Journal of Information Security, 2021, 12, 137-161
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Optimum Spending on Cybersecurity Measures: Part II

Sherita Tara Kissoon

IT Risk & Security Advisory Services (ITRS), Markham, Canada
Email: tkissoon1970@gmail.com, kissoon1970@gmail.com

How to cite this paper: Kissoon, S.T. (2021) Optimum Spending on Cybersecurity Measures: Part II. *Journal of Information Security*, **12**, 137-161.
https://doi.org/10.4236/jis.2021.121007

Received: November 28, 2020
Accepted: January 18, 2021
Published: January 21, 2021

Abstract

The purpose of this research is to investigate the decision-making process for cybersecurity investments in organizations through development and utilization of a digital cybersecurity risk management framework. The initial article, Optimum Spending on Cybersecurity Measures is published on Emerald Insight at: https://www.emerald.com/insight/1750-6166.htm, contains the detailed literature review, and the data results from Phase I and Phase II of this research [1]. This article will highlight the research completed in the area of organizational decision-making on cybersecurity spend. In leveraging the review of additional studies, this research utilizes a regression framework and case study methodology to demonstrate that effective risk-based decisions are necessary when implementing cybersecurity controls. Through regression analysis, the effectiveness of current implemented cybersecurity measures in organizations is explored when connecting a dependent variable with several independent variables. The focus of this article is on the strategic decisions made by organizations when implementing cybersecurity measures. This research belongs to the area of risk management, and various models within the field of 1) information security; 2) strategic management; and 3) organizational decision-making to determine optimum spending on cybersecurity measures for risk taking organizations. This research resulted in the development of a cyber risk investment model and a digital cybersecurity risk management framework. Using a case study methodology, this model and framework were leveraged to evaluate and implement cybersecurity measures. The case study methodology provides an in-depth view of a risk-taking organization's risk mitigation strategy within the bounds of the educational environment focusing on five areas identified within a digital cyber risk model: 1) technology landscape and application portfolio; 2) data centric focus; 3) risk management practices; 4) cost-benefit analysis for cybersecurity measures; and 5) strategic development. The outcome of this research provides greater insight into how an organization makes decisions when implementing cybersecurity controls. This research shows that most organizations are dili-

gently implementing security measures to effectively monitor and detect cyber security attacks, specifically showing that risk taking organizations implemented cybersecurity measures to meet compliance and audit obligations with an annual spend of $3.18 million. It also indicated that 23.6% of risk-taking organizations incurred more than 6 cybersecurity breaches with an average dollar loss of $3.5 million. In addition, the impact of a cybersecurity breach on risk taking organizations is as follows: 1) data loss; 2) brand/reputational impact; 3) financial loss fines; 4) increase oversight by regulators/internal audit; and 5) customer/client impact. The implication this research has on practice is extensive, as it focuses on a broad range of areas to include risk, funding and type and impact of cyber security breaches encountered. The survey study clearly demonstrated the need to develop and utilize a digital cybersecurity risk management framework to integrate current industry frameworks within the risk management practice to include continuous compliance management. This type of framework would provide a balanced approach to managing the gap between a risk-taking organization and a risk averse organization when implementing cybersecurity measures.

Keywords

Information Security, Risk Management, Strategy, Governance, Organizational Decision Making

1. Introduction

Investing in security measures to strengthen an organizations' information security posture will ensure global interconnected environments are protected from cybersecurity attacks and other information security vulnerabilities.

There is a global dependency on technology and its enablement of the internet. Many organizations believe that compliance with regulations set by the government is sufficient to ensure security. This minimizes the impact a cybersecurity breach has on interconnected environments, and provides a solid foundation to build an organization's information security framework. This research is critical, as it will analyze the decision-making process of various stakeholders who are involved in implementations of cybersecurity measures to safeguard sensitive data in organizations. It will provide the necessary information to demonstrate a strategic risk-based approach to implementing cybersecurity measures for risk taking organizations.

A wide range of principles are relevant to cybersecurity decision-making in this context. Specific security measures are important and should be implemented appropriately to alleviate cybersecurity threats. The outcomes of this research will assist executives in understanding the business impact of cybersecurity risks, enabling them to implement cost effective security measures aligned to their organization's enterprise risk appetite. It will also contribute to the research community in providing risk management concepts, as well as a strategic framework in minimizing cybersecurity risks.

1.1. Research Problem

Digital technology is increasingly relied upon by the global community to provide real-time services to customers. Evolution of the technology from the traditional infrastructure to include mobile, cloud-based computing, software as a service, virtual environments, system security and integrity is prevalent. To understand the benefits that networked technology provides, these systems must operate in a reliable and secure way. Companies must have assurance that their data will be safe from disruption, loss or theft. Therefore, the protection of data, and the integrity and availability of organizations are essential.

The primary focus for most business executives is to increase revenue, promote innovation and technological advances in support of customer growth and retention strategies. Therefore, reallocation of funds to cybersecurity is considered a business trade-off, where realized gains may not be clearly communicated, nor easily measured. Business leaders need to know the impact cybersecurity risks have within their organization, in order to make intelligent business decisions.

Conducting cost-benefit analyses on implementing cybersecurity controls is a challenge, since quantifying the cost of cybersecurity failures is usually not included, nor is the benefit of averted breaches captured. Business leaders are unclear whether their investment in cybersecurity controls is proportional to the risk within their portfolio.

1.2. Aim of the Research

The focus of this research is to investigate the decision-making process for cybersecurity investments in organizations using conceptual models. Most conceptual models consider the dynamic environment, which is adaptable to changes that occur within the decision-making process. These models and frameworks rely on either specific scenarios or controlled conditions. As a result of the dynamic environment within the industry of cybersecurity, mitigation strategies evolve to address emerging industry threats. These variations influence the conditions that were used within previous framework and economic models.

Decisions on cybersecurity spend within organizations vary based on stakeholders, specifically the funding available in comparison to the recommended security measures necessary for compliance.

These executive decisions may be coloured with bias, as to the appropriate security baseline required to protect relevant information assets within the organization. The tradeoff between the costs of implementing a security measure, and the benefit derived from the implementation is not easily measured. Therefore, the lack of this information may impact the business leader's decision to fund security measures, and choose to further invest in developing new technology to drive innovation, business growth and customer satisfaction. This research will demonstrate the need for an appropriate cybersecurity risk management framework to determine optimum cybersecurity spend utilizing the results from the survey study.

2. Research Background

This research aims to test the effectiveness of implemented cybersecurity frameworks leveraging regression analysis. It focuses on the dependent variables of level of risk, an organization's funding model and impact of a cybersecurity breach. Each area was reviewed in depth to provide an understanding of its application to cybersecurity and the risk management decision-making process used when evaluating and investing in various security measures. Three global industry areas were analyzed during the survey study to gain a further understanding of the current gaps, as noted below.

