

2024

Assessing Organizational Investments in Cybersecurity and Financial Performance Before and After Data Breach Incidents of Cloud SaaS Platforms

Munther B. Ghazawneh

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



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

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

Assessing Organizational Investments in Cybersecurity and Financial
Performance Before and After Data Breach Incidents of Cloud SaaS
Platforms

by

Munther B. Ghazawneh

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

College of Computing and Engineering
Nova Southeastern University

2024

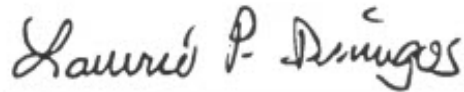
We hereby certify that this dissertation, submitted by Munther Ghazawneh conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.



Yair Levy, Ph.D.
Chairperson of Dissertation Committee

4/19/24

Date



Laurie P. Dringus, Ph.D.
Dissertation Committee Member

4/19/24

Date

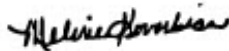


Junping Sun, Ph.D.
Dissertation Committee Member

4/19/24

Date

Approved:



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

4/19/24

Date

College of Computing and Engineering
Nova Southeastern University

2024

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

Assessing Organizational Investments in Cybersecurity and Financial
Performance Before and After Data Breach Incidents of Cloud SaaS
Platforms

by
Munther Ghazawneh
January 2024

Prior research indicated that providing inappropriate investment in organizations for Information Technology (IT) security makes these organizations suffer from IT security issues that may cause data breach incidents. Data breaches in cloud Software as a Service (SaaS) platforms lead to the disclosure of sensitive information, which causes disruption of services, damage to the organizational image, or financial losses. Massive data breaches still exist in cloud SaaS platforms which result in data leaks and data theft of customers in organizations.

IT security risks and vulnerabilities cost organizations millions of dollars a year as organizations may face an increase in cybersecurity challenges. The IT security risks and vulnerabilities exploit information through data breaches, which may harm the Confidentiality, Integrity, and Availability (CIA) of data, as well as lead to financial loss and failure of business. Data breaches impact organizational financial performance. Each organization has non-technical employees who do not have experience in cybersecurity. Organizations need to invest in effective cybersecurity activities such as Security Education, Training, and Awareness (SETA) to help their employees stay alert to avoid data breaches.

This study investigated the concepts of organizational financial performance indicators compared to organizations that operated cloud SaaS platforms before and after data breach incidents. IT security vulnerabilities are determined by certain organization's parameters such as technology, processes, and people. The main goal of this study was to empirically compare the role of organizational financial performance indicators on annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations. The organizations operate cloud SaaS platforms, and they reported in media between 2010 and 2023 that suffered from a data breach incident. This study empirically assessed the investments in cybersecurity as well as financial performance before and after data breach incidents that impacted different organizations. This study also addressed providing appropriate investment in organizations for IT security, which reduces cybersecurity issues that cause data breach incidents.

The research design for this study is defined as a multiple-case study analysis. A quantitative approach was used in this research study to collect and process the data provided as a sequential quantitative-qualitative survey to collect opinions from Subject Matter Experts (SMEs), as well as case samples from the LexusNexis database. This study also addressed the organizational financial performance indicators that may reduce cybersecurity risks and data breaches in cloud SaaS platforms in organizations. This research used an SME survey to first validate the organizational financial performance indicators relevant to organizational cybersecurity posture. Following the SMEs validation, the study used digital research news (LexusNexis database) to evaluate archived data of multiple past cases for data breach incidents in cloud SaaS platforms in different organizations. The multiple case study analysis was completed in two phases, which included a panel of SMEs and a case analysis of 100 organizations.

The results of this study indicated that there were significant differences in the annual budget for cybersecurity on liabilities and owner's equity account, as well as total expenses on IT on revenue and owner's equity account before and after a data breach incident. There were no significant differences in the annual budget for cybersecurity on revenue and total expenses on IT on liabilities before and after a data breach incident. There were significant differences in operating activities, investing activities, and financing activities on revenue, liabilities, as well as owner's equity account before and after a data breach incident. The results also indicated that there were significant differences in revenue, liabilities, and owner's equity account before and after data breach incident after controlling for number of total victims from a given organizational data breach, total organizational assets, as well as the size of the organization. There were no significant differences in revenue, liabilities, and owner's equity account before and after a data breach incident after controlling for the U.S. state where the organization is located.

Recommendations for future studies should expand their samples to include more organizations that are located inside and outside of the United States (U.S.). Future studies may include evaluating more past cases of data breaches in cloud SaaS platforms in organizations that suffered from data breach incidents. Future studies may also include proposing the appropriate investment in organizations to reduce data breaches and mitigate cybersecurity risks. The results of this study provided further understanding in the body of knowledge of mitigating data breaches by defining the organizational financial performance indicators that impact the risk of falling victim to such cybersecurity incidents.

Table of Contents

Abstract	ii
List of Tables	vii
List of Figures	x

Chapters

1. Introduction	1
Background	1
Problem Statement	3
Dissertation Goal	12
Research Questions	17
Relevance and Significance	19
Barriers and Issues	20
Assumptions, Limitations, and Delimitations	21
Assumptions	21
Limitations	22
Delimitations	22
Definition of Terms	23
List of Acronyms	26
Summary	27
2. Review of the Literature	30
Introduction	30
Investment in IT Security Due to Growing Pressure on Organizations	30
Impact of Providing Inappropriate Investment in Organizations' IT Security	32
Security Challenges in the Development of IT Used in Organizations	35
Existence of Data Breaches in Cloud SaaS Platforms	37
Loss and Disclosure of Customer Information Impacted by Data Breaches	42
Impact of Data Breaches on Confidentiality, Integrity, and Availability (CIA)	45
Data Breaches in Cloud SaaS Platforms Due to Unauthorized Access	50
Limiting Employees' Access to Data in Organizations Using Cybersecurity Controls	52
Organizations' Concerns about IT Security Vulnerabilities in Cloud SaaS Platforms	56
Financial and Legal Damages in Organizations Caused by Data Breaches	62
Proper Cybersecurity Implementation in Cloud SaaS Platforms by Organizations	69

Using Cybersecurity Posture by IT Security Leadership	72
Protection Software and Network Security in IT Security Techniques	75
Annual Budget for Cybersecurity	77
Total Annual Expenses on IT	80
Organizational Assets	84
Annual Organizational Liabilities	87
Annual Owners' Equity Accounts	91
Annual Organizational Revenue	93
Annual Operating Activities	96
Annual Investing Activities	99
Annual Financing Activities	101
Challenges in Defining Organizational Financial Performance Indicators for Mitigating Data Breaches	104
Comparing Organizational Financial Performance Indicators Before and After Data Breach Incidents	107
Evaluating Past Cases of Data Breaches in Cloud SaaS Platforms in Organizations	110
Summary of What Is Known and Unknown in Literature	113

3. Methodology 115

Overview of Research Design	115
Measures	117
Phase I Measures: SMEs Assessment	117
Phase II Measures: The Case Analysis of the 100 Organizations	118
Validity and Reliability	123
Proposed Sample	125
Phase I: SMEs Assessment	125
Phase II: The Case Analysis of the 100 Organizations	127
Pre-Analysis Data Screening	129
Data Analysis	130
Phase I: SMEs Assessment	130
Phase II: The Case Analysis of the 100 Organizations	130
Formats for Presenting Results	132
Resources	133
Summary	133

4. Results 136

Overview	136
Phase I – SME Survey Feedback and Findings	136
Phase I – RQ1	139
Phase I – RQ2	140

Phase I – Mean and Standard Deviation of Organizational Indicators	141
Phase I – SMEs Level of Agreement for Organizational Indicators (N=24)	143
Phase II – The Case Analysis of 100 Organizations	146
Phase II – RQ3	146
Phase II – RQ4	149
Phase II – RQ5	150
Phase II – RQ6	151
Phase II – RQ7	152
Phase II – RQ8	153
Phase II – Mean and Standard Deviation of Organizational Indicators Before and After Data Breach Incident	155
Summary	161

5. Conclusions, Implications, Recommendations, and Summary 166

Conclusions	166
Discussion	167
Implications for Practice	168
Implications for Research	168
Limitations	168
Recommendations and Future Research	170
Summary	171

Appendices

A. Example of SMEs' Invitation Email	178
B. Example of SME Survey	179
C. Organizational Indicators with Description	184
D. Data Collection Details	185
E. Institutional Review Board (IRB) Approval Letter	188

References 190

List of Tables

Tables

1. Literature Summary of Investment in IT Security 31
2. Literature Summary of the Impact of Providing Inappropriate Investment in IT Security 33
3. Literature Summary of Security Challenges in the Development of IT 36
4. Literature Summary of Existence of Data Breaches in Cloud SaaS Platforms 40
5. Literature Summary of Loss and Disclosure of Impacted Customer Information 44
6. Literature Summary of Impact of Data Breaches on CIA of Data 48
7. Literature Summary of Data Breaches Due to Unauthorized Access 51
8. Literature Summary of Limiting Employees' Access to Data Using Cybersecurity Controls 54
9. Literature Summary of Organizations' Concerns about IT Security Vulnerabilities in Cloud SaaS Platforms 59
10. Literature Summary of Financial and Legal Damages in Organizations Caused by Data Breaches 67
11. Literature Summary of Proper Cybersecurity Implementation in Cloud SaaS Platforms 71
12. Literature Summary of Using Cybersecurity Posture by IT Security Leadership 74
13. Literature Summary of Protection Software and Network Security in IT Security Techniques 76
14. Literature Summary of Annual Budget for Cybersecurity 79
15. Literature Summary of Total Annual Expenses on IT 82

16. Literature Summary of Organizational Assets	85
17. Literature Summary of Annual Organizational Liabilities	88
18. Literature Summary of Annual Owners' Equity Accounts	92
19. Literature Summary of Annual Organizational Revenue	95
20. Literature Summary of Annual Operating Activities	98
21. Literature Summary of Annual Investing Activities	100
22. Literature Summary of Annual Financing Activities	103
23. Literature Summary of Challenges in Defining Organizational Financial Performance Indicators	106
24. Literature Summary of Comparing Organizational Financial Performance Indicators Before and After Data Breach Incidents	109
25. Literature Summary of Evaluating Past Cases of Data Breaches in Cloud SaaS Platforms	111
26. Research Variables for Research Questions	122
27. Summary of Research Phases with Proposed Samples	131
28. Summary of SME Demographics (N=24)	137
29. Summary of Level of Agreement in Section A (N=24)	139
30. Summary of Level of Agreement in Section B (N=24)	140
31. Mean and Standard Deviation of Organizational Indicators of SMEs Feedback (N=24)	141
32. SMEs Level of Agreement for Organizational Indicators (N=24)	143

33. One-Way MANOVA Results of Difference in Annual Budget for Cybersecurity on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 147
34. One-Way MANOVA Results of Difference in Total Expenses on IT on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 150
35. One-Way MANOVA Results of Difference in Operating Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 151
36. One-Way MANOVA Results of Difference in Investing Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 152
37. One-Way MANOVA Results of Difference in Financing Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 153
38. One-Way ANCOVA Results of Difference in Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100) 155
39. Mean and Standard Deviation of Organizational Indicators Before and After Data Breach Incident (N=100) 156
40. Mean and Standard Deviation of Organizational Indicators for Each Organization Before and After Data Breach Incident (N=100) 157
41. Summary of Research Question Results 163

List of Figures

Figures

1. Interaction in Cloud Computing 59
2. Overview of Research Design Process 116
3. Organizational Financial Performance Indicators Before and After Data Breach Incidents 118
4. Conceptual Model for the Role of Organizational Financial Performance Indicators on Overall Organizational Financial Performances Before and After a Data Breach 122
5. Cloud SaaS Security 125
6. Mean and Standard Deviation of Organizational Financial Indicators of SMEs Feedback Related to RQ1 (N=24) 142
7. Mean and Standard Deviation of Organizational Financial Indicators of SMEs Feedback Related to RQ2 (N=24) 142
8. SMEs Level of Agreement for Organizational Indicators (OrgFinInd) with Cut-off Line for Minimum SMEs Consensus (N=24) 144
9. SMEs Level of Agreement for Organizational Indicators (IDBI-FI) with Cut-off Line for Minimum SMEs Consensus (N=24) 145
10. SMEs Level of Agreement for Organizational Indicators (Average of OrgFinInd and IDBI-FI) with Cut-off Line for Minimum SMEs Consensus (N=24) 145
11. One-Way MANOVA Results of Difference in Estimated Marginal Means of Revenue Before and After Data Breach Incident (N=100) 147

12. One-Way MANOVA Results of Difference in Estimated Marginal Means of Liabilities Before and After Data Breach Incident (N=100) 148
13. One-Way MANOVA Results of Difference in Estimated Marginal Means of Owner's Equity Account Before and After Data Breach Incident (N=100) 149

Chapter 1

Introduction

Background

Cloud computing appeared as a utility after the beginning of the Internet, where all technologies are available at any time and placed inside the “Internet Cloud” (Grubisic, 2014). Grubisic (2014) noted that many global projects can be categorized under Cloud computing and used as enterprise applications along with Software as a Service (SaaS) technology. Cloud SaaS architecture is implemented to support the needs of different users (Abbas et al., 2022). Abbas et al. (2022) noted that cloud SaaS implementation provides universal access to software or more general services to end users to use applications on a desired platform easily without knowing the main services infrastructure, which provides the required information and operations process. Cloud services may serve the information requirements of the software applications at the same time for both web and mobile applications (Grubisic, 2014).

Software and data are hosted on the servers of service providers in cloud-based environments, where they can be accessed through the Internet (Abbas et al., 2022). Users have access to real-time data anywhere and anytime using cloud solutions that do not require charges in advance (Diez et al., 2019). Diez et al. (2019) noted that their prices are set under a subscription system, which may cover all maintenance, upgrades, and support services. Cloud SaaS solutions will be cheaper, take less time to implement, and are easier to use (Grubisic, 2014). Cloud SaaS solutions offer organizations flexibility and growth based on Information Technology (IT) strategy and business needs that are supported by the IT team (Diez et al., 2019).

Data breaches are considered a common phenomenon that impacts computers, networks, and cloud-based platforms (Mohammed, 2022). Mohammed (2022) also noted that data breaches cause high financial costs as well as additional negative outcomes such as the negative reputation of the organizations. He noted financial costs associated with data breaches can cause loss of millions of dollars, restoration activities and lawsuits, as well as a decline in stock prices. Organizations are facing increasing cybersecurity challenges and the average cost of data breaches in the United States (U.S.) organizations reached millions of dollars (Nie & Xu, 2021). Nie and Xu (2021) noted that data breaches may impact victim organizations' short- and long-term financial performance.

Collecting large groups of sensitive customer data leads to privacy and IT security challenges that need to be considered by organizations (Kude et al., 2017). They also noted that one important challenge that has been reported in the media is the threat of large-scale data breaches, where external parties obtain unauthorized access to large amounts of sensitive customer data such as credit card and address information. Large-scale data breaches can be caused by internal or external parties at an organization that may utilize insecure software, introduce malware into the systems, or tamper with hardware (Kude et al., 2017).

