmentation does not only apply in marketing but also in cybersecurity management as risk scenarios in cybersecurity are not uniform. On the contrary, they are diverse, dynamic, and can

be grouped into several categories. Firms with sufficient resources will have the bandwidth to strategize by categorizing their risks by investments, processes, technology assets, business environment, and cyber risk environment, which will help them achieve a better cybersecurity readiness. Strategic segmentation in cybersecurity is useful in identifying areas in which an organization should focus their resources. For example, the financial sector recorded 23.6% of global phishing attacks in the first quarter of 2022 (Statista, 2022). The financial sector is arguably a high-risk environment due to the attraction of attackers to money movements within that sector. However, not all activities, processes, and technology assets of financial firms should be rated high risk. Items that process or hold consumers' personal identification information and data classified as restricted can be considered high risk. But those holding publicly available information may be rated low and treated differently.

H_3 results also contribute to the DRM theory as it shows that because the risk environment is dynamic, cyber threats evolve over time and so do the risk ratings. As such, risk management should be flexible, and controls should be frequently reevaluated (Benz & Chatterjee, 2020). Organizations cannot just adopt cybersecurity frameworks as they are without tailoring them to their specific risk environments and activities. Based on the data, organizations with more resources will be able to implement dynamic cybersecurity management as they can leverage strategic segmentation and make changes in individual areas instead of making unnecessary and costly changes when their risk environments shift.

The domain of technology is very diverse and complex, and disciplines are siloed within the field. For an organization, dealing with the evolution of technology and its inherent risks can be a difficult and costly task. In exploring technology wariness, the survey shows that on average 55% of respondents feel discomfort and insecurity around technology. In assessing H_4, this paper

shows that 56% of the variance in cybersecurity readiness can be explained by the moderation of technology wariness on the relationship between resource allocation and cybersecurity. The results show that for each incremental unit of technology wariness, the relationship between resource allocation and cybersecurity weakens by - 0.834. The hypothesis is supported. The foundation of H_4 is that organizations that score high on technology wariness experience a decrease in their cybersecurity readiness as they will not allocate enough technology resources to cybersecurity. This paper examined the spectrum of technology wariness to see if it affects the relationship of resource allocation to cybersecurity differently at each level of the spectrum. The results show that those in the "highest wariness" group who have a lower resource allocation score are more likely to be similar in cybersecurity readiness to those in the "intermediary wariness" group. Note that as wariness increases, so does resource allocation and cybersecurity readiness, to a level equal to an intermediary level. When groups in the "highest wariness" group have a higher resource allocation score, they are more likely to be similar in cybersecurity readiness to those in the "least wariness" group, which means that as firms have access to more resources, although they feel discomfort and insecurity around technology, they can use other means to enhance their controls increasing their cybersecurity readiness. Recalling the SoD in the access management example, firms that do not want to invest in technology but want to achieve the same level of control will hire more personnel.

The empirical support of H_4 contributes to the practitioners' fields by showing the importance of leveraging technology in cybersecurity management. The advantage of using technology in automating cybersecurity management is to first maintain the system and data integrity by avoiding introducing human error, which is frequent in manual processes (He et al., 2022). Automation helps maintain system availability, consistency, and accountability (He et al.,

2022). Investing in technology allows the organization to process a large amount of data in a short time enabling a faster detection of system vulnerabilities and cyber-attacks.

Automating cybersecurity management is even more important in very large companies. One of the main vulnerabilities organizations face is the people, mostly if they are not properly trained or aware of cyber threats. For example, one way for hackers to access a firm's information system is through phishing attacks. A phishing attack is a method used by a hacker impersonating a legitimate actor to trick a person into performing an action that will benefit the hacker (Alkhalil et al., 2021). It is usually done through an email containing a link that the victim is supposed to click. Once the link is clicked, a program will allow the hacker to access the victim's device and sensitive information like personal or bank information. In the case of firms, a successful phishing attack can be devastating as it allows the hacker to potentially have access to the entire firm's information system. Although it is possible to periodically train staff members, it is not enough to mitigate phishing attacks. Organizations should implement rigorous controls to block unauthorized external links through the organization's email. They should also restrict the use of personal emails on enterprise devices. Such controls cannot be performed manually and need automation and monitoring.