Why Are Current Implementations of Cybersecurity Frameworks Effective in Identifying, Monitoring and Responding to Cybersecurity Threats?

An analysis of industry data indicates that organizations currently leverage government and industry frameworks when implementing cybersecurity measures. In addition, the decisions made by most stakeholders are based on validating compliance with government regulations, industry standards and internal policy.

Most organizations anonymously expressed that they had experienced types of cybersecurity breaches, prioritized as follows: 1) malware/ransomware; 2) phishing; 3) lost/stolen computer media; and 4) external/data breaches. Organizational stakeholders believe they can detect, respond to and monitor security incidents, however they are not able to continuously prevent security incidents from occurring within their environment.

What Factors are Considered by an Organization when Investing in Cybersecurity Controls?

The decision-making mechanisms utilized by organizations when evaluating and implementing different security measures focus primarily on 1) compliance with government and industry regulations; 2) investment cost; 3) the impact of either a breach or a fine; 4) either reputational or brand risk; and 5) ease of use by the business.

What Decision-making Mechanisms Do Organizations Use When Evaluating Different Security Measures Prior to Implementation?

The roles of stakeholders making decisions on cybersecurity measures within their organization include the following in order of priority: 1) chief technology officer (CTO); 2) chief information security officer (CISO); 3) head of business line; 3) chief information officer (CIO); and 5) board of directors. Stakeholders believe that the CTO and CISO have the primary responsibility for advising and funding the investment cost in their organization and estimate that their organization's investment budget is between $1 and $5 million dollars annually.

Stakeholders are involved in the implementation of cybersecurity measures in the following ways: 1) directly involved in the decision-making mechanism; 2) attend meetings on evaluating cybersecurity measures; 3) involved in cybersecurity implementation activities; and 4) support the cybersecurity function.

Most organizations are faced with an array of choices when deciding on how

to fund cybersecurity measures. Funding the investment cost needed to provide a secure environment can be complex.

Cost-benefit analyses, risk appetite and business trade-offs are some of the areas that are factored into the overall decision-making process. Most stakeholders indicate that the following areas are critical in an organization's decision-making process when allocating funds for cybersecurity measures:

1) Allocation of budget: Although stakeholders believe that their organization has allocated a large enough budget to respond to or detect a cybersecurity breach, it is apparent that their organization's cybersecurity budget is insufficient to ensure appropriate cybersecurity measures are in place to continuously prevent cybersecurity breaches from occurring within their organization.

2) Ability to prevent a cybersecurity breach: Although stakeholders believe that their organization can detect a cybersecurity breach in a timely manner, it is apparent that their organization is unable to prevent a cybersecurity breach, as stakeholders indicate during the survey study that their organization has encountered more than 15 breaches, see Figure 1.

3) Risk appetite: Stakeholders indicate that their organization's decision-making process is aligned with a risk methodology, and as noted within most of the industry-recognized economic models, this methodology directly impacts the cost-benefit analysis, as shown in Figure 2.

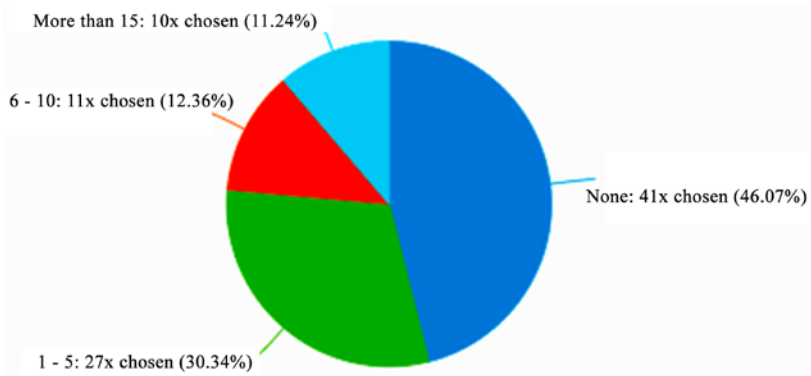


Figure 1. It shows the ability for an organization to prevent a cybersecurity breach, specifically 30% of respondents have experienced 5 or less cybersecurity breaches (Kissoon, 2019).

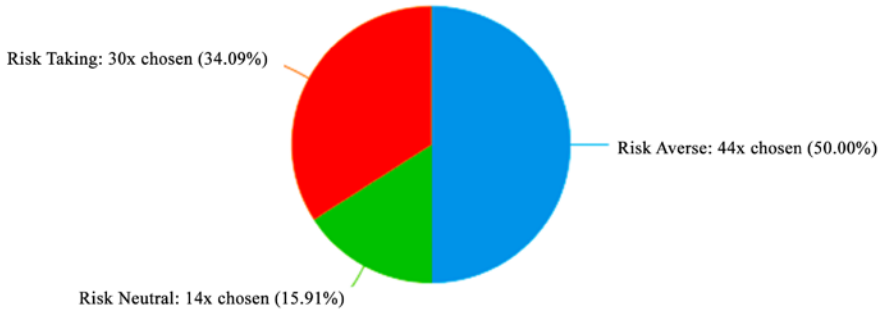


Figure 2. It demonstrates that 34% of organizations have a risk taking risk appetite (Kissoon, 2019).

4) Importance of decision-makers: It is apparent in most organizations that decisions made by the CIO and head of the business line have similar priorities with regard to 1) funding the investment cost; 2) implementing information security measures; and 3) reviewing the risk appetite statement. This parallel decision-making process may potentially have an adverse impact on the decision to fund cybersecurity measures, especially in circumstances where the viewpoints are vastly different.

3. Literature Review

Economic optimization of information security is an area of interest to researchers, as well as executives in organizations. From a financial viewpoint, cost benefit justification for security measures is impactful and necessary. Earlier researchers focused on either economic models for security optimization or quantification of business value for information security investments. This research aims to develop an evidence based digital cybersecurity risk management framework for organizations to effectively articulate the business impact of information security risks. There are a number of research studies that have been conducted in information security, all of which will be consulted thoroughly while undertaking this research. Optimum Spending on Cybersecurity Measures is published on Emerald Insight at: https://www.emerald.com/insight/1750-6166.htm, and contains the details of the Literature Review [1].

This article, using regression analysis and a case study will explore the area of risk management decision making leveraging the research completed by Dor and Elovici [2]. Utilizing grounded theory, researchers design a conceptual model that shows the current practices for decision-making about information security investment in organizations across industries. The framework takes into consideration that organizations may have different views, specifically depending on the stakeholder who finances the security measures, the organization's industry, structure and role of the Chief Information Security Officer's (CISO). Within this research, the case study methodology leverages a conceptual digital cybersecurity risk management framework. This will show that stakeholders in risk taking organizations can make effective decisions on implementing cybersecurity measures to reduce the likelihood of a cybersecurity breach.