Several vulnerabilities in IT systems prompt attackers to take greater chances to break into these systems, where inadequate examination for vulnerabilities in software may impact the organization's cybersecurity measures (Biswas & Mukhopadhyay, 2018). Biswas and Mukhopadhyay (2018) also noted that the study of the vulnerabilities' growth and their accurate prediction is essential to help minimize data breaches. Chief Technology

Officers (CTOs) may use effective IT security investments to reduce associated IT security risks (Biswas & Mukhopadhyay, 2018).

Cybercriminals unleash cyber-attacks and exploit vulnerabilities in organizational networks to successfully cause data breaches (Eling & Schnell, 2016). Eling and Schnell (2016) also noted that vulnerability is determined by certain organization's parameters such as technology, processes, and people. The cybersecurity level of an organization depends on the cybersecurity measures of other partners in the supply chain due to the public good features of IT security investments (Eling & Schnell, 2016).

IT security investments can change the probability or impact of IT security risks and data breach incidents (Hoppe et al., 2021). Hoppe et al. (2021) also noted that IT security investments are insufficient, but they are increasing, as well as the willingness of organizations to invest more money in IT security. Organizations make IT security investments and plan to increase their expenses on IT security investments, employee training, IT security consultants, and staffing or outsourcing (Eling & Schnell, 2016). It appears that IT security investments will never be sufficient if they are not associated with the necessary organizational financial performance indicators (Hoppe et al., 2021).

Problem Statement

The research problem that this study addressed is the growing pressure on organizations to prevent data breaches by investing in their IT security, especially as it pertains to their cloud computing and SaaS development (He et al., 2020). Providing inappropriate investment in organizations to assign a low budget for IT security makes these organizations suffer from IT security issues which may cause data breach incidents (Zhang et al., 2021). Zhang et al. (2021) also noted that organizations assign a high budget

for increasing cybersecurity to protect their employees and customers from data breach incidents.

Data breaches in organizational systems such as cloud SaaS platforms lead to the disclosure of sensitive information, which creates disruption of services, damage to the organizational image, or financial losses (Osuagwu et al., 2015). Data breaches are considered one of the most disruptive cybersecurity events in cloud SaaS platforms that organizations may face (Kaur & Bhardwaj, 2015; Singh & Malhotra, 2016). Massive data breaches still exist in cloud SaaS platforms which result in data leaks and data theft of customers such as credit card information (Akinbowale et al., 2020; Bhardwaj et al., 2016).

Fehér and Sándor (2019) noted that cloud SaaS is a service provided to consumers where they use the provider's cloud infrastructure applications. Examples of cloud SaaS platforms include Microsoft Azure, Amazon Web Service (AWS), GSuite as well as Salesforce (Fehér & Sándor, 2019; Spasic et al., 2019). Fehér and Sándor (2019) stated, "The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface" (p. 132).

Cloud SaaS platforms are applications used as services via the Internet that are deployed in data centers to manage resources within cloud computing (Yu & Wang, 2012). Yu and Wang (2012) stated, "SaaS applications are deployed in dynamic data centers with cloud computing technologies managing resources to achieve flexibility and scalability" (p. 197). Although cloud computing provides high-level security to its consumers, there are still many data breaches in cloud SaaS platforms (Singh & Malhotra, 2016).

Juma'h and Alnsour (2020) noted that the development of IT has many advantages for all organizations; however, such advantages also bring challenges including cybersecurity

and data breaches. The California Data Breach Report 2012-2015 is considered an example that describes the magnitude of data breaches (Juma'h & Alnsour, 2020). Juma'h and Alnsour (2020) stated, "The Attorney General has received reports on 657 data breaches, affecting over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk" (p. 276).

Dandapani (2017) noted that about 60% of managers who work in organizations throughout the world face data breaches, as well as more than 53% of financial institutions daily face data breach incidents. These incidents include stealing customers' passwords or information and using new techniques by hackers such as phishing (Dandapani, 2017). Dandapani (2017) stated:

At Target, corporation attackers installed malware on the company's network and stole credit information for more than 40 million customers and e-mails of 70 million customers. In 2014, hackers breached JP Morgan Chase's computer network, stealing gigabytes of data, and compromising sensitive account information of approximately 83 million households and small businesses. (p. 622)

Data breaches may result in the loss of customer information as well as identity theft, where data used by companies such as hospitality can provide extensive information on customers' lifestyles that can be disclosed by hackers (Gwebu & Barrows, 2020). Gwebu and Barrows (2020) also noted that hospitality, accommodation, as well as food service companies, have experienced dangerous data breaches due to the resumption of hacking and using malware, where these companies included Marriott, Hilton, Starbucks, McDonald's, and others. Gwebu and Barrows (2020) stated, "The industry has been

adversely affected by data breaches recently, including such iconic companies as Marriott, Starbucks, Hilton, Hyatt, Orbitz, Pizza Hut, Subway, and McDonald's" (p. 513).

Eling and Schnell (2016) noted that IT security investments in organizations rely on cybersecurity levels and measures, where these organizations can achieve successful IT security by investing an appropriate amount of money in the cybersecurity field. When attackers exploit information through data breaches, the attack may harm the confidentiality, integrity, as well as availability of data, which leads to financial loss or damage, and failure of business (Eling & Schnell, 2016). Eling and Schnell (2016) stated:

Depending on the aim of the attackers (e.g., espionage, sabotage, extortion, and exploiting information), the attack might compromise the availability of IT services, the integrity and confidentiality of data that in turn lead to monetary loss, reputational damage, and business interruption. (p. 476)

Cybersecurity controls are one main method by which organizations limit employees' access to data on cloud SaaS platforms (Kaur & Bhardwaj, 2015; Singh & Malhotra, 2016). Wang and Yongchareon (2020) stated, "Security controls are security measures and countermeasures that prevent, detect and mitigate the security risks of assets such as information, computer systems or other assets" (p. 499). Organizations provide these cybersecurity controls to determine which data an employee in the organization can access on these platforms, where these organizations can protect the confidentiality, integrity, as well as availability of their data, meet the IT security requirements, increase cybersecurity, and protect their business (Kaur & Bhardwaj, 2015; Wang & Yongchareon, 2020).

Organizations still have concerns about data security due to vulnerabilities in cloud computing, where data are distributed in the cloud through individual devices (Prasad et

al., 2013). Prasad et al. (2013) stated, "Industrious hackers can invade virtually at any server, and there are the statistics show that one-third of breaches result from stolen or lost laptops and other devices and from employees' accidentally exposing data on the Internet" (p. 138). Data breaches of cloud systems may lead to violation of data privacy, and this problem is a major risk in cloud SaaS platforms, while user data ownership is one of the main issues (Al-Marsy et al., 2021; Prasad et al., 2013). Coss and Dhillon (2019) stated, "Data ownership is also a privacy issue in cloud computing. These legal uncertainties may make it challenging to determine how to protect the privacy and confidentiality of users' information in the cloud" (p. 192).

Cloud SaaS platforms may have risks related to data security when data breaches lead to some problems such as data leakage that have an impact on the cloud system (Jouini & Rabai, 2014; Senyo et al., 2016). Palanisamy and Wu (2021) noted that security can be impacted in cloud SaaS platforms in organizations with the issues of data access level based on data analysis. Although IT security teams work to identify any suspicious activities on cloud SaaS platforms, the risk of data breaches is still eminent due to users' continuous risky cyber activities (Palanisamy & Wu 2021; Senyo et al., 2016).

Kude et al. (2017) noted that it could be impossible to completely protect organizations, which take advantage of big data from data breaches through technological or managerial actions. This difficulty can arise because there are several possible sources of data breaches such as hacking or losing devices (Kude et al., 2017). Organizations need to properly implement security in the cloud to reduce the chance of data breaches (Harrison et al., 2015; Khayer et al., 2021).

Several organizations have the desire to store their resources in the cloud, but they may have concerns about the risks associated with storing data in the cloud (Khayer et al., 2021). Data breaches have led to many financial and legal damages to organizations, such as the famous 2014 Target data breach that happened in the U.S. (Karanja & Rosso, 2017). Karanja and Rosso (2017) noted the resignation of Target's Chief Executive Officer (CEO), Gregg Steinhafel, after Target suffered from a massive data breach in 2014. At that time the company was "on track to make a \$39.4 million settlement with the financial institutions impacted by the data breach" (p. 37).

IT security leadership uses cybersecurity posture to define information assets, applications that run the main business processes, as well as confidential information (Granneman, 2018; Karanja & Rosso, 2017). Granneman (2018) stated, "Once the information security leadership, governance structure, and security framework have been created, the organization can assess its security posture" (pp. 4-5). Jia and Stan (2021) noted that cybersecurity depends on large investments in organizations, whereas implementing effective cybersecurity governance depends on investments to reduce data breaches by using different techniques. These techniques may include protection software packages such as antivirus and cryptographic software, as well as network security systems such as firewalls (Jia & Stan, 2021).

Annual budget for cybersecurity such as in the U.S. is a financial investment that organizations report on their annual financial reports related to the total expenditures provided to protect organizational systems (Chidinma et al., 2019). As non-technical employees are not cybersecurity experts, organizations need to develop Security Education, Training, and Awareness (SETA) programs to help their employees stay alert

to avoid data breaches (Zhang et al., 2021). Zhang et al. (2021) stated, "An adequate annual budget for [SETA] programs needs to include funding for training resources, consulting, testing, advertising, software/hardware and/or professional services costs" (p. 629). Providing an appropriate annual budget to build SETA programs is needed because cybersecurity prevention continuously changes to keep up with new methods that attackers cause data breaches (Chidinma et al., 2019; Zhang et al., 2021).

Total annual expenses on IT are all annual expenses that an organization spends to support its IT department and operations including hardware, software, networks, as well as Research and Development (R&D) to provide an impact on gross operating profit (Hua et al., 2020). Sukumar et al. (2020) stated, "Because of the huge size of their net sales or revenues, R&D expenditures still would account for just a small proportion, thus giving a false impression that these firms do not adequately invest in these important activities" (p. 973). Organizational R&D expenses can be measured by their total annual expenses on IT, representing their overall R&D annual investments (Sukumar et al., 2020).

Organizational assets are the broadest asset category in the organization's framework which includes all structural and intellectual assets (Boulton et al., 2000). Boulton et al. (2000) also noted that this category includes leadership, strategy, systems, processes, brands, and proprietary knowledge to help build a successful business for the organization's economy. Boulton et al. (2000) stated:

Organizational assets provide the glue that holds a company together. By allowing one asset to work with another, one system to talk to another, and one decision to mesh with another, they are crucial to galvanizing an organization to respond to the challenges of the New Economy. (p. 33)

Annual organizational liabilities are the liabilities established by contractual relationships with the organization's customers to determine the degree of annual liability for the performance of work (Sizov et al., 2015). Sizov et al. (2015) stated, "At realizing of technical and technological supervision the method of providing liability under supervisor services contract is a penalty, yet the customer is not obliged to prove the amount of losses for undetected defects and failures in production technology" (p. 5). Annual owners' equity accounts in the organization are the annual results of the evaluation procedures that the organization applies to its assets and liabilities (Reilly, 2018). Reilly (2018) stated, "The total net operating assets should equal the total long-term debt (including the current portion of that debt) plus the total owners' equity recorded on the company balance sheet" (p. 182).

Annual organizational revenue is the total annual income generated by the sale of goods or services related to the business operations, which are performed by the staff and employees in the organization who are expected to be available to do their work efficiently on this business (Couture, 2017). Couture (2017) stated, "The Agency had a time accounting system where all the work carried to deliver the services requested by the customers was recorded and could then be compiled into management reports indicating progress against the forecasted revenue" (p. 68). Annual operating activities are defined as the annual main revenue generator which focuses on producing and selling products, goods, as well as services (Jeletic, 2012). Gunawan and Lina (2015) stated, "Operating activities are all transactions relating to the earnings reported in the profit (loss). Details of the activity and the value of cash flows from operating activities can be seen in the consolidated financial statements precisely in sheet cash flows" (p. 312).

Annual investing activities are the activities related to the acquisition as well as disposal of long-term assets with other investments, which are not cash equivalents or included in cash equivalents (Türkössey, 2013). Gunawan and Lina (2015) stated, "Investing activities are the acquisition or disposal activity of long-term assets (current assets) and investments that are not included in the definition of cash equivalents" (pp. 312-313). Annual financing activities are the activities that change the equity capital and the borrowing structure of the entity, the result of changes in the size, as well as the composition of the equity along with the borrowings of the entity (Türkössey, 2013). Gunawan and Lina (2015) stated, "Financing activities are activities that result in changes in the amount and composition of liabilities (debt) and long-term capital" (p. 313).

One of the most important challenges in mitigating data breaches is defining the organizational financial performance indicators that impact the risk of falling victim to such cybersecurity incidents (Saxena et al., 2020). Saxena et al. (2020) also noted that organizational financial performance indicators can be compared in the organization that operates cloud SaaS platforms before and after data breach incidents. Thus, it appears that additional research is needed for assessing the organizational investment in cybersecurity, as well as organizational financial performance indicators that may reduce data breaches in cloud SaaS platforms (Granneman, 2018; Jia & Stan, 2021; Saxena et al., 2020). Also, additional research is needed for evaluating past cases of data breaches in cloud SaaS platforms in organizations, where employees and customers suffered from data breach incidents (Dandapani, 2017; Kayes et al., 2020; Zhang et al., 2021).

Dissertation Goal

The main goal of this research study was to empirically compare the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations. The organizations operate cloud SaaS platforms, and they reported in media between 2010 and 2023 that suffered from a data breach incident (Bhardwaj et al., 2016; Javidi et al., 2014; Ramluckan & van Niekerk, 2014).

The need for this work is demonstrated by the work of Aleem and Ryan (2013), Kaur and Bhardwaj (2015), as well as Khayer et al. (2021), who concurred that there is always a cybersecurity risk when using cloud SaaS platforms, where organizations have a significant risk for business failure due to data breaches, as well as using cloud SaaS platforms pushes the organizations to assess the cybersecurity concerns as a requirement for business success. The lack of control and knowledge of storing organizations' data in cloud SaaS platforms may cause inconvenience related to data breaches, where this may potentially lead to organizational financial problems (Kaur & Bhardwaj, 2015; Ramluckan & van Niekerk, 2014). Khayer et al. (2021) noted that several challenges face cloud computing such as lack of data security. Cybersecurity mitigation controls provide several levels of protection against data breaches in protecting customers' and employees' sensitive data from disclosure (Colicchia et al., 2019). Colicchia et al. (2019) also noted that the problems in IT systems may include website crashes and network failure, where these problems could happen by cyber attackers leading to financial loss and corruption of

services. Colicchia et al. (2019) stated, "Another risk debated in the literature is represented by the problems connected to the IT systems such as the crash of websites and the failure of companies' IT networks, leading to the unavailability of critical services" (p. 219).

This dissertation builds on previous research of Harrison et al. (2015), Khayer et al. (2021), Palanisamy and Wu (2021), as well as Zhang et al. (2021) by seeking to empirically compare the financial performance indicators when assessing annual organizational revenue, liabilities, as well as owners' equity account before and after data breach incidents of organizations that operate cloud SaaS platforms. The higher expected cost for investment in the organization corresponds to its lower failure cost, which means that the organization adopts a plan to reduce data breaches to invest in the safeguards designed to mitigate cybersecurity risks (Harrison et al., 2015; Zhang et al., 2021). Zhang et al. (2021) also showed on the contrary that a higher failure cost for the organization corresponds to its lower expected cost for investment, which means that the organization does not invest in the safeguards to reduce cybersecurity risks caused by data breaches, as well as it may accept its existing cybersecurity posture. Cloud SaaS platforms in organizations may face cybersecurity risks which include integrity where information cannot be changed by unauthorized users, availability where information may not be available to authorized users when they need it, as well as confidentiality where improper disclosure of information can be detected and prevented (Khayer et al., 2021; Palanisamy & Wu, 2021).