Large companies need to allocate more resources to cybersecurity than their smaller counterparts due to the complexity and scale of their operations, as well as their social footprints. Larger companies also have more resources due to their access to funds. In that perspective, this paper hypothesized in H_6 that larger companies would strengthen the relationship between resource allocation and cybersecurity readiness. In other words, larger companies will be more mature than their smaller counterparts in terms of cybersecurity (Benz & Chatterjee, 2020). However, the evaluation of H_6 shows that company size has no significant moderating effect on

the resource allocation-cybersecurity readiness relationship. This result can be explained through risk rating and the complexity and scale of companies' operations. It can also be explained by the complexity of companies' information technology infrastructures.

The scale of operations of large compagnies require them to have very complex information technology infrastructures (Asen et al., 2019). With the rise of cloud computing, large, and even small, firms are using hybrid infrastructure, meaning their information technology is hosted on both local premises and cloud systems. Additionally, they have several interconnected applications, with staff personnel connecting globally from various devices. With complex information technology systems come more cyber risks and subsequently the need for more resources. Larger firms need more skilled personnel to ensure the security of their systems, more technology not only to host their operating systems but also applications dedicated to vulnerability monitoring and cyber risk management, which in turn require more funds (Asen et al., 2019).

Small companies, on the other hand, although they have less resources, their systems are less complex and their risks more manageable. Their resources will be stretched thin regardless, resulting in the same effect as large companies (Benz & Chatterjee, 2020). Certain small companies do not need large physical data centers or information technology systems like their larger counterparts do. They are created directly and operate in the cloud, minimizing the need to acquire skilled personnel to ensure cybersecurity. Such services are largely provided by cloud providers. As a result, cybersecurity readiness does not strongly depend on the quantity of resources available, but on the optimization of the resource tailored to the needs of the firm. The findings in H_6 add value to the practitioner field by showing the importance of tailoring

resources to the cybersecurity needs of the firm. Using strategic segmentation becomes key to the success of companies in implementing optimal cybersecurity risk management programs.

Overall, this paper adds value to the academic and practitioner fields in cyber risk management. To the research question seeking to know if an organization's risk appetite impacts its ability to allocate the right resources to its cyber security readiness, the research shows positive results and strong significance in the connection between risk appetite and resource allocation. To the research question seeking to know if firms can achieve a mature cyber security framework adoption regardless of the resources available to them, the paper finds that segmenting risks to optimize the allocation of resources to cyber risk management could help firms achieve a mature cybersecurity framework adoption, thus achieving a better cybersecurity readiness.

However, there were some limitations that need to be addressed in future research. The current research focused only on firms located in the United States and would benefit if non-US firms are included to better allow a generalization of cybersecurity readiness globally. This study also narrowly focused on technology wariness and would benefit from exploring other sentiments that could affect resource allocation and cybersecurity readiness. Future research should also explore how the rapid development of technology, including artificial intelligence, is straining firms' resources, and their effects on cybersecurity readiness.

References

Akinwumi, D. A., Iwasokun, G. B., Alese, B. K., & Oluwadare, S. A. (2017). A review of game theory approach to cyber security risk management. *Nigerian Journal of Technology, 36(4)*, 1271-1285. http://dx.doi.org/10.4314/njt.v36i4.38http://dx.doi.org/10.4314/njt.v36i4.38

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*(1). frontiersin. https://doi.org/10.3389/fcomp.2021.563060

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach supports the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580. https://doi.org/10.1016/j.dss.2021.113580https://doi.org/10.1016/j.dss.2021.113580

Asen, A., Bohmayr, W., Deutscher, S., Gonzalez, marcial, & Mkrtchian, D. (2019). Are you spending big enough on cybersecurity? *Boston Consultation Group*.