4. Research

This research further analyzes the data gathered through the initial survey study to develop a cyber risk investment model and digital cybersecurity risk management framework. These conceptual models are used within the case study methodology to demonstrate a strategic approach to organizational decisions as it pertains to cybersecurity spend.

4.1. Gaps in the Literature

In reviewing the literature within the focus area of this research, specifically

economics of information security, it became apparent that there is significant literature on this topic. There are many variations of frameworks and economic models for investments in security measure and decision-making that are present in the literature. These models are applicable to specific phases in the decision process since they resolve various concerns within it. Model examples include: 1) creation of an economic model to assist the decision maker on their information security investment, Rue *et al.* [3]; 2) economic models which provide an estimate on the return on security investments (ROSI) for security measures, Cavusoglu *et al.* [4] [5], Gordon and Loeb [6] [7], Huang *et al.* [8], Purser [9]; 3) a management model that estimates various investment strategies on security management, Finne [10], Nazareth *et al.* [11]; and 4) a multi-criteria decision-making model that is used within the decision-making process in selecting projects, Comes *et al.* [12].

These models and frameworks rely on either specific scenarios or controlled conditions. In addition, decision-making in firms may include characteristics that are not present in these models, *i.e.*, politics, organizational, psychological cognitive biases, prejudice, Dutta *et al.* [13]. As a result of the dynamic environment within the industry of information security, mitigation strategies evolve to address emerging industry threats. These variations influence the conditions that were used within previous framework and economic models. Frameworks and economic models become outdated and narrow in the way it reflects current decision-making processes.

Furthermore, stakeholders in organizations may choose not to utilize these frameworks and economic models, since they are either complex or are not practical, Pettigrew [14]. Therefore, there is a need to develop a relevant, current conceptual model that represents the risk management process of how optimal information security investments occur in organizations. The current literature is limited in this realm of decision-making to include various models that can be applied by stakeholders on optimal cybersecurity spend within risk taking organizations.

4.2. Theoretical and Practical Contribution

This research will address a need in both the academic and practitioners' community, as this research developed and implemented an appropriate strategic framework to mitigate cybersecurity risks.

4.2.1. Contribution to Theory

The research will bring an in-depth theoretical understanding to this field, as it intends to test theory within the organizational behaviour, risk management and strategy discipline. The literature review provides two specific areas that can be further explored through empirical studies.

4.2.2. Contribution to Practice

The research also proposes to make an industry contribution by assisting busi-

ness leaders with an appropriate risk mitigation strategy when implementing cybersecurity controls. The application of the research within organizations will provide a framework to assist with the decisions made by executives pertaining to cybersecurity spend. This is demonstrated in Section 7 through a case study methodology.

5. Research Outline

5.1. Philosophical and Methodological Approaches

The relationship between data and theory has been discussed in depth by many philosophers over the years. This research has considered the main philosophical positions that underlie the design of the research. Specifically, being able to have a clear sense of my reflexive role in research methods, to assist with clarifying the research design, recognizing which design will be effective and providing ways on how to adapt the research according to the constraints presented. "Awareness of the philosophical assumptions can both increase the quality of research and contribute to creativity of the researcher", Easterby-Smith, Thorpe, Jackson [15].

5.2. Ontology, Epistemology and Methodology

The ontological approach for this research will be a combination of internal realism and relativism. Internal realism assumes that there is a single reality but asserts that it is never possible for scientists to access that reality directly. Relativism progresses further in suggesting that scientific laws are not simply present, they are available to be created by people. As people have different perspectives and their ability to gain acceptance from others may be influenced by many factors, Easterby-Smith, Thorpe, Jackson [15].

The epistemological approach for this research will be a combination of positivism and normal constructionism. The main idea of positivism is "that the social world exists externally, and that properties can be measured through objective methods rather than being inferred subjectively through sensation, reflection and/or intuition", Easterby-Smith, Thorpe, Jackson [15]. Combining this idea with a constructionist position would allow for many different realities, facilitating a research design that would gather multiple viewpoints. Using a combination of qualitative and quantitative methods, this research analyzed data gathered from a diverse population.

5.3. Methods and Techniques

The survey study research design utilizes an inductive, mixed methods approach, and employs a combination of techniques using a combined cross sectional and time series horizon. The partnership research design will apply a mixed methods study, to encompass a four phased approach using the data gathered through the survey study. To elaborate on partnership research designs, this "typically involves combining more than one method, such as a questionnaire survey and

interviews, where both assume similar importance in the study… When combined, the interview data will contain greater detail, clarifications and added explanations; the questionnaire data will contain shorter answers, possibly more focused, but will be able to cover responses from a wider range…", Easterby-Smith, Thorpe, Jackson [15].

Specifically, the mixed method approach will facilitate a sequential design with the following: 1) initial qualitative research; 2) the quantitative research is used as the dominant factor with respect to the findings; and 3) the case study methodology to demonstrate the implementation of the digital cybersecurity risk management framework.

Phase 1. Interview Study: Qualitative approach focused on seven participants providing input to refine the survey study questionnaire.

Phase 2. Survey Study: Qualitative approach focused on information gathered through an online descriptive survey study utilizing a five-point response Likert scale. Analysis of the data will leverage summary statistics of responses, differential and inferential statistics.

Phase 3. Regression Analysis: Quantitative statistical testing method used to examine the relationship between two or more variables of interest, specifically, examining the influence of one or more independent variables on a dependent variable. The purpose of regression analysis was to explore the effectiveness of current cybersecurity frameworks in organizations to minimize cybersecurity risks utilizing the data gathered through the survey study.

Phase 4. Case Study: The case study methodology provides an in-depth view of one organization's risk mitigation strategy within the bounded environment of the educational environment focusing on five areas identified within digital cyber risk model: 1) technology landscape and application portfolio; 2) data centric focus; 3) risk management practices; 4) cost-benefit analysis for cybersecurity measures; and 5) strategic development.

Optimum Spending on Cybersecurity Measures is published on Emerald Insight at: https://www.emerald.com/insight/1750-6166.htm, and contains the results from the survey study. Specifically, the research data to support Phase 1 and Phase 2.

6. Testing the Effectiveness of Cybersecurity Frameworks

Regression analysis was utilized to evaluate the way in which organizational decisions are made as it relates to cybersecurity spending. The purpose of regression analysis was to explore the effectiveness of current cybersecurity frameworks in organizations to minimize cybersecurity risks utilizing the data gathered through the survey study.

Single Multivariate Linear Regression Model

This analysis will utilize the data collected through the survey study which contains information on several variables in understanding an organization's prior-

ity when implementing cybersecurity measures. Appropriate analyses will be completed on this data using IBM's SPSS and statistical testing. To assess the effectiveness of cybersecurity measures, the following will be used to analyze the data to estimate a single linear equation that will test the effectiveness of the cybersecurity framework in place within organizations, as identified through participants within the survey study.