This study had eight specific goals. The first goal of this research study was to empirically validate, using Subject Matter Experts (SMEs), a set of proposed organizational financial indicators based on literature to assess organizational

cybersecurity posture for those that operate cloud SaaS platforms. The second goal of this research study was to empirically validate, using SMEs, a set of proposed organizational financial indicators that are relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms. SMEs are important elements for knowledge acquisition in different organizations that may include different types of employees or customers, as well as they are indicators of the role of knowledge in decision-making in the organizations (Murumba et al., 2020). Providing appropriate investment for cybersecurity has a positive impact on organizational performance, where financial indicators are subject to the research of identifying the best organizational investment (Murumba et al., 2020; Špaček, 2021).

The third goal of this research study was to empirically compare *the annual budget for cybersecurity* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. As organizations need cybersecurity to implement various solutions, all expenses for the cybersecurity implementation are required to be included in the annual budget of the organization's cybersecurity (Lamarca, 2020). Lamarca (2020) also noted that the various solutions may include protecting sensitive data, vulnerability scanning, risk assessment, IT security auditing, Enterprise Firewall, Virtual Private Network (VPN), as well as intrusion detection systems within the enterprise risk management.

The fourth goal of this research study was to empirically compare *total annual expenses on IT* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and

reported in media between 2010 and 2023 that suffered from a data breach incident. Total annual expenses on IT in organizations fund activities to analyze IT security vulnerabilities as well as IT governance, where vulnerability estimation and prediction can assist in IT risk assessment (Biswas & Mukhopadhyay, 2018).

The fifth goal of this research study was to empirically compare *annual operating activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. Implementing cybersecurity programs prevents fraud and performs risk vulnerability assessments for organizations to protect their business (Klamut, 2018). Klamut (2018) noted that audit activities are used to improve the monitoring and detection of fraud, where the ranking of the audit activities indicates focusing on annual operating activities along with financial risk as well as information management processes.

The sixth goal of this research study was to empirically compare *annual investing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. Investment banks are the direct source of payment for cardholders' credit card bills, where the incomes of the credit card issuers can be gained from annual investing activities in banks (Fan et al., 2018). Fan et al. (2018) also noted that some companies such as Target and Home Depot suffered from data breach incidents within the credit card issuing industry that affected annual investing activities, where traditional credit cards were subject to exposing private information when swiping these cards to complete transactions.

The seventh goal of this research study was to empirically compare *annual financing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. A cloud SaaS platform may include financial and human resource data along with organizational financial performance indicators, which are extracted from the business information of the organization to assess the data breach impact on annual financing activities for the business performance (Costa et al., 2021).

The eighth goal of this research study was to empirically assess if there are any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident when controlling for: (a) the number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located. Integrated performance-based maintenance management develops methods to integrate indicators for the performance and the efficiency of maintenance in organizations, where these indicators are organizational financial performance indicators of the maintenance unit which impact annual organizations' revenue (Yousefli et al., 2017). Organizational financial performance indicators are considered maintenance key performance indicators which can be used for integrating maintenance management, as well as manufacturing control to result in successful operations in these organizations along with protecting annual liabilities (Naji et al., 2020). Using traditional models based on ratio analysis for estimating the probability

of default for organizations may not help monitor the financial issues, where some key factors for these financial issues are the return on assets as well as the structure of current assets (Lukashevich & Garanin, 2016).

Research Questions

The main research question that this study addressed was: What is the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of organizations that operate cloud SaaS platforms that were reported in media between 2010 and 2023 to suffer from a data breach incident? This study had eight research questions:

RQ1: What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms?

RQ2: What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms?

RQ3: Are there any statistically significant mean differences for *the annual budget for cybersecurity* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ4: Are there any statistically significant mean differences for *total annual expenses on IT* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ5: Are there any statistically significant mean differences for *annual operating activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ6: Are there any statistically significant mean differences for *annual investing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ7: Are there any statistically significant mean differences for *annual financing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ8: Are there any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and

reported in media between 2010 and 2023 that suffered from data breach incidents after controlling for: (a) number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located?

Relevance and Significance

There has been a massive utilization of cloud computing in support of IT operations in organizations in recent years, which also has some challenges related to cybersecurity (Humayun et al., 2022; Singh & Dutta, 2014). Humayun et al. (2022) also noted that there have been critical threats to cloud security including data breaches, which are ranked as the top threat to cloud systems. Cloud SaaS platforms in organizations may still suffer from cyber threats, and they need to provide appropriate investment for IT security to reduce data breaches (Humayun et al., 2022; Singh & Dutta, 2014). Singh and Dutta (2014) noted that the cloud with huge information may become a target for attackers during data breaches.

Any organization may have at least one data breach incident that affects its employees or customers if it does not have a strong cybersecurity posture (Jácome et al., 2021; Nagarajan & Kumar, 2021). Jácome et al. (2021) also noted that the number of Personally Identifiable Information (PII) of the organization's employees and customers may reach millions, which may cause distrust in the organization. The organizational systems can be subject to cybersecurity vulnerabilities, especially if the customers need to store information in these systems such as credit cards (Jácome et al., 2021; Nagarajan & Kumar, 2021). Nagarajan and Kumar (2021) noted that this will lead to negative reputational and

financial impact on organizations, where these organizations cannot achieve success with their customers due to investing low budget in cybersecurity and data protection.

Although cloud computing with SaaS development will be costly for organizations under the item of total annual expenses on IT, organizations still need to invest in cybersecurity by providing the appropriate amount of annual budget for cybersecurity (Nagarajan & Kumar, 2021). Jácome et al. (2021) noted that organizations provide high investments to increase their systems security, which reduces cybercrimes such as data breaches that can happen due to the spread of malware. IT security managers work with their teams to provide data protection for their systems including cloud SaaS platforms (Zimba & Chama, 2018).

This study empirically assessed the organizational investments in cybersecurity and financial performance before and after data breach incidents. This study focused on organizations that operate cloud SaaS platforms, which were impacted by data breach incidents that were reported in the media between 2010 and 2023 (Jácome et al., 2021; Nagarajan & Kumar, 2021; Zimba & Chama, 2018).

Barriers and Issues

This study used a group of about 24 SMEs to empirically evaluate the financial indicators by completing the given survey. SMEs were contacted again through LinkedIn by sending them individual messages if they did not take the SME survey or skipped the message. The SMEs were selected and contacted from different organizations, where SMEs are expected to have experience in both cybersecurity and organizational financial indicators. Institutional Review Board (IRB) approval was required to conduct this research study, and about 24 SMEs were expected to take the survey in this research study.

This study plan was to reach out to 100 SMEs to get the 24 SMEs to participate in the SME survey as the response rate is about 24%. The SME survey contained demographic questions that asked the SMEs if they had a good level of expertise in both cybersecurity and finance.

This study used the LexusNexis database to find 100 sample cases for data breach incidents in cloud SaaS platforms, as well as this study limited the sample cases between 2010 and 2023 to keep up with new technologies. This study also needed the complete annual financial reports for the organizations that suffered from data breach incidents based on the 100 sample cases. The financial reports helped define the organizational financial performance indicators that impact the risk of falling victim to such cybersecurity incidents, as well as the indicators that help mitigate data breaches (Chidinma et al., 2019).

An organization may have branches inside and outside the U.S., where a data breach incident may impact customers or employees in the U.S. besides other countries. This study investigated the data breaches that happen in different locations of the organization. Using online libraries such as Alvin Sherman Library as well as digital research news such as LexusNexis database can be another potential barrier if any issue exists to block access for these platforms. Blocking the access may have impacted this research study and the data collection.

Assumptions, Limitations, and Delimitations

Assumptions

It was assumed that SMEs were honest when answering the survey and that the complete financial reports were obtained to help define the organizational financial performance indicators within this study, that impact the risk of falling victim to data

breach incidents. It was assumed that enough SMEs and sample cases for data breach incidents in cloud SaaS platforms obtained from the LexusNexis database were found to achieve an acceptable sample size, which provided validity for the statistical analysis that was performed. It was assumed that all SMEs from different organizations are experts in organizational financial indicators by collecting the information about them in the survey and relying on the accuracy of their reported experience. It was assumed that some organizations may have prior data breaches that SMEs may not have known about.

Limitations

A limitation of this study was that SMEs were chosen by convenience sampling. The population used in this study was limited to English-speaking employees who work in organizations. Another limitation was that SMEs used in this study could access cloud SaaS platforms on desktops and laptops in their organizations. A limitation for the 100 organizations found data breach incidents that impacted the organizations between 2010 and 2023, where the impact reached the cloud SaaS platforms and affected employees and customers. Another limitation for the 100 organizations found all their annual financial reports online for the years before and after the data breach incidents with the organizational financial performance indicators that include an annual budget for cybersecurity, liabilities, owners' equity accounts, revenue, operating activities, investing activities, financing activities, as well as total expenses on IT.

Delimitations

A delimitation of this study was that the LexusNexis database was used to find a sample of 100 cases of data breach incidents in cloud SaaS platforms. Another delimitation of this study was that these sample cases only include U.S. organizations. This is a potential

delimitation given that there is not the same level of censorship in the U.S. that exists in other countries. Reporting of data breach incidents in the U.S. is made public when reporters find the incidents, but reporters cannot report the incidents without government approval in other countries.

Definition of Terms

Annual Budget for Cybersecurity - A financial investment that organizations report on their annual financial reports related to the total expenditures provided to protect organizational systems (Chidinma et al., 2019).

Annual Financing Activities - The activities which change the equity capital as well as the borrowing structure of the entity, result in changes in the size, and composition of the equity along with borrowings of the entity (Türkössy, 2013).

Annual Investing Activities - The activities related to the acquisition as well as disposal of long-term assets with other investments, which are not cash equivalents or included in cash equivalents (Türkössy, 2013).

Annual Operating Activities - The annual main revenue generator that focuses on producing and selling products, goods, as well as services (Jeletic, 2012).

Annual Organizational Liabilities - The liabilities established by contractual relationships toward the organization's customers to determine the degree of annual liability for the performance of work (Sizov et al., 2015).

Annual Organizational Revenue - The total annual income generated by the sale of goods or services related to business operations that are performed by the staff and employees in the organization (Couture, 2017).

Annual Owners' Equity Accounts - The annual result of the evaluation procedures that the organization applies for its assets and liabilities (Reilly, 2018).

Business Email Compromise (BEC) - A type of scam that targets organizations with wire transfers and suppliers overseas. (Kolouch, 2018).

Cloud SaaS Platforms - Applications used as services via the Internet that are deployed in data centers to manage resources within cloud computing (Yu & Wang, 2012).

Cloud Software as a Service (SaaS) - A service provided to the consumers where they use the provider's cloud infrastructure applications (Fehér & Sándor, 2019).

Cybersecurity - A feature in a technical system designed and developed by computer programmers to create security procedures for protecting the system from threats and vulnerabilities (Bella, 2020).

Cybersecurity Controls – “Security measures and countermeasures that prevent, detect and mitigate the cybersecurity risks of assets such as information, computer systems or other assets” (Wang & Yongchareon, 2020, p. 499).

Data Availability – The case where data may not be available to authorized users when they need it (Khayer et al., 2021; Palanisamy & Wu, 2021).

Data Breach - A breach of security that leads to the accidental or unlawful destruction, loss, change, unauthorized disclosure, or access to an individual's data in a technical system (Nield et al., 2020).

Data Confidentiality - Improper disclosure of information can be detected and prevented (Khayer et al., 2021; Palanisamy & Wu, 2021).

Data Integrity – The case where data or information cannot be changed by unauthorized users (Khayer et al., 2021; Palanisamy & Wu, 2021).

Hacker - A technical individual who has skills in IT to achieve a goal within a computer system using illegal means, such as exploiting vulnerabilities or breaching data (Jamieson, 2019).

Identity Theft - A fastest-growing online crime that affects the online retail industry by stealing an individual's whole identity, his personal information, or his bank card details (Maitlo et al., 2019).

Information Technology (IT) - The use of computers to create, process, store, retrieve, as well as exchange all types of electronic information and data, where this technology can be used with business operations in different organizations (Wibowo et al., 2019).

Malware - Malicious software that is used to harm computers or servers by stealing information, corrupting files, or implementing harmful activities to annoy the users of these computers or servers (Tahir, 2018).

Organizational Assets - The broadest asset category in the organization's framework which includes all structural and intellectual assets (Boulton et al., 2000).

Organizational Financial Performance Indicators - Indicators defined in organizations and used in mitigating data breaches, as well as assessing organizational investments in cybersecurity and financial performance (Saxena et al., 2020).

Personally Identifiable Information (PII) – “The data which can be used to identify a person” (Kulkarni & Cauvery, 2021, p. 508).

Phishing - A fraudulent or tricky act that aims to gain information about the user such as username, password, credit card number, PIN, or other information to be used by the attacker (Kolouch, 2018).

SQL Injection – “One type of web application vulnerability where unwanted SQL queries are injected to an application input. If successful, this allows the attacker to add or delete database content and browse e-mails, passwords, and personal information of website users.” (Kouatli, 2014, p. 419).

Total Annual Expenses on IT - All annual expenses that an organization spends to support its IT department and operations including hardware, software, as well as networks to provide an impact on gross operating profit (Hua et al., 2020).

List of Acronyms

ANCOVA	Analysis of Covariance
API	Application Programming Interface
BEC	Business Email Compromise
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISA	Cybersecurity and Critical Infrastructure Agency
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
CV	Covariate Variable
DV	Dependent Variable
FBI	Federal Bureau of Investigation
IC3	Internet Crime Complaint Center
ICT	Information and Communications Technology

IDBI-FI	Impact of Data Breach Incidents on Organizational Financial Indicators
IoT	Internet of Things
IRB	Institutional Review Board
IT	Information Technology
IV	Independent Variable
MANOVA	Multivariate Analysis of Variance
OrgFinInd	Organizational Financial Indicators Evaluation
PII	Personally Identifiable Information
R&D	Research and Development
RQs	Research Questions
SaaS	Software as a Service
SETA	Security Education, Training, and Awareness
SMEs	Subject Matter Experts
SPSS	Statistical Package for the Social Sciences
SQL	Structured Query Language
U.S.	United States
VPN	Virtual Private Network

Summary

Data breaches are still an open problem that costs organizations millions of dollars every year (Kaur & Bhardwaj, 2015; Singh & Malhotra, 2016). Data breaches continue to present a significant cybersecurity threat to users in organizations that leads to reputation loss with their customers or employees (Akinbowale et al., 2020; Bhardwaj et al., 2016).

The research problem that this study addressed is growing pressure on organizations to prevent data breaches by investing in their IT security in cloud SaaS platforms (He et al., 2020). Providing inappropriate investment in organizations with a low budget for IT security makes these organizations suffer from low cybersecurity posture, which then causes their networks and cloud SaaS platforms to be more vulnerable to data breaches (Zhang et al., 2021).