Aven, T. (2013). On the meaning and use of the risk appetite concept. *Risk Analysis, 33(3)*, 462-468. 10.1111/j.1539-6924.2012.01887.x

Bartlet, M. S. (1954). A further note on the multiplying factors for various chi-square approximations in factor analysis. *Journal of the Royal Statistical Society, Series B, 16*, 296-298.

Belghitar, Y., & Clark, E. A. (2012). The effect of CEO risk appetite on firm volatility: An empirical analysis of financial firms. *International Journal of the Economics of Business*, 19(2), 195-211. https://doi.org/10.1080/13571516.2012.642640

Benaroch, M., Lichtenstein, Y., & Robinson, K. (2006). Real options in information technology risk management: An empirical validation of risk-option relationships. *MIS Quarterly*, 30(4), 827. https://doi.org/10.2307/25148756

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540. https://doi.org/10.1016/j.bushor.2020.03.010

Berger, D. E. (2003). *Introduction to Multiple Regression*. Claremont Graduate University

Candell Jr., R., Zimmerman, T. A., & Stouffer, K. A. (2015). An industrial control system cybersecurity performance testbed. *National Institute of Standards and Technology*. https://doi.org/10.6028/nist.ir.8089

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019). *The risk-based approach to cybersecurity*. McKinsey & Company, 9.

Chau, P. Y. (1996). An empirical assessment of a modified technology acceptance model. *Journal of Management Information Systems, 13(2),* 185-204. https://doi.org/10.1080/07421222.1996.11518128

Child D. (2006). *The essentials of factor analysis* (3rd ed.). Continuum.

Day, G. S. (1994). The capabilities of market-driven organizations. *Journal of Marketing, 58(4),* 37. https://doi.org/10.2307/1251915

Dickason, Z., Ferreira, S., & McMillan, D. (2018). Establishing a link between risk tolerance, investor personality and behavioural finance in South Africa. *Cogent Economics & Finance, 6(1),* 1519898. https://doi.org/10.1080/23322039.2018.1519898

Fehle, F., & Tsyplakov, S. (2005). Dynamic risk management: Theory and evidence. *Journal of Financial Economics, 78(1),* 3-47. www.elsevier.com/locatejfee

Ganapathy, V. (2021). Investing in corporate governance risk management in insurance industry – an analysis. *The Journal of Insurance Institute of India*.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications, 58,* 102726. https://doi.org/10.1016/j.jisa.2020.102726

Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3553470

He, S., Ficke, E., Pritom, M. M. A., Chen, H., Tang, Q., Chen, Q., Pendleton, M., Njilla, L., & Xu, S. (2022). Blockchain-based automated and robust cyber security management. *Journal of Parallel and Distributed Computing*. https://doi.org/10.1016/j.jpdc.2022.01.002

Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, *44*, 655–662. https://doi.org/10.1016/j.promfg.2020.02.243

Hörisch, J., Johnson, M. P., & Schaltegger, S. (2014). Implementation of sustainability management and company size: A knowledge-based view. *Business Strategy and the Environment, 24(8),* 765–779. https://doi.org/10.1002/bse.1844

Hunt, S. D. (1999). The strategic imperative and sustainable competitive advantage: Public policy implications of the resource advantage theory. *Journal of the Academy of Marketing Science*, 27(2), 144-159. https://link.springer.com/article/10.1177/0092070399272003

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(4), 574–588. Sciencedirect. https://doi.org/10.1016/j.jestch.2018.05.010

Jan, A. U., & Contreras, V. (2011). Technology acceptance model for the use of information technology in universities. *Computers in Human Behavior,* 27(2), 845-851. https://doi.org/10.1016/j.chb.2010.11.009

Jenrich R. L., Sampson P. F. (1966). Rotation for simple loading. *Psychometrika*, 31, 313-323.

Johnson, J. (2021, April 29). Topic: U.S. consumers and cyber crime. *Statista*. https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/#dossierKeyfigures

Kaiser H. F. (1974). An index of factorial simplicity. *Psychometrika*, 39, 31-36.