The data from the survey study shows the following:

Analysis 1: Using a dependent variable based on the Level of Risk an organization is willing to assume when implementing cybersecurity measures, specifically, 0—risk neutral, 1—risk taking and 2—risk averse, this regression demonstrates that risk taking organizations measure the effectiveness of their cybersecurity framework in the following priority:

1) Ability to meet compliance obligations.

2) Tested through the Audit/Assurance function.

3) Measured using Key Performance Indicators and Key Risk Indicators (KPI/KRI).

4) Measure using a Capacity Maturity Model (CMM).

5) Funds available/cost to implement security measure.

Analysis 2: Using a dependent variable based on the Investment Budget, specifically, 0—$0 - $500K, 1—$500K - $1M, 2 - $1M - $5M, and 3 - above $5M. This regression demonstrates that the average investment budget allocated by an organization when implementing cybersecurity measures is approximately $3 million, and organizations are effectively able to detect, respond and monitor an information security breach, however, are unable to adequately prevent an information security breach.

Analysis 3: Using a dependent variable based on the Average Dollar Loss after a Cybersecurity Breach, specifically, 1—$0 - $1M, 2—$1M- $3M, 3—$3M - $5M, and 4—above $5M. This regression demonstrates that the average funding allocated by organizations when implementing cybersecurity measures is 15% of the overall enterprise budget. Risk taking organizations incur an average of $3.5 million in loss after a cybersecurity breach has occurred.

Analysis 4: Using a dependent variable based on the Level of Risk an organization is willing to assume when implementing cybersecurity measures, specifically, 0—risk neutral, 1—risk taking and 2—risk averse, this regression demonstrates that risk taking organizations indicated that a strong security posture meets government regulations and company policy. However, on average, these organizations continue to experience approximately 5 cybersecurity breaches annually after meeting compliance obligations.

In conclusion, it is evident from the data analyzed through the survey study that risk taking organizations implement cybersecurity measures when required, and therefore spend minimal in support of a foundational security posture. In addition, continuous compliance management to facilitate a preventative approach is nonexistent, resulting in unforeseen losses due to the impact of reoc-

curring cybersecurity breaches.

7. Case Study

The case study methodology was utilized to evaluate the way in which risk management decisions are made as it relates to cybersecurity spending. The purpose of the case study was to demonstrate that a digital cybersecurity risk management framework is effective in minimizing cybersecurity risks, with a focus on the decision-making process by applicable stakeholders within organizations. Through utilizing the digital cybersecurity risk management framework, this case study shows that an appropriate risk mitigation strategy can be utilized by risk taking organizations to reduce the likelihood of a cybersecurity breach.

7.1. Methodology Used for Evaluating Cybersecurity Risk Management Framework

This case study provides an in-depth view of a risk-taking organization's risk mitigation strategy within the bounded environment of the educational environment focusing on five areas identified within cyber risk investment model: 1) technology landscape and application portfolio; 2) data centric focus; 3) risk management practices; 4) cost-benefit analysis for cybersecurity measures; and 5) strategic development, see Figure 3.

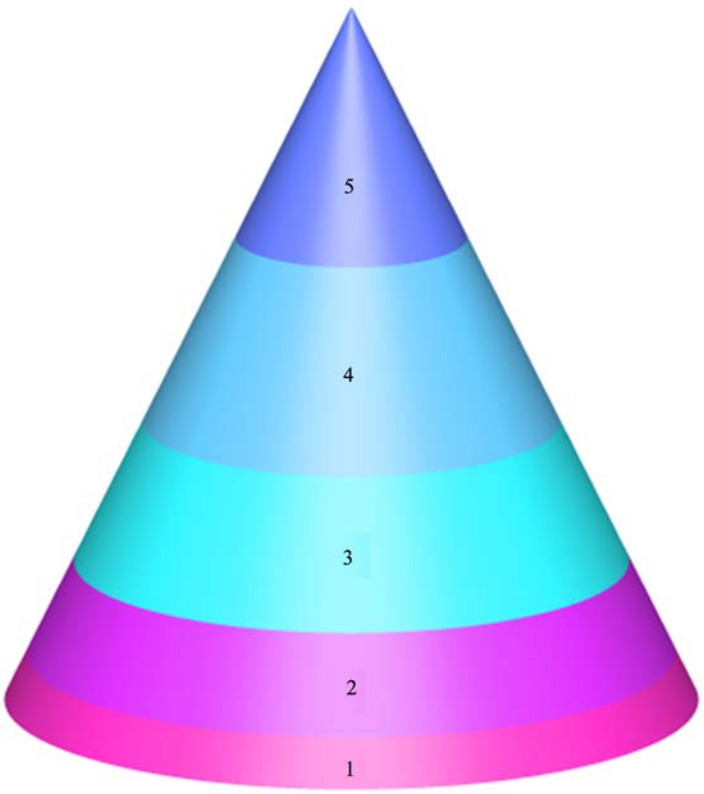


Figure 3. It shows the cyber risk investment model which is comprised of the 1) technology landscape and application portfolio; 2) data centric focus; 3) risk management practices; 4) cost-benefit analysis; and 5) strategic development (Kissoon, 2020).

Technology Landscape and Application Portfolio

The technology landscape is defined as the technology and information security measures in place within the enterprise architecture. This landscape is usually depicted through enterprise architecture artefacts that include but are not limited to the visual layout of the technology, system interfaces, communication channels, application portfolios, technology stack and security measures. This landscape extends from the on-premises environment to suppliers, service providers, agents and partners.

Data Centric Focus

Data classification, in the context of cyber risk management, is the classification of data based on its level of impact on an organization and includes collection, use, disclosure and retention. Protection of data is based on the data classification level, *i.e.*, public, internal use, confidential, or restricted. These levels define the type of cybersecurity safeguards that should be in place to adequately protect the data, regardless of how they are stored. Protection of data includes safeguards to minimize loss, theft, unauthorized access, use, disclosure, copying and modification.

Risk Management Practices

All organizations are confronted with risks that have the potential to negatively affect their business. Risk management practices in the financial services sector focuses on identifying, measuring and analyzing those threats to reduce material, reputation, opportunity and other costs. These practices utilize the enterprise risk management (ERM) framework, which is integrated with information security, privacy risk, vulnerability management, system and application development lifecycle and business continuity management (BCM).

Cost-Benefit Analysis for Cybersecurity Measures

Cost-benefit analysis is the widely accepted economic principle for managing an organization's resources. This principle requires that the costs of an activity be compared to the benefits. When the benefits exceed the costs, it pays to engage in those activities, whereas if the costs exceed the benefits, the opposite is true. When the costs and benefits of an activity are equal, the decision-maker may factor other qualitative measures into the decision.