This research study was to assess if the organizational investments in cybersecurity and IT expenses increased after data breach incidents (Wang & Yongchareon, 2020). This study used organizational financial performance indicators, which are defined in organizations and used in mitigating data breaches, as well as assessing organizational investments in cybersecurity and financial performance (Saxena et al., 2020).

The main research question that this study addressed was: What is the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? The first specific research question addressed what the SMEs' approved organizational financial indicators are to be valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms. The second specific research question addressed what the SMEs' approved organizational financial indicators are relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms.

The third through seventh research questions addressed if there are any statistically significant mean differences in the annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. The eighth specific research question addressed whether there are any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for: (a) the number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located.

This study was relevant and significant because data breaches in cloud SaaS platforms are still a significant problem that needs to be addressed to reduce data breaches among end users in organizations, where organizations still have concerns about data security due to vulnerabilities in cloud computing. This study proposed an appropriate investment in organizations to reduce data breaches and mitigate cybersecurity risks.

Chapter 2

Review of the Literature

Introduction

In this chapter, a literature review was used to provide an assessment of the organizational investment in cybersecurity and organizational financial performance indicators that may reduce data breaches in cloud SaaS platforms (Granneman, 2018; Jia & Stan, 2021; Saxena et al., 2020). The literature offers a summary of relevant literature related to cybersecurity challenges, vulnerabilities, and data breaches. Literature reviews are needed so that the researcher can gain a better understanding of prior research on a topic to find out what has been done, what the issues are, and how the analysis was performed (Al-Marsy et al., 2021; Palanisamy & Wu, 2021; Prasad et al., 2013; Zhang et al., 2021). Using a quantitative approach and quality resources, researchers can build a solid foundation for their research (Wen-ai et al., 2012). Quality peer-reviewed journals were searched for research to support relevant data and findings for the study.

Investment in IT Security Due to Growing Pressure on Organizations

Cloud computing is used within IT across different industries to replace the need of organizations to buy, rent, or lease on-premises solutions, as well as cloud computing allows organizations to access flexible models and pay for IT services on an on-demand basis (Gashami et al., 2020; Kumar et al., 2021). However, the disadvantages of cloud computing solutions may include inflexibility, the need for a significant investment of money, and the requirement for a permanent IT team to solve any technical issues, as well as the need to invest in IT security to maintain and protect the organizational systems that use the cloud computing services (Gashami et al., 2020; Chang et al., 2022). Many

organizations may fail to provide adequate cybersecurity to their IT systems, where the damage cost for an organization impacted by a data breach incident is often insufficient to force the organization to invest enough in cybersecurity (Verstraete & Zarsky, 2022).

Organizations look at their cybersecurity spending as a cost center for their businesses, where information security investments that include training, technology purchases, and improved information security culture are considered burdens for the organizations (Kumar et al., 2021). Thus, cloud computing requires appropriate technology investment for users, which makes adoption of IT easier for organizations that might find a trouble to invest large amounts of money in their systems and technology to facilitate ongoing maintenance of IT systems, as well as cloud SaaS platforms inside organizations (Schniederjans et al., 2016). However, organizations and IT personnel need technical knowledge to decide on investment to deploy a new strong cybersecurity posture in cloud SaaS platforms, which may include vulnerability scanning, vulnerability monitoring, as well as intrusion detection systems used by organizations with a large technology infrastructure (Chang et al., 2022; Webb & Aly, 2020). The studies discussed in this section are summarized in Table 1.

Table 1

Literature Summary of Investment in IT Security

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Verstraete & Zarsky, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Many organizations may fail to provide adequate cybersecurity in their IT systems to reduce data breach incidents.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gashami et al., 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Investing in IT security can maintain and protect organizational systems.
Kumar et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Information security investments can be considered as a load for organizations.
Schniederjans et al., 2016	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Investment in cloud computing has helped facilitate the ongoing maintenance of cloud computing services.
Webb & Aly, 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations and IT personnel need technical knowledge to decide about investment for a strong cybersecurity posture
Chang et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	IT security services invested in organizations may vary based on the organization's technology infrastructure

Impact of Providing Inappropriate Investment in Organizations' IT Security

Investment in cybersecurity at an organization helps build activities to face the crisis of the rapid growth in data breaches, where the crisis can impact the organization's

trustworthiness and efficiency (Diers-Lawson et al., 2021). However, organizations need to understand the terms of their businesses and industries to decide on the most appropriate implementation strategies, which need the appropriate investments to reduce IT security risks (Stojkovic & Butt, 2022). Therefore, if an organization's attention increases towards cybersecurity, it will help improve the information transparency and the information environment for the organization (Zhang et al., 2021). Lee (2022) showed that organizations can develop an overall data IT security plan to minimize the threats of data breaches and prioritize investment budgets for high-level cybersecurity projects.

Stojkovic and Butt (2022) noted that the challenges of technology along with cybersecurity add pressure and force organizations to focus on more tactical targets because the time spans to resolve the technical challenges may take a long time. However, organizations' refusal to make adequate investments in cybersecurity will increase the probability of data breaches with all harms that happen in organizations (Spinello, 2021). Jiang and Wang (2022) added that inappropriate investment can impact the market structure of an organization as well as destroy the flow of factors between its business and industry. Zhang et al. (2021) also showed that the increase in an organization's information disclosure that is restricted by inappropriate investment may impact the organization's reputation. The studies discussed in this section are summarized in Table 2.

Table 2

Literature Summary of the Impact of Providing Inappropriate Investment in IT Security

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Stojkovic & Butt, 2022	Empirical	Commentary	Digital Libraries	Challenges of technology and cybersecurity add pressure and force

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Diers-Lawson et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	organizations to focus on more tactical targets. Investment in cybersecurity helps build activities to face the crisis of the rapid growth in data breaches
Spinello, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations' refusal to make adequate investments in cybersecurity increases the probability of data breaches
Zhang et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations restricted by inappropriate investment may impact the organizations' reputation.
Jiang & Wang, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Inappropriate investment can impact the market structure of an organization and destroy its business.
Lee, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations can develop an overall data IT security plan and prioritize investment budgets for high-level cybersecurity projects

Security Challenges in the Development of IT Used in Organizations

Although users do not implement technical procedures during the work process, more data breaches were discovered by users compared with the data breaches that were discovered by the organization's technology team or internal process, as well as technology cannot provide complete security by itself (Carlton et al., 2019). However, technology firms support financial institutions such as banks that are firstly responsible for affected stakeholders and customers when a confidential data breach happens, as well as technology firms help improve customer confidence in electronic commerce, business transactions, and cloud SaaS platforms due to the rising number of cybersecurity incidents (Uddin et al., 2020). Berlilana et al. (2021) showed that both cybersecurity and technology have a significant impact on organizational IT security performance, where increasing cybersecurity, as well as technology, can help organizations obtain great features in organizational IT security performance. The features in IT security performance may include reduced data breaches, great security reputation, as well as increased security for processing information (Berlilana et al., 2021).

General data protection regulation will affect the development of cloud computing and artificial intelligence because the algorithms that support their processes require a high percentage of accuracy, as well as efficiency when analyzing personal data (Poritskiy et al., 2019; Thamik & Wu, 2022). However, Poritskiy et al. (2019) showed that general data protection regulation can help increase consumer confidence, which may lead to an increase the sales in organizations, encourage organizations to make more investments in cybersecurity, as well as hiring cybersecurity professionals and data protection officers. Also, a sound cybersecurity posture may focus on enhancing identity authentication,

executing control mechanisms, and IT security audits, but the cybersecurity posture still cannot be compared with the high level of IT security to prevent data breach incidents in organizations (Poritskiy et al., 2019; Zhao et al., 2022). Zhao et al. (2022) added that the need for authentication to protect privacy increased after data breaches had happened in some companies such as Equifax and Alteryx.

There may be challenges to using new technologies to handle personal data in organizations, where personal data will operate as big data used in the cloud systems (Poritskiy et al., 2019). As technology is used in many fields with highly changing possibilities, artificial intelligence needs to be carefully examined in terms of positive and negative impacts on organizations from two different perspectives (Thamik & Wu, 2022; Uddin et al., 2020). Thamik and Wu (2022) showed that the theoretical perspective indicates the technological advancements from a human perspective that includes behavioral, cultural, ethical, and social market perspectives, as well as the practical perspective indicates that the primary concerns of artificial intelligence used in organizational systems should be safety and privacy, where the organization's members should make the systems within their control. The studies discussed in this section are summarized in Table 3.

Table 3

Literature Summary of Security Challenges in the Development of IT

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Carlton et al., 2019	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	More data breaches were discovered by users compared with the data breaches discovered by the technology team.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Uddin et al., 2020	Empirical	Commentary	Digital Libraries	Protection laws can help improve customer confidence in electronic commerce and cloud SaaS platforms.
Berlilana et al., 2021	Empirical	Commentary	Digital Libraries	IT security performance features will include reduced data breaches and increased security for processing information.
Poritskiy et al., 2019	Empirical	Commentary	Digital Libraries	General data protection regulation will affect the development of cloud computing and artificial intelligence
Thamik & Wu, 2022	Empirical	Commentary	Digital Libraries	Artificial intelligence needs to be carefully examined in terms of positive and negative impacts on organizations
Zhao et al., 2022	Empirical	Commentary	Digital Libraries	Great cybersecurity posture still cannot be compared with the high level of IT security to prevent data breach incidents.

Existence of Data Breaches in Cloud SaaS Platforms

Cloud computing is considered multitenant, which means many users share the same cloud environment, as well as Internet access is considered a challenge in cloud computing, where cloud service providers offer many resources to be used by many online users (Georgiou & Lambrinoudakis, 2020; Kamariah et al., 2018). Georgiou and

Lambrinoudakis (2020) noted that as cloud SaaS platforms are based on the Internet, data can be stolen by hackers for fraudulent purposes that impact data privacy in different industries. Alghofaili et al. (2021) showed that there are many attacks on cloud SaaS platforms, such as phishing, fraud, and data breaches that may impact the platforms' infrastructure.

Data breaches can lead to stealing a legitimate user's identity, such as credentials and credit card information, as well as help cyber attackers seize user information when using cloud SaaS platforms, where the information such as username and password can be used by the attackers to attack the platforms (Alghofaili et al., 2021; Vida et al., 2022). Similarly, some sensors used in Internet of Things (IoT) tools can disclose sensitive information such as passwords and credit card information to violate user privacy, as well as use the information for future attacks (Krishna et al., 2021). Torre et al. (2018) added that stealing or buying hacked digital data to obtain a competitive advantage is easier than in the past, which leads to creating a real data marketplace on the dark web, where hackers buy and sell hacked and stolen data.

There has been a growing number of cyber-attacks caused by data breaches that impacted different organizations across all businesses and industries such as the public sector, as well as healthcare, where cloud SaaS platforms are considered the greatest number of confirmed data breaches, especially in finance, information, and educational sectors (Griffy-Brown et al., 2017). Donner and Steep (2021) added that many organizations have suffered from data breaches that impacted millions of their customer records related to sensitive information, such as social security numbers, addresses, and credit card information. Similarly, millions of users have been affected by data breaches in

the past decades, where cloud computing was implemented on untrusted devices with low security (Patwary et al., 2021).

Although cloud computing is protected by firewalls, authentication, and authorizations, vulnerability in cloud computing providers may still lead to data breaches by other untrusted and malicious users (Kamariah et al., 2018). Vida et al. (2022) showed that many cyberattacks exploit organizational systems' vulnerabilities, where unpatched vulnerabilities lead to 60% of data breaches. Therefore, some organizations use vulnerability risk management as an essential aspect of information security management, which is used to identify, evaluate, and reduce IT security vulnerabilities (Kamariah et al., 2018; Vida et al., 2022).

Most data breaches happen due to financial reasons or cyberespionage, such as Yahoo which has experienced a massive data breach of its user data, where the stolen data was later sold on the dark web for \$300,000 per unit (Torre et al., 2018). Donner and Steep (2021) added that Equifax is an example of a credit-scoring company that suffered from a data breach incident. Also, about 250,000 data leak implications have been reported in many organizations in different countries, such as the Careem taxi service that lost 14 million users' data, which included names, email addresses, phone numbers, and trip data from the Middle East and North Africa in 2018 (Aslam et al., 2022).

Data breaches become more frequent and dangerous, which require valid and secure methods for data protection by restricting access to sensitive data, as well as specifying how the data should be protected (Renwick & Martin, 2017). Patwary et al. (2021) showed that about 74% of Information and Communications Technology (ICT) executive officers have rejected adopting cloud computing due to the associated privacy and IT security risks

for cloud systems, where ICT executive officers considered the privacy boundary is authentication while the confidentiality boundary is access control and trust management. However, organizations need to protect important information such as credit card information and medical records related to their customers, which can be subject to cyber-attack in the cloud by untrusted and malicious users (Aldossary & Allen, 2016). The studies discussed in this section are summarized in Table 4.

Table 4

Literature Summary of Existence of Data Breaches in Cloud SaaS Platforms

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Georgiou & Lambrinouidakis, 2020	Empirical	Commentary	Digital Libraries	Internet access is a challenge in cloud computing that is used by many online users.
Alghofaili et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	Data breaches help cyber attackers seize user information when using cloud SaaS platforms.
Donner & Steep, 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Many organizations have suffered from data breaches that impacted sensitive information, such as social security numbers and credit card information.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Aldossary & Allen, 2016	Empirical	Commentary	Digital Libraries	Credit card information and medical records could be subject to cyber-attack in the cloud by untrusted users.
Renwick & Martin, 2017	Empirical	Commentary	Digital Libraries	Restricting access to sensitive data can be used as a valid secure method for data protection.
Vida et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	Unpatched vulnerabilities caused 60% of the data breaches in organizational systems.
Torre et al., 2018	Empirical	Commentary	Digital Libraries	Most data breaches happen for financial reasons or cyber espionage that may cause massive data breaches.
Aslam et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	About 250,000 data leak implications have been reported in many organizations in different countries including the Middle East and North Africa.
Krishna et al., 2021	Empirical	Commentary	Digital Libraries	Some sensors used in IoT tools can disclose sensitive information to violate user

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Patwary et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	privacy and use the information for future attacks. About 74% of ICT executive officers have rejected adopting cloud computing due to the associated privacy and IT security risks in cloud systems.
Kamariah et al., 2018	Empirical	Commentary	Digital Libraries	Vulnerability in cloud computing providers may still lead to data breaches by untrusted users.
Griffy-Brown et al., 2017	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Patterns were classified as confirmed data breach incidents such as crimeware that happened in the public sector and healthcare.

Loss and Disclosure of Customer Information Impacted by Data Breaches

Credit card information, customer information, and employee data are all subject to data breaches, where data breaches compromise consumer privacy, as well as lead to a violation of trust, which makes the consumer or buyer realize that the seller's failure violated the contract between the seller and the buyer (Mohammed, 2022; Wei et al., 2019). Wei et al. (2019) added that any data breach of customer information privacy based on the violation of trust can be considered a service failure, which leads to the customers' bad

perceptions of service quality presented by the organization. Solove and Citron (2018) showed that Equifax reported a cyber-attack may have impacted around 143 million of its U.S. customers, where the cyberattack resulted in a data breach of sensitive customer information, as well as hackers released data from a website that revealed customers' personal and financial data. Mohammed (2022) also added that Equifax has been compromised many times since 2013 when Equifax used Mandiant to provide cybersecurity services and cyber risk analysis. Similarly, the Target data breach spilled information on around 70 million customers, and the data breach was reported in late 2013 (Solove & Citron, 2018).