Ketikidis, P., Dimitrovski, T., Lazuras, L., & Bath, P. A. (2012). Acceptance of health information technology in health professionals: An application of the revised technology acceptance model. *Health Informatics Journal, 18(2)*, 124-134. 10.1177/1460458211435425

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information & Management, 43(6)*, 740-755. www.elsevier.com/locate

Kraaijenbrink, J., Spender, J. C., & Groen, A. J. (2010). The resource-based view: A review and assessment of its critiques. *Journal of Management*, 36(1), 349-372. 10.1177/0149206309350775

Ma, Q., & Liu, L. (2004). The technology acceptance model: A meta-analysis of empirical findings. *Journal of Organizational and End User Computing (JOEUC)*, 16(1), 59- https://www.researchgate.net/publication/22006878

Malhotra, N. (2017). *Review of marketing research* Volume 1. Florence Routledge.

Malhotra, Y., & Galletta, D. F. (2019). *Extending the technology acceptance model to account for social influence: Theoretical bases and empirical validation*. Proceedings of the 32nd Annual Hawaii International Conference on Systems Sciences. 1999. HICSS-32. Abstracts and CD-ROM of Full Papers. https://doi.org/10.1109/hicss.1999.772658

Marangunić, N., & Granić, A. (2014). Technology acceptance model: A literature review from 1986 to 2013. *Universal Access in the Information Society*, 14(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Martens, F., & Rittenberg, L. (2020). *COCO Guidance Risk Appetite Critical to Success.* The Institute of Management Accountants (IMA). Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/Shared%20Documents/COSO-Guidance-Risk-Appetite-Critical-to-Success.pdf

Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). Cyber threat metrics. *Sandia Report*, *SAND2012-2427*. Sandia National Laboratories.

OECD. (2017). Entrepreneurship - enterprises by business size - OECD data. *The OECD*. https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm

Okagbue, H. I., Oguntunde, P. E., Obasi, E. C. M., & Akhmetshin, E. M. (2021). Trends and usage pattern of SPSS and Minitab Software in Scientific research. *Journal of Physics: Conference Series*, 1734. https://iopscience.iop.org/article/10.1088/1742-6596/1734/1/012017/pdf

Porter, M. (1990). Competitive advantage of nations. *Competitive Intelligence Review*, 1(1). https://doi.org/10.1002/cir.3880010112

Purnanandam, A. (2008). Financial distress and corporate risk management: Theory and evidence. *Journal of Financial Economics*, 87(3), 706–739. https://doi.org/10.1016/j.jfineco.2007.04.003

Parasuraman, A. (2000). Technology Readiness Index (TRI). *Journal of Service Research*, 2(4), 307–320. https://doi.org/10.1177/109467050024001

Sagnier, C., Loup-Escande, E., Lourdeaux, D., Thouvenin, I., & Valléry, G. (2020). User acceptance of virtual reality: An extended technology acceptance model. *International Journal of Human-Computer Interaction*, 36(11), 993-1007. f10.1080/10447318.2019.1708612ff. Final-02446117f

Schonlau, M., Fricker Jr., R.D., & Elliot, M.N. (2002). *Conducting research via e-mail and the web.* Rand Distribution Services.

Servaes, H., & Tamayo, A. (2021). The impact of corporate social responsibility on firm value: The role of customer awareness. *Management Science, 59(5),* 1045-1061. https://doi.org/10.1287/mnsc.1120.1630

Shrestha, N. (2021). Factor analysis as a tool for survey analysis. *American Journal of Applied Mathematics and Statistics*, 9 (1), 4-11.

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

Statista. (2022). IT spend on cyber security U.S. and Europe 2022. (2022, May). *Statista*. https://www.statista.com/statistics/1245356/it-spend-on-cyber-security/

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC

27002 and PCI DSS. *International Journal on Informatics Visualization*, VOL 4 (2020) NO 4(2549-9610).