The three major activities usually associated with cybersecurity are 1) protecting information from authorized users of the information; 2) making information available to authorized users on a timely basis; and 3) protecting information from integrity flaws.

Strategic Development

Business objectives are specific and measurable goals that an organization pursues as it focuses on growth, profitability, efficiency and stability. These objectives are interconnected with the enterprise strategy and appear directly within the business strategy and multi-year road map.

7.2. Digital Cybersecurity Risk Management Framework

Cybersecurity spending is discussed across the literature, and various approach-

es, methodologies and models are used. Using a case study methodology, the aim of this research is to demonstrate that a digital cybersecurity risk management framework may be utilized when evaluating and implementing cybersecurity measures. The digital cybersecurity risk management framework consists of: 1) risk assessment; 2) internal control assessment; 3) an understanding of the organization's risk appetite; and 4) risk mitigation strategy.

7.3. Risk Assessment

The risk assessment process identifies critical risk elements, examples are as follows:

1) Data classification
2) Strategic/Business requirements
3) Application development
4) Vendor relationships
5) Technology landscape
6) Legal/Regulatory
7) Brand /Reputational
8) Operational
9) Financial
10) Security/Fraud

Risk Prioritization: Assess the Inherent Risk

The risk assessment process is based on a questionnaire in which a set of questions are formulated for each risk element. Examples of question categories include:

- Financial loss
- Media attention
- Reportable to Regulator
- Impact to suppliers and employees
- Loss or damage to Information Systems

Each question can be answered in one of five ways, in increasing order of risk, such that a risk score between 1 and 5 can be assigned for that question based on two rating scales: likelihood and impact.

A quantitative inherent risk score can be calculated for each question, each risk element and the overall initiative as follows:

- Risk score per question: product of the likelihood and impact rating.
- Risk score per element: accumulating the numerical score per question and dividing it by the number of questions for a risk element.
- Risk score for the overall initiative: accumulating the numerical score per risk element and dividing it by the number of risk elements in each project.

This quantitative inherent risk score is assigned a qualitative risk score categorized as high, medium or low. The qualitative inherent risk score shows what element carries the most risk, making it simple for decision-makers to allocate resources.

Impact Rating Scale

Figure 4 below shows the quantitative scale for the impact rating based on a score of 1 - 5.

Likelihood Rating Scale

Figure 5 below shows the quantitative scale for the impact rating based on a score of 1 - 4.

Qualitative Inherent Risk Rating

Figure 6 below shows the scale of the qualitative inherent risk rating based on the quantitative inherent risk score.

Impact	Criteria
Critical **5**	• Financial loss of over $5 million. • International short-term negative media coverage with impact to market share. • Reportable to Regulator requiring corrective action plan and implementation dates. • Legal and regulatory impact to include: fees, fines, litigation, compliance enforcement, senior executive impact. • Significant Impact to suppliers and employees. • Significant loss or permanent damage to Information Systems; excessive downtime; over triple the expected RTO.
Major **4**	• Financial loss of $1 million up to $5 million. • National short-term negative media coverage, potential to lose market share. • Reportable to Regulator requiring corrective action plan. • Some senior managers are impacted. • Impact to suppliers and employees. • Major loss or damage to Information Systems, continuous downtime, increase to expected RTO.
Moderate **3**	• Financial loss of $500,00 up to $1 million. • Short-term negative media coverage. • Reportable to Regulator with potential of corrective plan to be provided. • Minimal impact to suppliers and employees. • Some loss or damage to Information Systems, intermittent downtime, possible to achieve expected RTO.
Minor **2**	• Financial loss of $100,000 up to $500,00. • No reputational damage. • No media attention. • Not reportable to Regulator. • Minimal impact to suppliers and employees. • Minimal loss or damage to Information Systems.
Insignificant **1**	• Financial loss up to $100,000. • No media attention. • Not reportable to Regulator. • No impact to suppliers and employees. • No significant loss or damage to Information Systems.

Figure 4. It shows a sample impact rating scale (Kissoon, 2020).

Likelihood	Criteria
Almost Certain 5	• Almost certain • No defined preventive controls, or no available data regarding potential rate of failure. • 85% to 100% chance of occurrence.
Likely 4	• Likely • Minimal preventive controls defined, or preventive controls are minimally effective. • 60% to 85% chance of occurrence.
Possible 3	• Possible • Preventive controls are in place, but minimal data exists to support effectiveness claims. • 35% to 60% chance of occurrence.
Unlikely 2	• Unlikely • Preventive controls are in place and data exists to support effective claims. • 10% to 35% chance of occurrence.
Rare 1	• Rare • Preventive controls are designed into the process, and supporting significant data exists to demonstrate effectiveness. • 0% to 10% chance of occurrence.

Figure 5. It shows a sample likelihood rating scale (Kissoon, 2020).

Inherent Risk	Quantitative Risk Calculation
High	Range: 10+
Medium	Range: 4 - 10
Low	Range: 1 - 4

Figure 6. It shows a sample Qualitative Inherent Risk Rating Scale (Kissoon, 2020).

7.4. Internal Controls Assessment

The internal control environment is defined as the technology and cybersecurity measure in place within the enterprise architecture. This landscape is usually depicted through enterprise architecture artefacts, which include but are not limited to diagrams, interfaces, communication channels and application/technology portfolios. In addition, it extends from the on-premises environment to suppliers, service providers, agents and partners. Therefore, in addition to internal assessments, external third-party assurance reports are utilized to assist with the assessment of the internal control environment.

Some organizations utilize a cybersecurity risk-based framework to manage cybersecurity risk. The industry framework has been established through NIST and is composed of three parts:

- the framework core
- the framework implementation tiers
- the framework profiles

Each framework component strengthens the integration between cybersecurity activities and business drivers. The framework core is a set of cybersecurity activities, desired outcomes and applicable references that are common across critical infrastructure sectors.

The core provides industry standards, guidelines and practices in a way that allows for communication of cybersecurity activities and outcomes from the executive level to the implementation/operations level.

The framework core consists of five concurrent and continuous functions – identify, protect, detect, respond, recover, as shown in Figure 7. When considered as a whole, these functions provide a high-level strategic perspective on the lifecycle of an organization's management of cybersecurity risk through assessment of the internal control environment.

The framework core then identifies underlying key categories and subcategories that are specific outcomes for each function. These outcomes are equated with informative references such as existing standards, guidelines, and practices for each subcategory.

Vendor Assurance Reports

As outsourcing service providers (OSPs) manage a significant amount of customer data, systems, processes and operations, their ability to manage associated risks while meeting increasing compliance requirements often emerges as a priority. Many service providers are reactive to third-party reporting due to the lack of full visibility in their reporting portfolios. Creating a library of enterprise-wide requirements and mapping individual obligations to corresponding controls can help identify gaps and overlaps. For example, an organization may have one control for regulating physical access to its data center, but it may align with 20 different internal and external requirements. An integrated library of requirements and control tests can make it easier to compile customer-centric reports.