Several organizations observe an increased risk of cyber threats as countries throughout the world started to become developed by increasing the use of computer and Internet technology, but the technology will increase the chances of electronic theft, as well as cyber-crimes (Mohd Aizuddin et al., 2019). Plave and Edson (2018) gave CareFirst, Inc. an example of the impact of a data breach incident in 2014, where hackers obtained access to CareFirst databases that contain sensitive customer information. CareFirst members filed a suit that stated breach of contract, negligence, and violation of various state customer protection laws, but the D.C. Circuit Court dismissed the case due to lack of standing, as well as finding that the risk of harm to CareFirst members was too hypothetical (Mohammed, 2022). However, the D.C. Circuit Court in the U.S. can be ready to consider the threat of future harm as sufficient to establish a position in a case related to data breaches (Mohammed, 2022; Plave & Edson, 2018).

The higher number of data breach incidents can be related to the number and type of individuals with access to sensitive information in financial institutions such as banks

(Posey Garrison & Ncube, 2011). Mohd Aizuddin et al. (2019) showed that customer information in the traditional business environment is limited to a few employees or there is a limited access time, such as general retail and restaurant workers who have access to credit card information with limited opportunity for a data breach. Also, student social security numbers have been used as a means of identification, where teachers in schools often have continuous access to the sensitive information of their students (Posey Garrison & Ncube, 2011). The studies discussed in this section are summarized in Table 5.

Table 5

Literature Summary of Loss and Disclosure of Impacted Customer Information

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Mohammed, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Credit reports, customer information, and employee data are all subject to data breaches.
Wei et al., 2019	Empirical	Commentary	Digital Libraries	Data breaches compromise consumer privacy and lead to a violation of trust.
Solove & Citron, 2018	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Equifax cyberattack resulted in a data breach of sensitive customer information that may have impacted around 143 million of its U.S. customers

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Plave & Edson, 2018	Empirical	Commentary	Digital Libraries	The D.C. Circuit Court in the U.S. may consider the threat of future harm sufficient to establish a position in a case related to data breaches
Mohd Aizuddin et al., 2019	Empirical	Commentary	Digital Libraries	Several organizations see an increased risk of cyber threats due to countries' development by increasing the use of computer and Internet technology
Posey Garrison & Ncube, 2011	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The higher number of data breach incidents can be related to the number and type of individuals with access to sensitive information in organizations.

Impact of Data Breaches on Confidentiality, Integrity, and Availability (CIA)

Organizations should focus on three essential goals when building an IT security infrastructure that includes confidentiality, integrity, and availability (Spinello, 2021). Georgiopoulou et al. (2020) added that data protection principles should be maintained in cloud SaaS platforms by using several service-level cybersecurity measures to ensure the confidentiality, integrity, and availability of the recommended processed data. However,

the protection principles help cloud customers protect their data to support organizational IT security commitments and compliance requirements of general data protection regulation (Georgiopoulou et al., 2020; Spinello, 2021).

Confidentiality indicates that IT systems must keep valuable data private or inaccessible, which is achieved by tools such as access controls and encryption software, as well as indicates that unauthorized access to data, data destruction, or data modification by any unauthorized entity leads to losses at an organization (Sharma & Sehrawat, 2020; Spinello, 2021). Integrity indicates protecting information systems from being improperly altered or compromised, which is achieved using various tools that obstruct the efforts of hackers to infect a system with malware, as well as indicates that the rareness of integrity controls at the data level may lead to deep obstructions in future (Sharma & Sehrawat, 2020; Spinello, 2021). Availability indicates that employees and customers can use an IT system at an organization without disruption, which is achieved by safeguarding online platforms from denial-of-service attacks, as well as indicates that the data exists with service providers or third-party vendors, but the users cannot benefit from it due to several problems such as bandwidth or service provider system failure (Sharma & Sehrawat, 2020; Spinello, 2021).

Threats and attacks to IT security, as well as data integrity, availability, and confidentiality, are identified as significant factors for cloud users (Joia & Marchisotti, 2020). Harmandeep and Kumar (2018) defined a cybercrime caused by cyberattacks on the Internet as a malicious activity that can impact the three fundamental principles of IT security, which include confidentiality, integrity, and availability, as well as cybercrimes may include some terms such as fraud and stealing that are used on the Internet with

different techniques. Torre et al. (2018) also showed that as privacy issues are one of the concerns in data security, Big Data brings more security challenges, where Big Data security concerns are related to three features of data that include confidentiality, integrity, and the availability of data.

The main objectives of an information security management system are to maintain the confidentiality, integrity, and availability of information by applying a risk management process, as well as to give confidence to interested parties in mitigating IT security risks (Torre et al., 2018). Similarly, data security and privacy include protection of the integrity and confidentiality of the available data, as well as threats and attacks against cloud computing security when the used systems are vulnerable (Alaoui & El, 2022; Joia & Marchisotti, 2020). However, IT security and privacy management are considered major challenges associated with cloud computing implementation in organizations (Joia & Marchisotti, 2020).

The vulnerable systems can be considered a significant issue that continues to bring users' attention when using cloud systems because the issue is not simple or easily solved in cloud computing (Georgiopoulou et al., 2020; Joia & Marchisotti, 2020). Similarly, web vulnerabilities are continuously growing due to the large use of web applications such as cloud SaaS platforms (Alaoui & El, 2022). Thus, many cloud SaaS platforms can be vulnerable and subject to data breaches if there is an intrusion caused by unauthorized access to the platforms (Alaoui & El, 2022; Nagarajan & Kumar, 2021). The studies discussed in this section are summarized in Table 6.

Table 6

Literature Summary of Impact of Data Breaches on CIA of Data

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Georgiopoulou et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Data protection principles help cloud customers protect their data to support organizational IT security commitments and compliance requirements of general data protection regulation.
Spinello, 2021	Empirical	Commentary	Digital Libraries	Organizations should focus on three essential goals when building an IT security infrastructure that will include confidentiality, integrity, and availability.
Sharma & Sehwat, 2020	Empirical	Commentary	Digital Libraries	Existing data with service providers or third-party vendors (data availability) and the rareness of integrity controls at the data level may lead to deep obstructions in the future (data integrity). Unauthorized access to data or data modification by any unauthorized

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Harmandeep & Kumar, 2018	Empirical	Commentary	Digital Libraries	A cybercrime is a malicious activity that can impact the three fundamental principles of IT security, which include confidentiality, integrity, and availability.
Torre et al., 2018	Empirical	Commentary	Digital Libraries	Big Data brings more security challenges, where Big Data security concerns are related to three features of data that will include confidentiality, integrity, and availability.
Joia & Marchisotti, 2020	Empirical	Commentary	Digital Libraries	Data security and privacy include protection of the integrity and confidentiality of the available data when the used systems are vulnerable.
Alaoui & El, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	Many cloud SaaS platforms can be subject to data breaches if there is an intrusion caused by unauthorized access.

Data Breaches in Cloud SaaS Platforms Due to Unauthorized Access

Successful cloud computing can be identified by the accessibility of computer resources (Chang et al., 2022). However, the Internet is changing methods of computing rapidly, which leads to increasing opportunities for malicious intrusions (Rawindaran et al., 2021). Ahmad et al. (2022) showed that cloud systems are more subject to phishing attacks than other systems, as well as a malicious user can obtain access to login information to log into a cloud system, where the malicious user can be a former or existing employee in the organization. Therefore, when malicious users obtain access to data, the data becomes vulnerable and other malicious users can seize vulnerable data (Rawindaran et al., 2021).

When the device or mobile is used for personal use too, authorized users may process the data outside of the organization with a lack of security, which may lead to illegal access to confidential data in the cloud without the organization's authorization (Palanisamy & Wu, 2021). However, mobile wireless networks used in transmitting data within an organization are subject to intentional security attacks, as well as more vulnerable to a malicious attack, which may affect the confidentiality and integrity of data compared with desktop computers (Wang & Yongchareon, 2020). Palanisamy and Wu (2021) showed that when a device or mobile that accesses organizational systems is lost or stolen, there is a potential IT security risk of losing critical data if they are not stored on the organizational systems.

Organizations can ensure the protection of information in systems and applications in the network, as well as its support for information processing facilities within the IT security (Wang & Yongchareon, 2020). Georgiopolou et al. (2020) added that cloud SaaS

providers need to place response mechanisms for data breach incidents to immediately identify and respond to the incidents that lead to unauthorized access in cloud SaaS platforms. Similarly, many intrusion detection systems were designed to protect personal information in organizations from data breaches due to unauthorized access to the cloud (Chang et al., 2022). Also, IT security may include controlling information security in networks, connecting services to authorized access, transferring policies and procedures, securing business transfers between the organization and external parties, as well as defining confidentiality or non-disclosure agreements (Wang & Yongchareon, 2020). The studies discussed in this section are summarized in Table 7.

Table 7

Literature Summary of Data Breaches Due to Unauthorized Access

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ahmad et al., 2022	Empirical	Commentary	Digital Libraries	Cloud SaaS systems are more subject to phishing attacks than the other systems in many organizations.
Rawindaran et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Obtaining malicious users to access data can make the data vulnerable and other malicious users can seize vulnerable data
Chang et al., 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Many intrusion detection systems were designed to protect personal

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Georgiopolou et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	information in organizations from data breaches Cloud SaaS providers use response mechanisms to immediately identify and respond to data breach incidents.
Palanisamy & Wu, 2021	Empirical	Commentary	Digital Libraries	Organizational networks can be subject to intentional security attacks, which may affect the confidentiality and integrity of data.
Wang & Yongchareon, 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations can ensure the protection of their systems and the support for information processing facilities.

Limiting Employees' Access to Data in Organizations Using Cybersecurity Controls

Data access is based on privilege access, where access for a particular user should not be given to all locations in a cloud SaaS platform if the user does not need access to other locations, or s/he is only allowed to use a certain location in the platform, such as the user who is not an accountant and is not allowed to access payroll data for the organization's employees, the payroll access should not be granted to the user (Perry, 2021). However,

organizations with a larger number of customers in their databases may have a larger cybersecurity footprint than organizations with a smaller number of customers in their databases, as well as cloud systems may have gaps related to IT security vulnerabilities that are subject to exploitation by cyber-attackers (Levy & Gafni, 2021; Malatji et al., 2019). Similarly, some organizations may have outdated or incomplete cybersecurity posture in their current business, which mainly focuses on IT (Sezer & Caliyurt, 2018). Levy and Gafni (2021) also showed that organizations with greater cybersecurity controls may still have a larger number of customers in their databases, while their general cybersecurity footprint is smaller due to their abilities to mitigate and contain cyberattacks more quickly.

Organizations must collaborate with IT and information security leaders to design, develop, as well as coordinate guidelines or practices to address the IT security needs of the organizations (Sezer & Caliyurt, 2018). However, IT security employees should understand the organization's desire to resist and reduce cyber threats by performing continuous auditing on cybersecurity controls, as well as having a strong partnership with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) to assess cloud service providers (Bozkus Kahyaoglu & Caliyurt, 2018). Malatji et al. (2019) added that cybersecurity strategists and IT security employees at an organization may use techniques to validate the security features in the cloud systems. However, IT security employees should also understand the full impact of cyber threats on the organization by including their risk-based security plan at the same time, as well as proactively identifying apparent cybersecurity risks (Bozkus Kahyaoglu & Caliyurt, 2018; Malatji et al., 2019).

Organizations usually implement cybersecurity posture on a case-by-case basis due to focusing on the main approach of IT, as well as having an integrated approach to overcome cybersecurity risks, where there is limited awareness of cybersecurity risks at the organizational level to accurately manage the cybersecurity risks (Sezer & Caliyurt, 2018). Kosseff (2018) showed that the Data Privacy Act contains several exceptions that allow cloud service providers to monitor networks and share information with the government. However, it can be more difficult for the government and private sector to work together to mitigate cyber-attacks due to limited restrictions on monitoring the networks (Sezer & Caliyurt, 2018). Kosseff (2018) added that the Data Privacy Act restrictions on access to data are essential to protect privacy, as well as prevent the government and organizations' overreach, where the privacy protections may obstruct the potential for cooperation between the government and the private sector to enhance the cybersecurity posture. The studies discussed in this section are summarized in Table 8.

Table 8

Literature Summary of Limiting Employees' Access to Data Using Cybersecurity Controls

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Levy & Gafni, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations with greater cybersecurity controls may still have a larger number of customers in their databases.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Malatji et al., 2019	Quantitative Survey	24 SMEs	Surveys for SMEs	Techniques used by cybersecurity strategists and IT security employees can validate the security features in the cloud systems.
Bozkus Kahyaoglu & Caliyurt, 2018	Quantitative Survey	24 SMEs	Surveys for SMEs	IT security employees' understanding of the full impact of cyber threats and the organization's risk desire can help reduce cyber threats.
Sezer & Caliyurt, 2018	Quantitative Survey	24 SMEs	Surveys for SMEs	Some organizations may have outdated or incomplete cybersecurity posture in current business focusing on IT.
Perry, 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Data access is based on privileged access given to the right user for using cloud SaaS platforms in organizations.
Kosseff, 2018	Empirical	Commentary	Digital Libraries	Data Privacy Act contains several exceptions that allow cloud service providers to monitor networks and share information with the government.

Organizations' Concerns about IT Security Vulnerabilities in Cloud SaaS Platforms

Kouatli (2014) showed that the main strength of cloud computing is also one of its weaknesses, which is technically completely based on the Internet. The main issue of security in cloud computing is the existence of many and various technologies connected through the same IT infrastructure, which includes networks, databases, operating systems, as well as virtualization (Brumă, 2020; Kouatli, 2014). Aleem and Ryan Sprott (2013) considered IT security threats as the third highest threat that is followed by insecure Application Programming Interface (API), shared technology vulnerabilities, and the corrupt use of cloud computing. Brumă (2020) added that data breach incidents can be later used by cyber-attackers within the software design and implementation processes. Adee and Mouratidis (2022) showed that the impact of data breaches through cyberattacks can be harmful to organizations that employ cloud computing services, where the impact includes loss of data and leakage of confidential information, loss of clients' trust in the organizations, as well as contribution to large financial setbacks. Similarly, cyber-attacks on cloud SaaS platforms can give a chance to financial threats to individuals by losing or exposing their confidential data (Kumar et al., 2020). If cyber-attacks cause any connectivity failure in cloud systems, the whole business and operation will freeze in organizations (Kouatli, 2014).