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management Science*, 42(1), 85-92. https://doi.org/10.1287/mnsc.42.1.85

Thoeni, A. T., Marshall, G. W., & Campbell, S. M. (2016). A resource advantage theory typology of strategic segmentation. *European Journal of Marketing*. www.emeraldinsight.com/0309-0566.htm

Tohidi, H. (2011). The role of risk management in IT systems of organizations. *Procedia Computer Science, 3*, 881–887. https://doi.org/10.1016/j.procs.2010.12.144

Tunggal, A. T. (2023, May 1). *The 70 biggest data breaches.* Upguard.com. https://www.upguard.com/blog/biggest-data-breaches

W. Kobelsky, K. (2014). A conceptual model for segregation of duties: Integrating theory and practice for manual and it-supported processes. *International Journal of Accounting Information Systems, 15*(4), 304–322. https://doi.org/10.1016/j.accinf.2014.05.003

Wernerfelt, B. (1984). A resource-based view of the firm. *Strategic Management Journal, 5(2),* 171–180. https://www.jstor.org/stable/2486175

West S. G., Finch J. F., Curran P.J. (1995) Structural equation models with nonnormal variables: Problems and remedies. In R . H. Hoyle (Ed.), *Structural equation modeling: Concepts, issues and applications* (56-75). Sage.

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 1–24. https://doi.org/10.1080/19361610.2021.1918995

Appendix A

Questions	**Codes**
Country	Country
Please check one of the activities that you see as part of your job or role.	Screen_Act
How familiar are you with your organization's management of IT security technologies and services?	Screen_Familiarity
What organizational level best describes your current position?	Screen_Pos
Which department do you primarily work within at your organization?	Screen_Dep
What best describes your primary role in the organization?	Screen_Role
What industry best describes your organization's industry focus?	Screen_Indust
Is the IT security budget part of or separate from the overall IT budget?	Screen_IT_Budget

Appendix B

Questions	**Codes**
What is the estimated number of headcounts of your organization?	CompSize_Headcount
Rate the adequacy of the IT security budget to achieve a strong security posture within your organization? (Select from 1 to 9, 1 being less than adequate and 9 being more than adequate).	Res_ITBudget
Rate the human resource adequacy to achieve a strong security posture within your organization? (Select from 1 to 9, 1 being less than adequate and 9 being more than adequate).	Res_Human
Rate the adequacy of the IT security technology to achieve a strong security posture within your organization? (Select from 1 to 9, 1 being less than adequate and 9 being more than adequate).	Res_Tech
While responding to this question, think of risk appetite as a type and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Rate your organization risk appetite. (Select from 1 to 9, 1 being more risk averse and 9 being more risk seeking).	Risk_App
While responding to this question, think of risk tolerance as the loss your organization can actually cope with. Rate your organization risk appetite. (Select from 1 to 9, 1 being less risk tolerant and 9 being more risk tolerant).	Risk_Tol

Asset Management: Rate the maturity of your organization's adoption of the National Institute of Standards and Technology (NIST) framework components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	NIST_AssetM
Business Environment: Rate the maturity of your organization's adoption of the National Institute of Standards and Technology (NIST) framework components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	NIST_BusEnv
Governance: Rate the maturity of your organization's adoption of the National Institute of Standards and Technology (NIST) framework components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	NIST_Gov
Information Security Policies: Rate the maturity of your organization's adoption of the ISO 27002 framework components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	ISO27002_Ispolicies
Organization of Information Security: Rate the maturity of your organization's adoption of the ISO 27002 framework components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	ISO27002_OrgIS
Human Resources Security: Rate the maturity of your organization's adoption of the ISO 27002 framework	ISO27002_HumanResSec

components below. (Rate from 1 to 9, 1 being not mature and 9 being very mature).	
Rate the level of discomfort of your company in adopting cyber security technology. (Rate from 1 to 9, 1 being no discomfort and 9 being high discomfort).	TeAccp_Discomfort
Rate the level of insecurity of your company in adopting cyber security technology. (Rate from 1 to 9, 1 being no insecurity and 9 being high insecurity).	TeAccp_Insecurity