Outsourcing is a growing trend, and companies increasingly depend on third-party providers to deliver critical services. The purpose of third-party reports, *i.e.*, SOC2 or ISAE3402 review, is to provide client auditors with an objective report that expresses an opinion about the control environment of a service

Figure 7. It shows the NIST cyber security framework which consists of five concurrent and continuous functions—identify, protect, detect, respond, recover (NIST, 2018).

organization. These reports are designed to provide assurances about the effectiveness of controls in place at a service organization, *i.e.*, SOC for Service Organizations: Trust Services Criteria (SOC2) assesses the security, availability, or processing integrity of the system used to process client information or the confidentiality or privacy of that information.

7.5. Organization's Risk Appetite

An organization's risk appetite is the amount of risk, on a broad level, that an organization is willing to accept as it tries to achieve its goals and provide value to stakeholders.

During the risk assessment process, an organization's residual risk is assessed to determine the remaining risk after internal controls are implemented. Assessing this risk shows the organization the areas where a gap or lack of internal control exists. Usually, this is the area of focus for key stakeholders as they determine the cost-benefit analysis and risk mitigation strategy. In essence, residual risk should be aligned with the organization's/business unit's risk profile within the risk tolerance level.

Specifically, the residual risk score is a qualitative score that is more granular than the score of inherent risk, as shown in Figure 8. Inherent risk is assigned based on one of three scores, high, medium or low, while residual risk is commonly assessed based on one of five or more scores: high, medium-high, medium, medium-low and low. This granularity highlights control implementation progress over time and better reflects changes in overall risk.

7.6. Risk Mitigation Strategy

In some circumstances, to align the residual risk with the organization's/business unit's risk appetite, further mitigation is required. Therefore, organizations are required to make decisions about funding cybersecurity activities in a manner consistent with the viewpoint of various stakeholders. Below is a risk treatment scale, which aligns the impact, likelihood and inherent risk rating scale to identify areas that may require governance and risk mitigation through senior management oversight and additional cybersecurity measures, as shown in Figure 9.

		Inherent Risk		
		Low	Medium	High
Control Effectiveness	Highly Effective	Low	Low	Medium-Low
	Effective	Low	Medium-Low	Medium
	Partially Effective	Low	Medium-Low	Medium-High
	Ineffective	Low	Medium	High
		Low	Medium	High
		Residual Risk		

Figure 8. It shows a sample residual risk rating scale (Optiv, 2011).

Impact					
Likelihood	Insignificant	Minor	Moderate	Major	Critical
Rare	LOW accept the risk, routine management	LOW accept the risk, routine management	LOW accept the risk, routine management	MEDIUM, specific accountability, risk mitigation plan	HIGH, quarterly senior management review
Unlikely	LOW accept the risk, routine management	LOW accept the risk, routine management	MEDIUM, specific accountability, risk mitigation plan	MEDIUM, specific accountability, risk mitigation plan	HIGH, quarterly senior management review
Possible	LOW accept the risk, routine management	MEDIUM, specific accountability, risk mitigation plan	MEDIUM, specific accountability, risk mitigation plan	HIGH, quarterly senior management review	HIGH, quarterly senior management review
Likely	MEDIUM, specific accountability, risk mitigation plan	MEDIUM, specific accountability, risk mitigation plan	HIGH, quarterly senior management review	HIGH, quarterly senior management review	EXTREME, monthly senior management review
Almost Certain	MEDIUM, specific accountability, risk mitigation plan	MEDIUM, specific accountability, risk mitigation plan	HIGH, quarterly senior management review	EXTREME, monthly senior management review	EXTREME, monthly senior management review

Figure 9. It shows a sample Risk Treatment Scale (Queensland Treasury and Trade, 2011).

Cost-benefit analysis is the widely accepted economic principle for managing an organization's resources. This principle requires that the costs of an activity be compared to the benefits. When the benefits exceed the costs, it pays to engage in those activities, whereas if the costs exceed the benefits, the opposite is true. When the costs and benefits of an activity are equal, the decision-maker may factor other qualitative measures into the decision.

The three major activities usually associated with cybersecurity are: 1) protecting information from authorized users of the information; 2) making information available to authorized users on a timely basis; and 3) protecting information from integrity flaws.

The costs associated with these activities are significant, as organizations will incur costs to detect and correct security breaches that cannot be prevented. The benefits of cybersecurity are directly related to the cost savings, known as cost avoidance, associated with preventing cybersecurity breaches.

The cost-benefit framework states that the goal of an organization should be to implement security procedures up to a point where the benefits minus the costs are maximized. In this framework, implementing cybersecurity activities beyond that point means that the incremental costs are maximized. Implementing cybersecurity activities beyond that point means that the incremental costs are greater than the incremental benefits of the additional security measures. In

essence, the net benefit of implementing incremental cybersecurity measures beyond the maximum point is negative and therefore represents a financial cost to the organization.

In contrast, the digital cybersecurity risk management framework has four areas of consideration: 1) alignment with the organization's risk appetite; 2) alignment with the risk assessment process; 3) understanding of the cost-benefit analysis; and 4) justification of risk mitigation strategy. Although cost-benefit analysis is impactful from a financial perspective, in some cases, other factors need to be considered to fully understand the impact of not implementing additional security measures. For example, the cost of preventive cybersecurity measures is usually not factored into the organization's cost-benefit analyses. Specifically, the cost of preventative security measures usually includes development and implementation of a continuous compliance monitoring program. The survey study showed that respondents from risk taking organizations are focused on implementation of foundational cybersecurity measures to meet mandatory compliance obligations. In addition, most organizations do not have the data to appropriately factor the cost/impact of a cybersecurity breach on an organization, *i.e.*, its effect on the organization's brand/reputation, legal/regulatory landscape, operational/technology environment, forensic/e-discovery-related items, third-party suppliers, and therefore the actual cost of remediating a cybersecurity breach is unrealized.

To adequately implement cybersecurity measures, in addition to cost-benefit analysis, stakeholders should implement an elaborate decision-making process to determine the additional security measures needed to adequately protect an organization from a cybersecurity breach while aligning with its risk appetite.

8. Case Study: ABC University is Exploring a Vendor Relationship to Utilize the Mobius Platform

Business Overview

With over 15 years in the market, the Möbius platform is used by students, teaching assistants and professors at some of largest institutions globally. Möbius is a robust online authoring and delivery environment specifically designed for the needs of STEM classrooms. It includes a suite of tools and features for authors looking to design and develop digital assets for their students or peers, and a delivery environment that enables and promotes deep and active learning for users through the combination of instructional material with hands-on activities.