The vulnerabilities of on-premises technologies are applicable in cloud computing and have a high-level impact generated by cyber-attacks, where cyber-attacks have caused business damage to organizations, as well as impacted the image of brands for a long-term period (Brumă, 2020). However, one of the significant issues in the cloud data center is protecting clients' sensitive data from leaking over the Internet and cyber-attacks, where

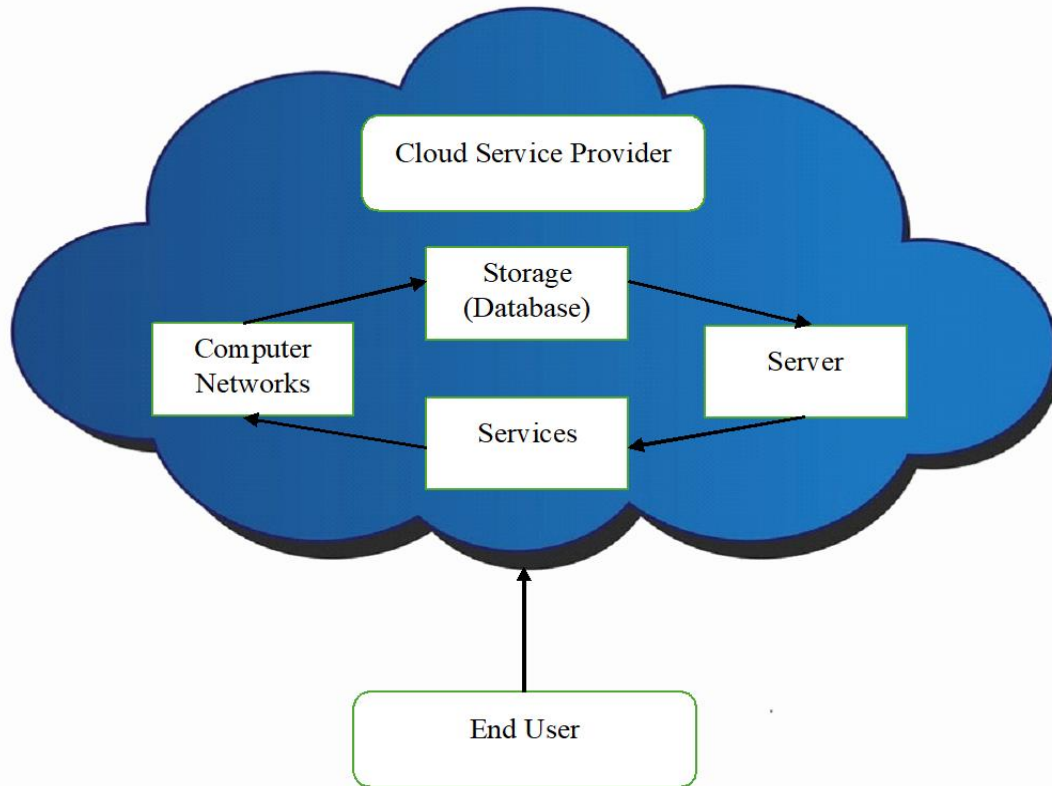
the data stored in the storage devices are unencrypted and processed by cloud administrators hired by cloud service providers, which may lead to trust issues (Uddin et al., 2021). Similarly, data security is one of the most significant challenges that represents a real threat to the future development of cloud computing (Kumar et al., 2020). Aleem and Ryan Sprott (2013) considered data loss and data leakage as the top threats to cloud computing, which is followed by accounts and services hacking.

Data protection and authorized access became major requirements in cloud computing with the increasing number of IT security risks and the rising development of cyber-attacks (Palanisamy & Wu, 2021). Thus, organizations use data security policies to protect their data, but the data security policy does not necessarily guarantee compliance (Cope et al., 2017; Stewart, 2022). Cope et al. (2017) added that access to sensitive or personal data in production environments can be controlled by user role or business function, where policies for production data are not necessarily applied to non-production environments that contain copies of live data, which increases the risk of data loss (Cope et al., 2017). However, IT security vulnerabilities require a high-level solution for the identified security threats in the cloud infrastructure to provide secure, efficient, and transparent services to the cloud end-users (Uddin et al., 2021).

Web and mobile applications are used within cloud computing core technologies, where understanding data breaches in these technologies and their associated risk mitigation actions may help mitigate vulnerabilities in cloud computing (Gashami et al., 2020). Palanisamy and Wu (2021) added that cloud computing has suffered from data breaches and malicious intrusions via mobile network systems despite the benefits of mobile technologies, where cloud computing is always subject to commercial hacking.

Similarly, SaaS development still faces challenges with the adoption of cloud computing, which need to be addressed to identify the factors that could block the functionality of cloud SaaS platforms in organizations, where SaaS development may include the risk of damage, injury, liability, loss, or other negative events caused by internal or external vulnerabilities (Stewart, 2022).

Unauthorized access to sensitive client data in cloud SaaS platforms in organizations may result in data breaches where sensitive data are exposed to cause problems for most organizations that use cloud computing (Adee & Mouratidis, 2022). Also, data leakage describes the unauthorized transfer of personal or sensitive data from a computer, system, or data center outside of the organization (Cope et al., 2017). Wang and Yongchareon (2020) considered cybersecurity assessment as third-party audits of cloud services, where cloud providers can ensure that their cloud services provide proper functionalities under cloud security. An appropriate cybersecurity assessment may also enable cloud service providers to assess IT security risks in cloud systems, allow clients to contribute to risk assessments, as well as include the procedure of IT security awareness from both cloud providers and users, where Figure 1 shows the interaction between cloud providers and users in cloud computing (Kouatli, 2014; Wang & Yongchareon, 2020). Aslam et al. (2022) showed that general data protection regulations and the U.S. breach notification laws state that data breach incidents should be notified without any delay to the supervisory authority, organizations must inform their impacted clients immediately about high-risk data leakage, as well as organizations must promise their clients with data protection under the Federal Trade Commission Act. The studies discussed in this section are summarized in Table 9.

Figure 1*Interaction in Cloud Computing***Table 9***Literature Summary of Organizations' Concerns about IT Security Vulnerabilities in Cloud**SaaS Platforms*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Brumă, 2020	Empirical	Commentary	Digital Libraries	The main issue of security in cloud computing is the existence of many and various technologies connected through the same IT infrastructure

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kumar et al., 2020	Empirical	Commentary	Digital Libraries	Data security is one of the most significant challenges which represent a real threat to the future development of cloud computing
Uddin et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	One of the significant issues in the cloud data center is protecting clients' sensitive data from leaking over the Internet and cyber-attacks.
Aleem & Ryan Sprott, 2013	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	IT security threats lead to the corrupt use of cloud computing in organizational systems.
Gashami et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Understanding data breaches in cloud computing core technologies may help mitigate vulnerabilities in cloud computing.
Adee & Mouratidis, 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Unauthorized access to sensitive client data in cloud SaaS platforms in organizations may result in data breaches in organizations that use cloud computing.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Cope et al., 2017	Empirical	Commentary	Digital Libraries	Data leakage describes the unauthorized transfer of personal or sensitive data from a computer, system, or data center outside of the organization.
Stewart, 2022	Empirical	Commentary	Digital Libraries	The risk of SaaS development may lead to damage, loss, or other negative events caused by IT security vulnerabilities.
Aslam et al., 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Data breach incidents should be notified without any delay to the supervisory based on the general data protection regulations.
Wang & Yongchareon, 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Appropriate cybersecurity assessment may enable cloud service providers to assess IT security risks and include the procedure of IT security awareness from both cloud providers and users.
Kouatli, 2014	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	The whole business will freeze in organizations if cyber-attacks cause any connectivity failure in their systems.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Palanisamy & Wu, 2021	Empirical	Commentary	Cloud SaaS Platforms	Data protection and authorized access became major requirements in cloud computing with the increasing number of IT security risks and cyber-attacks.

Financial and Legal Damages in Organizations Caused by Data Breaches

Organizations have been losing millions of dollars after falling victim to different types of cyber-attacks such as data breaches, Business Email Compromise (BEC), and phishing emails (Murtaza et al., 2022; Teng, 2022). Kuo-Chung et al. (2020) showed the Target data breach as an example of stealing data of \$70 million, as well as an amount of \$39 million paid in 2015 for collective litigation. Dinger and Wade (2019) also showed that Equifax's data breach was considered the most expensive in history with \$439 million after covering \$125 million by insurance, where the remaining \$314 million is only 9.3% of the revenue of \$3.36 billion in 2017. Similarly, Yahoo was a victim of two massive data breaches in 2013 and 2014, which impacted more than 1.5 billion users with around \$350 million in losses (Fabio & Samara, 2021). Anthem was also a victim of data breaches, where it agreed to pay \$115 million after the data breach incident, as well as \$15 million to cover the cost of damages to impacted customers by the data breach (Fabio & Samara, 2021).

IT security vulnerabilities include the cost of repairing vulnerable hardware or software, the loss of intellectual property assets that are essential to the competitive advantage of the business, as well as business losses caused by reputational damage or

regulation with affected third parties (Wang & Yongchareon, 2020). Dinger and Wade (2019) also noted that around 60% of small businesses go bankrupt within six months of a cyber-attack due to business losses, where the cost of the average data breach has risen over the past several years to an average of \$3.9 million. Fabio and Samara (2021) gave examples that the average total organizational cost in the U.S. was \$7.35 million and \$4.94 million in the Middle East. Dinger and Wade (2019) also gave examples that data breach costs were estimated at less than 2% of Sony's 2014 sales, less than 0.1% of Target's 2014 sales, and less than 0.01% of Home Depot's 2014 sales.

When a data breach incident happens, the organization cannot immediately know the exact volume of the incident impact and the size of the data leak, as well as the organization, faces immediate costs such as identifying the source of the data breach, resolving the IT security vulnerability, paying regulatory fines, as well as paying reparations for damages to customers (Dinger & Wade, 2019; Kuo-Chung et al., 2020). Kuo-Chung et al. (2020) showed that only investigating the relationship between the size of the data breach suffered by the organization and its short-term impact cannot be a complete measure of the impact of the data breach incident. Similarly, it could be harder to determine the number of damages related to harm to a reputation and lost revenue that may damage the organization in the marketplace (Dinger & Wade, 2019).

The market reactions to the announcement of data breaches can be considered another way to view the damage caused by data breaches (Dinger & Wade, 2019). Kuo-Chung et al. (2020) gave the reason that the volume of the data breach incident and the follow-up legal damages cannot be sufficiently measured in the short-term period after the data breach incident. After the first announcement of SONY's data breach incident, the volume of data

breaches continued to expand over time due to the evolution of the cyber attacker's type of intrusion, as well as intruders' stealing behavior of hiding in the organizational systems (Dinger & Wade, 2019; Kuo-Chung et al., 2020). Spinello (2021) also showed that attackers may break into an organization's database and steal customers' information to make fraudulent charges or assume the customers' identities.

The inability to determine the various costs may enlarge the level of IT security risks, and large data breaches may lead to losing customers and heavy legal responsibility (Dinger & Wade, 2019; Kuo-Chung et al., 2020). Fabio and Samara (2021) showed that Anthem Inc. was hacked in 2014 in the largest cyber-attack in the healthcare industry, which resulted in the theft of personal information, sensitive medical information, and social security numbers of over 78 million customers. Bennet Simon et al. (2022) considered that an organization's size can be an important factor in examining data breach incidents, where large organizations were more likely to report dangerous data breaches such as ransomware and CEO fraud compared with small, as well as medium-sized organizations that report spyware and other malware in their incidents. The reasons why large organizations experience many data breach incidents can be found in the complex and large organization's IT infrastructure, as well as the involvement of more agents, staff, vendors, and clients in the organization (Bennet Simon et al., 2022; Kuo-Chung et al., 2020). Bennet Simon et al. (2022) added that large organizations report more data breach incidents, but they have better IT security measures to reduce the incidents' harm.

The U.S. Department of Homeland Security showed that manufacturing is the second industry that is a target for cyber-attacks and data breaches, where cybercriminals target small and medium-sized manufacturers that do not have adequate preventative measures

(Fabio & Samara, 2021). Although many organizations such as manufacturing organizations have already used IT security measures, the organizations are still impacted by cyber-attacks and data breach incidents, where management boards in the organizations need to take care of cyber-attacks, as well as data breach incidents that may lead to extreme damages (Bennet Simon et al., 2022). Fabio and Samara (2021) noted that data breaches cause real economic damage to organizations that may take months or years to resolve, as well as around 53% of all cyber-attacks and data breaches result in financial damages that include lost revenue, customers, and opportunities. The federal courts only recognize the damage that may occur in data breach incidents, which depends on the hacker's skill and intent (Spinello, 2021). Max et al. (2021) defined external environment threats as the threats of financial or legal damages due to noncompliance with regulations, standards, or other agreements with third parties, as well as physical threats are threats related to the damage, theft, or loss of organizational physical assets.

Some federal courts have found an increase in the risk of identity theft with high severity and susceptibility (Spinello, 2021). Dzidzah et al. (2020) defined perceived severity as the extent of damage malicious threats to IT that could cause issues for the user, as well as perceived susceptibility as the possibility that malware could lead the user to negative outcomes. Both perceived severity and perceived susceptibility were expected to interact together to increase the perceptions of IT security threats (Dzidzah et al., 2020; Spinello, 2021). The federal courts' resolutions related to harm in data breach cases have led to huge confusion about viewing the harm as the threat has the potential to harm IT systems through the destruction, disclosure, or modification of data (Max et al., 2021; Spinello, 2021). Spinello (2021) showed that the confusion has prevented many victims

from seeking compensation after the data breach incidents, as well as some federal courts, may minimize intangible harms and dismiss cases for lack of perceivable harm (Spinello, 2021). The legal system must properly address data breach harms to ensure predictability, clarity, and precision in judicial decision-making (Max et al., 2021).

Cloud SaaS platforms can be subject to an attack called malware injection attack, which is a type of Structured Query Language (SQL) injection attack in cloud computing that started around 2011, where an attacker tries to damage an application or service in the cloud by injecting his credentials if it is a legitimate one (Kouatli, 2014). Max et al. (2021) added that the attacker can upload a virus program into the cloud structure if his attack succeeds. Max et al. (2021) defined ransomware as a type of malware that infects the computer systems of an organization's users and manipulates the systems in a way that the victims will not be able to use their data stored on the systems, as well as denial of service is the prevention of authorized access to resources or the delaying of time-critical operations. Spam is defined as the abuse of electronic messaging systems to randomly send undesirable bulk messages which is considered a cybersecurity threat, as well as web application threats are defined as threats to the security of web applications and services, which abuse misconfigurations or vulnerabilities in the application implementation (Kouatli, 2014; Max et al., 2021).

Bennet Simon et al. (2022) defined web-based threats as threats with an attractive method by which threat actors can trick victims using web systems and services. Average direct and opportunity costs related to severe data breach incidents can be manageable, as well as only impact a small proportion of organizations (Kouatli, 2014; Max et al., 2021). Successful past attempts to reduce cybercrimes might make the average direct and

opportunity costs low because organizations had previously prepared themselves for the cybercrimes (Bennet Simon et al., 2022; Max et al., 2021). The studies discussed in this section are summarized in Table 10.