The Möbius platform offers:

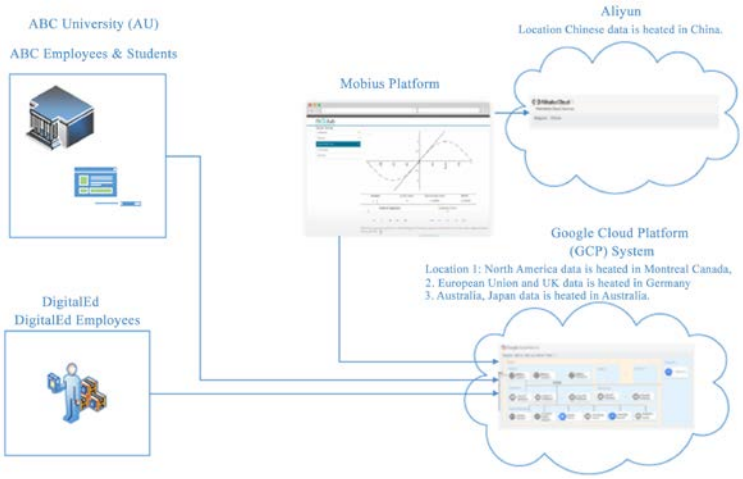
- A mechanism for creating and deploying online STEM courses.
- Lessons, assessments and interactive learning activities, it unfolds the potential for the STEM student to acquire knowledge at a guided yet self-defined pace.
- Complex STEM disciplines with its world-class math-engine.
- The ability to create and use powerful multimedia visualizations to anchor

key STEM concepts.

- Students immediate and meaningful feedback and provides instructors with data on student engagement and understanding.
- Advance question types with algorithmically generated and randomized questions.
- Access to high-quality content created by curriculum experts.
- Seamlessly integration with ABC's University Learning Management System (LMS).

Technical Overview

The Möbius Platform is vendor owned by DigitalEd. This cloud-based solution is hosted within the Google Cloud Platform System and the Alibaba Cloud.



8.1. Risk Assessment

Impact and Likelihood

The impact and likelihood rating scale located in the Section 7.3, outlines the evaluation of the protection requirement level for each protection requirement. The table below shows the impact and likelihood rating as it applies to the risk elements.

	Risk Element	Impact	Likelihood
1	Data Classification PII: The protection of PII is subject to routine risk assessment processes. A Privacy Impact Assessment (PIA) is managed by ABC University's Privacy's office. PII elements are captured and stored through this cloud hosted web application platform, specifically any personal information that is used with an ABC University student to include but not limited to: • Student information • Grades • Course information • Connectivity to the Learning Tool Interoperability Sensitive Authentication Data (SAD): is the information on a payment card used for authentication at the time of a purchase. This includes data from the full magnetic strip, card security code (CSC, CVV2, CID, CAV2) and personal identification number (PIN). The Mobius Platform facilitates payment card transactions from ABC University individuals, and therefore protection of sensitive authentication data is required by DigitalEd.	Major	Frequent

Continued

2	Business Requirements The Möbius Platform is used within the ABC University student environment to provide a comprehensive online courseware platform focusing on the unique needs of science, technology, engineering and mathematics students.	Moderate	Likely
3	Application Development Application develop is minimal to include integration with the Möbius Platform. Development includes standard interface within the University's Learning Management System (LMS) and connectivity to Learning Tool Interoperability (LTI).	Minor	Possible
4	Vendor Relationship DigitalEd is a privately held Canadian company, with approximately 65 employees worldwide. DigitalEd is an online learning company with a simple and resonant purpose to shape the world through digital learning. DigitalEd, introduced the Möbius platform in Spring 2017 with the intent to improve the online learning experiences of authors, instructors and students in science, technology, engineering and mathematics (STEM)-based classrooms.	Moderate	Likely
5	Technology landscape • Suppliers and third-party partners include Google Cloud Platform (GCP) System and Aliyun.	Major	Frequent
6	Legal/regulatory • Disclosure of data subject to specific regulatory requirement • Lawsuits by aggrieved owners of lost or compromised data, *i.e.*, PII. • Fines and penalties assessed by regulators.	Major	Possible
7	Brand/reputational • Unflattering or negative publicity due to press coverage which damages ABC University's brand. • Loss of customer confidence due to the release or compromise of data.	Minor	Possible
8	Operational • Loss of operations and use of system by authorized users.	Moderate	Likely
9	Financial • Significant costs to restore/repair any damages caused by intentional/unintentional users.	Minor	Possible
10	Security and fraud issues • Loss and/or manipulation of sensitive data, *i.e.*, PII through disclosure of authentication credentials, distributed denial of service attack, malware attack.	Major	Frequent

Inherent Risk

The inherent risk has been assigned based one of three scores of either high, medium or low, as shown in the below chart.

	Risk Element	Quantitative Inherent Risk Rating			Qualitative Inherent Risk Rating
		Impact	Likelihood	Rating	
1	Data Classification	4	5	20	High
2	Business Requirements	3	4	12	High
3	Application Development	2	3	6	Medium
4	Vendor Relationship	3	4	12	High
5	Technology Landscape	4	5	20	High
6	Legal/regulatory	4	3	12	High
7	Brand/reputational	2	3	6	Medium
8	Operational	3	4	12	High
9	Financial	2	3	6	Medium
10	Security and fraud issues	4	5	20	High
	Average			12.6	High

8.2. Internal Control Assessment: Effective

The core components of the NIST Cybersecurity Framework were utilized to adequately assess the DigitalEd environment supporting the Möbius Platform. Specifically, the following vendor assurance reports were provided: 1) Higher Education Community Vendor Assessment Tool (HECVAT)-Lite: DigitalEd; 2) System and Organization Controls (SOC) 2 Type II Report: Google Cloud Platform System for the Period May 1, 2019 to April 30, 2020; and 3) Payment Card Industry (PCI) Data Security Standard (DSS) self-assessment questionnaire (SAQ) as of March 21, 2019.

8.3. Organization's Risk Appetite

The residual risk is a MEDIUM rating for the Möbius Platform.

8.4. Risk Mitigation Strategy

Further risk mitigation recommendations can be utilized to align the organization's risk profile with the NIST Cybersecurity Framework core components. This area is essential as it provides recommendations to include additional cybersecurity measures that may provide a preventative approach. This would strengthen a risk-taking organization's risk profile without requiring the organization to transition to a risk averse profile. It is important to note that recommendations are not mandatory, and are used to identify additional cybersecurity measures to strengthen the organization's security posture while aligning with the organization's risk appetite.

Recommendations

Supplier Chain Risk Management

- ABC University should ensure that Aliyun is routinely assessed using audits, test results or other forms of evaluations to confirm they are meeting their contractual obligations.
- ABC University should ensure that response, recovery planning and testing are conducted with suppliers and third-party providers.