Table 10

Literature Summary of Financial and Legal Damages in Organizations Caused by Data

Breaches

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Murtaza et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Some organizations lost millions of dollars after falling victim to different types of cyber-attacks.
Wang & Yongcharon, 2020	Empirical	Commentary	Digital Libraries	IT security vulnerabilities result in business losses caused by reputational damage or regulation with affected third parties.
Kuo-Chung et al., 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	When a data breach incident happens, the organization cannot immediately know the exact volume of the incident impact and the size of the data leak
Dinger & Wade, 2019	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	When data breaches happen, organizations face immediate costs such as identifying the source of the data breach and resolving the IT security vulnerability

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Fabio & Samara, 2021	Empirical	Commentary	Digital Libraries	The U.S. Department of Homeland Security showed that manufacturing is the second industry as a target for cyber-attacks and data breaches
Spinello, 2021	Empirical	Commentary	Digital Libraries	Some federal courts have found an increase in the risk of identity theft and hackers breaking into an organization's database and stealing customers' information.
Dzidzah et al., 2020	Empirical	Commentary	Digital Libraries	Both perceived severity and perceived susceptibility were expected to interact together to increase the perceptions of IT security threats.
Kouatli, 2014	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	Malware injection attacks in cloud computing enable attackers to damage an application or service in the cloud by injecting their credentials and uploading virus programs into the cloud structure.
Max et al., 2021	Empirical	Commentary	Digital Libraries	Denial of service is the prevention of authorized access to resources or the delaying of time-critical operations

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Bennet Simon et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	An organization's size is considered an important factor in examining data breach incidents

Proper Cybersecurity Implementation in Cloud SaaS Platforms by Organizations

Some organizations such as real estate organizations do not consider information security as a priority as it is not a part of their core business (Mani et al., 2014). However, Shahzadi et al. (2020) showed that if the organization has IT systems such as cloud SaaS platforms, they will need to deploy a strong cybersecurity posture that sufficiently manages the security in cloud SaaS platforms to reduce IT security obstacles. Mani et al. (2014) also noted that business organizations must be aware of IT best practices and information security risk management to reduce the risks of cybercrimes, where information security risk management is used to assess risk, mitigate risk, as well as maintain the level of risk to an acceptable level.

Organizations take steps to reduce the risk of data breaches based on the organization's size and the potential IT security risks because organizations need to defeat IT security dangers to protect their reputation with clients (Algarni et al., 2021; Shahzadi et al., 2020). The system security risk can be reduced if the organization has a consistent strategy for guiding employees to take appropriate procedures, such as backup, documentation, data storage, and file access practices (Palanisamy & Wu, 2021). However, Gashami et al. (2020) showed that organizations can focus on what type of information that needs more security to reduce the impact of data breaches in cloud SaaS platforms. The indirect data breach costs include recurring costs of the cybersecurity measures and cybersecurity

upgrades, where cybersecurity upgrades can mitigate internal security vulnerabilities and minimize the data breach probability to protect organizations from data loss (Algarni et al., 2021).

Organizations should have a goal to reduce the impact of the IT security threat by informing their employees and users how to protect their data, which will help support the reputation of the organizations (Gashami et al., 2020). Users' position towards organizations-related issues is strongly correlated with the perceived security of the web and mobile systems (Palanisamy & Wu, 2021). Thus, cybersecurity has an important role in designing and developing web and mobile systems by clear allocation, which is based on who has the right to access or modify the system data (Gashami et al., 2020; Palanisamy & Wu, 2021). Organizations must find out whether they invest in proactive or reactive technology procedures to reduce cyber-attacks in their systems (Kumar et al., 2021; Shahzadi et al., 2020). Kumar et al. (2021) showed that the proactive information security procedures include techniques such as digital signatures, cryptographic keys, digital certificates, and anti-virus scanners, as well as the reactive information security procedures include techniques such as access controls, firewalls, passwords, remote access, and intrusion detection systems. The studies discussed in this section are summarized in Table 11.

Table 11*Literature Summary of Proper Cybersecurity Implementation in Cloud SaaS Platforms*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Mani et al., 2014	Empirical	Commentary	Digital Libraries	Some organizations that are related to real estate do not consider information security a priority as it is not a part of these organizations' core business.
Algarni et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations take steps to reduce the risk of data breaches based on the organization's size and the potential IT security risks to protect their reputation with clients.
Shahzadi et al., 2020	Empirical	Commentary	Digital Libraries	Cloud computing can enable organizations to break the physical bonds between the IT foundation and the organization's clients.
Palanisamy & Wu, 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	The system security risk can be reduced if the organization has a consistent strategy for guiding employees to take appropriate procedures to save and protect their data.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gashami et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations may reduce the impact of the IT security threat by informing their employees and users how to protect their data to support the reputation of the organizations.
Kumar et al., 2021	Empirical	Commentary	Cloud SaaS Platforms	Organizations that invest in proactive or reactive technology procedures may reduce cyber-attacks in their systems.

Using Cybersecurity Posture by IT Security Leadership

Although organizations have spent billions of dollars on IT systems to detect and reduce cybersecurity threats, organizational systems are still subject to massive IT security threats and data breaches due to the potential for cyber-threats such as malware that may gain escalated privileges (Harris & Patten, 2014; Triplett, 2022). Cybersecurity leadership faces huge challenges in the work environment of organizations, where cybersecurity vulnerabilities have evolved into serious IT security threats in the organizations (Triplett, 2022). Harris and Patten (2014) noted that several IT security professionals have suggested a ban on all hacked organizational systems and networks.

Individuals and firms that are specialists in IT security may have an important role by forwarding information coming from the main source and forming communities, as well as they may serve as key partners in spreading cybersecurity actions and reducing the potential impact of data breaches (Gashami et al., 2020). Although IT security is managed by technical personnel who are more knowledgeable in technology, awareness is

considered a complex issue that impacts the behavior of all employees in the organization (Smit et al., 2021). Kumar et al. (2021) added another issue faced in the organization related to human factors that may impact cybersecurity, which include the role of senior management and the technical work experience of the IT security manager. Human factors include data elements, human behaviors, human performance to reduce errors, as well as human interactions with computer workstations and mobile devices (Triplett, 2022). However, Kumar et al. (2021) showed that technology and organizational indicators include strategies adopted by senior management of the organization, as well as legal procedures adopted for enhanced IT security.

Information security courses heavily focus on the technology used by an organization's employees, where the impact of data breach incidents may lead to a failure of the employee's duties (Smit et al., 2021; Wirth, 2017). Wirth (2017) also showed that technical details about security architecture, security decisions, as well as establishing a strong cybersecurity posture belong to the board's duties. Smit et al. (2021) described the CISO position in the organization as a senior-level executive who has the responsibility to establish and maintain the organization's IT security program, which may include a set of technology measures such as awareness. IT security leadership including CIO and CISO will be responsible for communicating cybersecurity issues to the board (Wirth, 2017). The studies discussed in this section are summarized in Table 12.

Table 12*Literature Summary of Using Cybersecurity Posture by IT Security Leadership*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Harris & Patten, 2014	Quantitative Survey	24 SMEs	Surveys for SMEs	Several IT security professionals suggested a ban on all hacked organizational systems that suffered from massive data breaches.
Gashami et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Individuals and firms that are specialists in IT security may spread cybersecurity actions to reduce the potential impact of data breaches.
Wirth, 2017	Quantitative Survey	24 SMEs	Surveys for SMEs	Information security courses are used where the impacts of data breach incidents can reflect a failure of board members at an organization to support their duties.
Smit et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	CISO position in the organization is described as a senior-level executive who has the responsibility to establish and maintain the organization's IT security program.
Triplett, 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Cybersecurity leadership faces enormous challenges in the work environment of organizations related

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kumar et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	to cybersecurity vulnerabilities and threats. Organizational and technological factors include technical procedures to enhance cybersecurity posture in organizations.

Protection Software and Network Security in IT Security Techniques

Sensitive data stored in cloud SaaS platforms at an organization will be more than mandatory to be protected from cyber-attacks and IT security threats, where IT security threats that lead to data breaches can happen due to unethical behavior, which could be a result of firing unethical individuals from their positions or a small business facing of strong competition (Georgiopolou et al., 2020; Kouatli, 2014). Xing and Zhang (2022) added that as the organizational systems' network became more complex along with using big data, the awareness methods of the traditional network security may have difficulty in addressing the network complexity issue due to the generated data speed, volume, and structure, where data can be sensitive and stored in cloud SaaS platforms. Organizations need to find a network security awareness method for cyber-attacks that effectively supports IT security administrators' decision-making due to the large-scale and multistage features of network attack threats (Georgiopolou et al., 2020; Xing & Zhang, 2022).

New techniques and methodologies must be developed to meet IT security and privacy requirements, as well as they can be used in organizational systems, such as smartphones, cloud computing, and social networks (Shammar & Zahary, 2020). Ramakic and Bundalo

(2014) added organizations use several approaches and methods for IT systems' protection, which may include cryptography, programming, backup, antivirus solutions, antispyware, firewalls, as well as digital signature techniques. Georgiopoulou et al. (2020) showed that the organization must have encryption techniques and all the procedures related to data protection levels to reduce data breach incidents. Additionally, Kouatli (2014) showed that counterattacks on malicious techniques by using anti-virus techniques and proper management can minimize and correct any possible problem in unethical IT behavior.

The financial data at an organization are stored as nodes in intelligent financial systems using blockchain technology, which improves the requirements for node data security (Lu et al., 2022). Georgiopoulou et al. (2020) added that when the systems are established, each business node must create an intranet for data transmission and ensure that the data on the intranet are separated from the data on the public network. Each node may utilize encryption hardware to improve data management and control, as well as monitor network threats and prevent data theft using high-security protection software (Lu et al., 2022). The studies discussed in this section are summarized in Table 13.

Table 13

Literature Summary of Protection Software and Network Security in IT Security

Techniques

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Georgiopoulou et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations must have encryption techniques and all procedures related to data protection levels to reduce data breach incidents.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kouatli, 2014	Quantitative Survey	24 SMEs	Surveys for SMEs	Minimizing unethical behavior related to IT security threats can be done by counterattacking the malicious techniques using anti-virus techniques and proper management.
Xing & Zhang, 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Awareness methods of traditional network security may have difficulty in addressing the network complexity issue due to the generated data speed, volume, and structure
Ramakic & Bundalo, 2014	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations use several approaches and methods for IT such as cryptography, programming, and antivirus solutions
Lu et al., 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	The financial data at an organization are stored as nodes in intelligent financial systems using blockchain technology
Shammar & Zahary, 2020	Empirical	Commentary	Cloud SaaS Platforms	Different techniques can be used in IT and organization systems that may impact cybersecurity.

Annual Budget for Cybersecurity

As employees are often the weakest link in the cybersecurity posture at an organization, the organization must develop an effective program for cybersecurity assessment that can motivate the organization's employees to stay alert and avoid data

breaches (Zhang et al., 2021). However, Creado and Ramteke (2020) showed that employees' surveillance can be covered by the IT department, as well as using cybersecurity to prevent, detect, and mitigate IT security risks. The number of employees and the size of the annual budget for cybersecurity in organizations significantly impact the cybersecurity posture (Ermicioi & Liu, 2021).

Organizations that suffer from data breaches may use outdated devices that have low cybersecurity measures or outdated operating systems such as old versions of Windows that Microsoft stopped supporting in a particular year (Brody et al., 2018). An appropriate annual budget for cybersecurity assessment programs needs to include funding for training resources, consulting, testing, advertising, software, hardware, as well as technical services costs (Zhang et al., 2021). Therefore, many organizations spend millions of dollars on their annual budget for IT and cybersecurity, where the annual budget can be different based on the industry sector (Brody et al., 2018).

The lack of awareness and integration inside an organization may create an IT security vulnerability that several cyber attackers can exploit with the least possible effort (Creado & Ramteke, 2020). Ermicioi and Liu (2021) added that limited resources, such as the annual budget for cybersecurity, cause big challenges that make organizations more vulnerable to cyber-attacks and data breaches. Ogu et al. (2019) also showed that the number of reported cybercrimes rose to more than one million in the past 10 years, which resulted in financial losses that exceeded the annual budget in organizations in monetary value. Creado and Ramteke (2020) suggested that the issue of cyberattacks at an organization must be reported to its boardroom and decision-makers, who must take into consideration that cybersecurity is a part of the organization's annual budget.

The Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3.gov) in 2014 has received three million complaints about Internet crimes since its establishment, which led to total financial losses that exceeded two billion dollars (Ogu et al., 2019). Moreover, Shihan and Radif (2022) showed that the U.S. Cybersecurity and Critical Infrastructure Agency (CISA) recommended in 2018 that every organization should assign at least 8% of its annual budget to establish, maintain, and enhance its cybersecurity posture. The annual master plans for the cybersecurity budget that are implemented in the branches of an organization will improve the organization's overall cybersecurity posture (Ogu et al., 2019; Shihan & Radif 2022). The studies discussed in this section are summarized in Table 14.

Table 14

Literature Summary of Annual Budget for Cybersecurity

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Zhang et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations develop effective programs for cybersecurity assessment to motivate their employees to stay alert and avoid data breaches.
Brody et al., 2018	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Annual budgets for IT and cybersecurity in organizations can be different based on the industry sector of each organization.
Ermicioi & Liu, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The number of employees and the size of the annual budget for cybersecurity in

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ogu et al., 2019	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	organizations significantly impact the cybersecurity posture. Increasing the number of reported cybercrimes resulted in financial losses that exceeded the annual budget of organizations.
Creado & Ramteke, 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	The lack of awareness and integration inside an organization may create an IT security vulnerability exploited by several cyber attackers.
Shihan & Radif, 2022	Empirical	Commentary	Cloud SaaS Platforms	U.S. Cybersecurity and Critical Infrastructure Agency recommended that organizations should assign at least 8% of their annual budget to establish, maintain, and enhance their cybersecurity posture

Total Annual Expenses on IT

Financial reports in organizations can be used as accounting information for the annual expenses in organizations that include the total annual expenses on IT, where total annual expenses on IT may include hardware, software, networks, as well as R&D (Pathak et al., 2020; Peruško & Šestan, 2020). Similarly, Marcus (2017) showed that the total annual expenses on IT represent an essential part of the annual expenses in the organization. Each

organization has different total expenses on IT that vary every year, especially when the organization is subject to cyber-attacks and data breach incidents (Marcus, 2017; Pathak et al., 2020). Also, IT management at an organization generates an initial IT portfolio, facilitates an overview of the IT area, helps keep the organization's members aware of the different IT systems, as well as enhances an improvement in both organizational and IT strategies, where the IT management duties rely on the investments budget in IT and the annual expenses on IT (Pietro et al., 2014).

Employees who work in the accounting and finance departments should have theoretical knowledge, as well as experience in accounting and finance concepts, where the experience may include the accrual basis of accounting, as well as historical cost concept to help the employees in creating annual financial reports for their organization (Thottoli & Ahmed, 2022). Xue et al. (2015) added that the values of quality of service for each financial solution can be calculated using aggression formulas for the quality of service, which include the total process time, the total expense and price, as well as the production capacity. An accountant should have great knowledge of using cloud SaaS platforms related to accounting, where they may get phishing emails from hackers who use manipulation of accountants and other employees to get information or access to data or money (Egan et al., 2019; Thottoli & Ahmed, 2022).

Phishing emails are one of the major issues of cyber threats in organizations, and they can be fraudulent emails from the Chief Financial Officer (CFO) or a vendor who asks for a payment to be wired to a certain bank account, which is his bank account (Egan et al., 2019; Saxena et al., 2020). Egan et al. (2019) showed that the Californian Insurance Commission has stated that data breach incidents along with phishing emails can be caused

by hackers from other countries. Saxena et al. (2020) added that email sharing practice can be used as a part of the threats related to phishing, where cyber-attacks along with phishing emails have increased to 56%, which led organizations to decide to create defensive actions to reduce the cyber threats. The studies discussed in this section are summarized in Table 15.