Identity Management, Authentication and Access Control

- Existing technology and processes within ABC University should be reviewed and appropriate security controls implemented to include integration with ABC University's LMS.
- The web-based interface should support authentication, including standards-based single-sign-on, leveraging multi-factor authentication and password/passphrase aging requirements.

Information Protection Processes and Procedures

- DigitalEd should consider implementing an approved disaster recovery process documentation.
- All components of DigitalEd's disaster recovery plan should be reviewed at least annually and updated as needed to reflect change.
- PII related Information Security controls:

- Protect transfer of data from ABC University to Cloud Hosting environment, *i.e.*, Google, Alibaba.
- Secure application programmable interfaces (API), examples include:
  - Creation of accounts for client applications.
  - Account updates to use HTTP basic authentication.
  - Granularity of access control to ensure each client application has access to the functions it needs for the applicable operation.
- The database containing PII located within the cloud hosting environment should:
  - Protect PII elements *i.e.*, encryption, masking, hashing.
  - Provide reports for database logging of administrator/administrator equivalent accounts for review by ABC University's management.
  - Implement integrity controls on database and system logs.

Awareness and Training

- Implement on-going training and awareness of employees in the handling and processing of PII and data privacy.

Security Monitoring

- The ability to monitor for intrusions within the DigitalEd environment.
- Integrate security/data related breach policies and procedures with ABC University's incident management process.

9. Ethical Considerations

Four critical ethical principles were reviewed when conducting this research study. Specifically, "1) avoidance of harm or loss of dignity; 2) transparency and honest; 3) right to privacy; and 4) researcher integrity", Rose, Spinks and Canhoto, [15]. Each key area was reviewed in terms of stakeholder groups, the researcher, the participants in the research study, and the impact on the industry.

10. Implication for Research, Practice and/or Society

It is apparent that although organizations have actively implemented cybersecurity frameworks, there is a need to enhance the decision-making process to reduce the number and type of breaches, and to strengthen the implemented cybersecurity frameworks to facilitate stronger preventive approaches. Decisions that are made by an organization when investing in cybersecurity controls are heavily focused on baseline compliance with government and industry regulations which may omit emerging technologies and continuous compliance management. It is evident from the data analyzed through the survey study that risk taking organizations implement cybersecurity measures when required, and therefore spend minimal in support of a foundational security posture. In addition, continuous compliance management to facilitate a preventative approach is nonexistent, resulting in unforeseen losses due to the impact of reoccurring cybersecurity breaches.

The decision-making process utilized when evaluating, implementing and in-

vesting in cybersecurity controls is weighted towards the technology organization and therefore may be biased on the basis of competing priorities. The outcome of this study provides greater insight into how an organization makes decisions when implementing cybersecurity controls. This exploratory research shows that most organizations are diligently implementing security measures to effectively monitor and detect cyber security attacks. Specifically showing that risk taking organizations implemented cybersecurity measures to meet compliance and audit obligations with an annual spend of $3.18 million. It also indicated that 23.6% of risk-taking organizations incurred more than 6 cybersecurity breaches with an average dollar loss of $3.5 million. In addition, the impact of a cybersecurity breach on risk taking organizations is as follows: 1) data loss; 2) brand/reputational impact; 3) financial loss fines; 4) increase oversight by regulators/internal audit; and 5) customer/client impact.

The implication this research has on practice is extensive, as it focuses on a broad range of areas to include risk, funding, type and impact of cybersecurity breaches encountered.

The survey study clearly demonstrated the need to utilize a digital cybersecurity risk management framework to integrate current industry frameworks within the risk management practice to include recommendations. This type of framework would provide a balanced approach to managing the gap between a risk-taking organization and a risk averse organization when implementing cybersecurity measures.

11. Further Work

There were several limitations of the research, and these can be incorporated into the next phase. Further development of the survey study instrument should be considered by leveraging a more robust tool such as Qualtrics and randomly allocating the positions of the questions to avoid order effects that may bias participants completing the survey. The partnership research design could be expanded to facilitate other quantitative and qualitative techniques in parallel with equal weight. In-depth data collection and analysis can be completed to facilitate broader data collection using grounded theory and data modelling techniques.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Kissoon, T. (2019) Optimum Spending on Cybersecurity Measures. *Transforming Government: People, Process and Policy*, **14**, 417-431. https://doi.org/10.1108/TG-11-2019-0112

[2] Dor, D. and Elovici, Y. (2016) A Model of the Information Security Investment Decision-Making Process. *Computer & Security*, **63**, 1-13. https://doi.org/10.1016/j.cose.2016.09.006

[3] Rue, R., Pfleeger, S. and Ortiz, D. (2007) A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. *Sixth Workshop on the Economics of Information Security*, Pittsburgh, 7-8 June 2007, 1-23.

[4] Cavusoglu, H., Mishra, B. and Ragunathan, S. (2004) A Model for Evaluating It Security Investments. *Communications of the ACM*, **47**, 87-92. https://doi.org/10.1145/1005817.1005828

[5] Cavusoglu, H., Raghunathan, S. and Raghunathan, W. (2008) Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, **25**, 281-304. https://doi.org/10.2753/MIS0742-1222250211

[6] Gordon, L.A. and loeb, M.P. (2002) The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, **5**, 438-457. https://doi.org/10.1145/581271.581274

[7] Gordon, L.A., Loeb, M.P. and Zhou, L. (2016) Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security*, **7**, 49-59. http://dx.doi.org/10.4236/jis.2016.72004

[8] Huang, C.D., Hu, Q. and Behara, R.S. (2008) An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm. *International Journal of Production Economics*, **114**, 793-804. https://doi.org/10.1016/j.ijpe.2008.04.002

[9] Purser, S.A. (2004) Improving the ROI of the Security Management Process. *Computers & Security*, **23**, 542-546. https://doi.org/10.1016/j.cose.2004.09.004

[10] Finne, T. (1998) A Conceptual Framework for Information Security Management. *Computers & Security*, **17**, 303-307. https://doi.org/10.1016/S0167-4048(98)80010-2

[11] Nazareth, D. and Choi, J. (2015) A System Dynamics Model for Information Security Management. *Information & Management*, **52**, 123-134. https://doi.org/10.1016/j.im.2014.10.009

[12] Comes, T., Hiete, M., Wijngaards, N. and Schultmann, F. (2011) Decision Maps: A Framework for Multi Criteria Decision Support under Severe Uncertainty. *Decision Support System*, **52**, 108-118. https://doi.org/10.1016/j.dss.2011.05.008

[13] Dutta, A. and Mccrohan, K. (2002) Management's Role in Information Security in a Cyber Economy. *California Management*, **45**, 67-87. https://doi.org/10.2307/41166154

[14] Pettigrew, A. (2009). The Politics of Organizational Decision-Making. Routledge, London.

[15] Easterby-Smith, M., Thorpe, R. and Jackson, P.R. (2015) Management & Business Research. Sage, London.