Table 15

Literature Summary of Total Annual Expenses on IT

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Pathak et al., 2020	Empirical	Commentary	Digital Libraries	The IT expenses and costs can be obtained from the organization's annual financial report.
Thottoli & Ahmed, 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Employees who work in the accounting and finance departments should have theoretical knowledge and experience in accounting and finance concepts to help in creating annual financial reports
Xue et al., 2015	Empirical	Commentary	Digital Libraries	The values of quality of service for each service composition solution can be calculated using aggression formulas for the

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Peruško & Šestan, 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	quality of service. Financial reports in organizations can be used as accounting information for the annual expenses in organizations that include the total annual expenses on IT.
Marcus, 2017	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Each organization has different total expenses on IT that vary every year, especially when facing cyber-attacks and data breach incidents.
Pietro et al., 2014	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	IT management is used based on the users' and fields' needs, as well as the annual expenses on IT and investments budget.
Egan et al., 2019	Quantitative Survey	24 SMEs	Surveys for SMEs	Phishing emails from hackers use manipulation of accountants and other employees to get information or access to data or money.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Saxena et al., 2020	Empirical	Commentary	Digital Libraries	Phishing emails are one of the major issues of cyber threats in organizations.

Organizational Assets

An increasing number of organizations have adopted and used cloud computing with its advanced evolution, where cloud computing has advanced and enabled new plans of action, as well as it has become one of the most current patterns in the data advancements world (Moudud-UI-Huq et al., 2020). As organizations became more complex, employees found more ways to engage in counterproductive work experiences (Kouatli, 2014). Thus, accounting can provide considerable assets to any estimated size of a project at an organization (Moudud-UI-Huq et al., 2020). Nguyen and Park (2022) showed that as organizational assets include the organization's property, confidential documents, as well as organizational systems architecture, the security operations center supervises and defends the organizational assets.

Management in organizations has proposed new approaches toward asset evaluation as a part of knowledge management of organizational assets (Kouatli, 2014). Also, asset management in organizations identifies organizational assets, defines appropriate protection responsibilities, as well as ensures that assets are properly protected, and mitigates unauthorized disclosure, modification, deletion, or destruction of information stored in organizational systems (Wang & Yongchareon, 2020). Similarly, security risk management includes identifying, assessing, and treating risks related to organizational assets (Orlando, 2021).

Data breach events are considered negative and value declining events to the organizational financial performance, where the events negatively impact the organization's profitability, which leads to the exhaustion of the organizational assets (Avery, 2021). Nguyen and Park (2022) showed that many IT departments in organizations address IT security issues by establishing a security operations center internally or through a third-party security service provider, which monitors and analyzes the organization's IT security, as well as improves the IT security and takes actions against cybersecurity incidents. However, some organizations may not perform better business due to a data breach event, as well as they can be considered financially sustainable in the first quarter of the year after a data breach disclosure (Avery, 2021). The studies discussed in this section are summarized in Table 16.

Table 16

Literature Summary of Organizational Assets

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Moudud-Ul-Huq et al., 2020	Empirical	Commentary	Cloud SaaS Platforms	An increasing number of organizations have used cloud computing with its advanced evolution to enable new plans of action and to become a current pattern in the data advancements world.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wang & Yongchareon, 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Asset management in organizations identifies organizational assets, defines appropriate protection responsibilities, and ensures that assets are properly protected to prevent unauthorized disclosure in organizational systems.
Kouatli, 2014	Empirical	Commentary	Digital Libraries	Management in organizations has proposed new approaches towards asset evaluation as a part of knowledge management of organizational assets.
Orlando, 2021	Empirical	Commentary	Digital Libraries	Adoption of the best cybersecurity posture and the setup of different procedures may reduce cyber-attacks and data breach incidents.
Avery, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Data breach events are considered as negative and value declining events to the organizational financial performance as the events negatively impact the organization's profitability.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Nguyen & Park, 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Many IT departments in organizations address security issues by establishing a security operations center to monitor and improve cybersecurity.

Annual Organizational Liabilities

Assets and liabilities in organizations can interact as organizational financial performance indicators to publish and share information related to the annual financial report of the organization (Ben-Abdallah et al., 2020). Pevnick et al. (2012) added that organizational concern about liabilities was one of the factors aligned with an organization's commitment to its annual financial performance. The value of current liabilities is less than the value of net short-term assets which are calculated as (current assets – book value of Inventories – current liabilities + debt in current liabilities) (Moorthy & Polley, 2010). However, organizations may apply an integrated approach of asset liability management that forms the organizational assets and liabilities, where organizations have interdependencies between assets and liabilities that impact data breaches as organizational financial performance indicators (Kramer & van Welie, 2001).

The increase in the average total cost of a data breach incident in recent years was around one million dollars, which is a cost difference where remote work was a key factor in causing the data breaches (Pevnick et al., 2012; Sun & Lu, 2022). Sun and Lu (2022) also showed that the increase in data breach frequency and average cost raises the

importance of cyber insurance for businesses in organizations to protect their liabilities from data breaches. Therefore, if data breaches affect liabilities in organizations, confidential customer information can be disclosed in the cloud systems (Rigg, 2018).

Data breaches impact customer restitution and outcomes that may impact the organization's cost, as well as the organization's liabilities that can have high efficiency in using IT security services (Johnston, 2022). Khey and Sainato (2013) showed that an organization may have mandatory disclosure policies to disclose information about the risk of its data breach incident to enable consumers to take action to mitigate the impact of data breaches, which can reduce any loss or damage that may impact the organization's performance and liabilities. However, cybersecurity provides the required coverage after a data breach occurrence, where cybersecurity is an essential part of the response plan for a data breach incident, which helps minimize the organization's damage such as its performance and liabilities (Algarni et al., 2021). The studies discussed in this section are summarized in Table 17.

Table 17

Literature Summary of Annual Organizational Liabilities

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Kramer & van Welie, 2001	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations have interdependencies between assets and liabilities that impact data breaches as organizational financial performance indicators.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ben-Abdallah et al., 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Assets and liabilities at an organization can interact as organizational financial performance indicators to share information related to the annual financial report
Moorthy & Polley, 2010	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Current liabilities valued at the book are less than the value of net short-term assets which are calculated as (current assets – book value of Inventories – current liabilities + debt in current liabilities).
Pevnick et al., 2012	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizational concern about the calculated liabilities was one of the factors that are aligned with an organization's commitment to its annual financial performance.
Sun & Lu, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The increase in data breach frequency and average cost raises the importance of cyber insurance for organizations' business to protect their liabilities from data breaches.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Rigg, 2018	Quantitative Survey	24 SMEs	Surveys for SMEs	If data breaches affect liabilities in organizations, confidential customer information can be disclosed in the cloud SaaS systems.
Johnston, 2022	Empirical	Commentary	Digital Libraries	Data breaches impact customer restitution and customer outcomes that may impact the organization's cost and liabilities.
Khey & Sainato, 2013	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	An organization may have mandatory disclosure policies to disclose information about the risk of its data breach incident to enable consumers to take action to mitigate the impact of data breaches.
Algarni et al., 2021	Empirical	Commentary	Digital Libraries	Cybersecurity provides the required coverage after a data breach occurrence to minimize the organization's damage such as its performance and liabilities.

Annual Owners' Equity Accounts

The statement of an organization's financial report is a statement that explains the assets, liabilities, and owner's equity account in the organization in each period to understand the financial situation in the organization, the quality of accounting information, as well as make a proper evaluation of the financial flexibility of the organization (Qin et al., 2022). Owners' equity account is based on a simple equation (owners' equity account = assets - liabilities), which indicates that the accounts of assets and liabilities form the category of owners' equity (Mattessich & Küpper, 2003). Annual financial reports for some organizations show that projects continue to highly rely on debt with a high percentage of the total financing sources for infrastructure and a low percentage funded by the owners' equity, as well as organizations rely on the intensive use of illiquid forms of capital that includes all organizational systems and devices (Anago, 2022; Hubbs & Kuethe, 2017).

Hubbs and Kuethe (2017) noted that managers may rely on debt capital along with owners' equity accounts to finance their capital base for conducting marketing and production plans, as well as providing a valuable source of short-term liquidity to respond to IT security risks and data breaches that threaten organizations. However, the organization's market evaluates the common probability that a certain auditor will discover a data breach incident in the organizational system and report the incident, where the audit quality is considered both the auditor's efficiency in discovering the incident, as well as the auditor's objectivity in reporting the incident. Ozkaya (2018) showed that there are significant differences between financial reports when using a new cybersecurity posture,

where the financial reports analyze the data breaches' impact on the owners' equity accounts. The studies discussed in this section are summarized in Table 18.

Table 18

Literature Summary of Annual Owners' Equity Accounts

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Anago, 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Annual financial reports for some organizations may show that projects continue to rely on debt with a high percentage of the total financing sources for infrastructure and a low percentage funded by the owners' equity.
Qin et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The purpose of a financial report statement at an organization is to understand the financial situation in the organization and make a proper evaluation of the financial flexibility.
Hubbs & Kuethe, 2017	Quantitative Survey	24 SMEs	Surveys for SMEs	Managers may rely on debt capital along with owners' equity accounts to finance their capital base for providing a valuable source of short-term liquidity to respond to data breaches.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Mattessich & Küpper, 2003	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The basic equation of owners' equity account indicates that the accounts of assets and liabilities form the category of owners' equity.
Raslan et al., 2016	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The organization's market evaluates the common probability that a certain auditor will discover a data breach incident in the organizational system and report the incident
Ozkaya, 2018	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	There are significant differences between financial reports when using a new cybersecurity posture as the financial reports analyze the data breaches' impact on the owners' equity accounts

Annual Organizational Revenue

The demand for cloud SaaS platforms is growing with lower obstacles to enter IT markets and rapidly growing competition between the markets, as well as IT markets are experiencing a fast shift due to cloud computing maturity and the need for revenue generation (Shammar & Zahary, 2020; Wang & Yongchareon, 2020). Shammar and Zahary (2020) also added that vendors in organizations focus more on marketing and

selling cloud SaaS platforms to achieve high revenues, where the cloud SaaS industry has been relatively stable over the past years with the existence of IT security threats and data breaches. Wang and Yongchareon (2020) showed that cloud SaaS revenues usually rely on only the services and resources that clients use, which can potentially cover the legacy revenues that are often based on licensing fees, implementation costs, as well as maintenance contracts.

Organizations reach and serve their existing customers, where the organizations can communicate with their customers to deliver valuable IT services with reduced or eliminated middle or third parties (Upadhyay et al., 2021). Simon (2021) gave an example that many organizations may obtain significant financial benefits from API adoption, where the organizational revenue can be generated from APIs and API-related implementations, which leads to increases in net income, sales, and market capitalization. However, the relationship that organizations establish with their customers can be enhanced by acquiring customers, retaining customers, increasing sales, as well as providing professional IT services by technology firms to generate revenue from network transaction fees, business customer support, or cloud SaaS platform fees (Upadhyay et al., 2021).

Organizations that offer data security and privacy must continue to participate in providing more knowledge about cybersecurity (Yadav et al., 2022). If organizations are impacted by data breach incidents and fail to be trustworthy with their customers, they will lose their customers, which will impact the organizational revenue (Frøystad et al., 2018). Yadav et al. (2022) showed that cybersecurity threats may create a dangerous situation that impacts user visibility, which will have a long-term impact on organizational revenue due

to loss of viewership and subscription. Thus, organizations need to be careful when explaining data breach incidents to ensure it is noted in an understandable way to their customers (Frøystad et al., 2018). The studies discussed in this section are summarized in Table 19.

Table 19

Literature Summary of Annual Organizational Revenue

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Wang & Yongchareon, 2020	Empirical	Commentary	Cloud SaaS Platforms	Demand for cloud SaaS platforms is growing obviously with lower obstacles to entering IT markets and rapidly growing competition between the markets.
Shammar & Zahary, 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The cloud SaaS industry has been relatively stable over the past years with the existence of data breaches.
Upadhyay et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Enhancing the relationship between organizations and their helps generate revenue from transaction fees, customer support, and cloud SaaS platform fees.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Simon, 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Many organizations may obtain significant financial benefits from API adoption as organizational revenue can be generated from APIs.
Frøystad et al., 2018	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations are subject to losing their customers when failing to be trustworthy, which will impact the revenue of these organizations.
Yadav et al., 2022	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Cybersecurity threats may create a dangerous situation that impacts user visibility, which will have a long-term impact on organizational revenue.

Annual Operating Activities

Accounting processing relies on recording economic data necessary for the summary statements, which include the balance sheet and the income statement that is linked to the operating activities of organizations (Feghali et al., 2022). Ganda (2019) added that each organization consists of different stakeholders with imbalanced power that impacts the operating activities of the business in the organization. Deflorin et al. (2021) showed that each production process at an organization has an assigned owner responsible for the

provision of the needed data, the continuous improvement of workflows and products, as well as coordinating the operating activities at each production site in the organization's network. Also, organizational financial indicators show the positive impact of operating activities on organizational financial performance when providing a strong cybersecurity posture for organizations (Muda et al., 2018).

Some organizations use critical success factors to identify a few parts of activities that must go right to achieve the expected performance for the organizations, where the critical success factors include vital issues to an organization's current operating activities and its future success (Gromis di Trana et al., 2022; Patel & Patel, 2021). Patel and Patel (2021) also added that critical success factors require careful observation and can be addressed with vital importance as an ongoing activity by the management to achieve the expected goals. Similarly, management works on monitoring daily activities by improving the awareness of the organization to identify the priorities for its clients and their needs, which can reduce the time of market reaction, as well as substitute generally expensive market investigations (Gromis di Trana et al., 2022). Also, the management must provide support for the technical knowledge that is gained through investments in innovation, which can allow a high degree of flexibility with diversification in the operating activities and the detected opportunities (Ganda, 2019; Gromis di Trana et al., 2022). The studies discussed in this section are summarized in Table 20.

Table 20*Literature Summary of Annual Operating Activities*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Patel & Patel, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Using critical success factors can achieve the expected performance and goals.
Ganda, 2019	Empirical	Commentary	Digital Libraries	Each organization consists of different stakeholders with imbalanced power that impacts the operating activities of the business in the organization.
Feghali et al., 2022	Empirical	Commentary	Digital Libraries	Accounting processing relies on recording economic data necessary for the summary statements, which include the balance sheet and the income statement linked to the operating activities of organizations.
Muda et al., 2018	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizational financial indicators show the positive impact of operating activities on organizational financial performance when providing a strong cybersecurity posture.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Gromis di Trana et al., 2022	Empirical	Commentary	Digital Libraries	Proactiveness should focus on the management experience with the support of the technical knowledge that can allow a high degree of flexibility with diversification in the operating activities.
Deflorin et al., 2021	Empirical	Commentary	Digital Libraries	Each production process has an assigned owner responsible for the provision of the needed data and coordinating the operating activities at each production site.

Annual Investing Activities

The finance department in organizations plays an active role in evaluating the organizational financial performance, especially related to the organization's investing effort, through discussion of investment reviews and the annual financial performance (Saj, 2013). Martins et al. (2021) added that organizations in societies and countries with different cultural values can produce different economic outcomes, such as different development levels of investing activities, where cultural values are unique in each country, as well as relatively stable over time. The most relevant cultural values for developed investment are entrepreneurialism to enable individuals to start a business, social capital, trust, and uncertainty avoidance (Martins et al., 2021). Investors can

determine the present value of all future cash flows of investing activities, as well as should keep in mind the life cycle stage while investing in organizations (Bin Khidmat et al., 2019). Lee and Park (2018) added that cash inflows from investing activities are the primary source of funding for capital expenditure, followed by cash flows from operations, as well as cash inflows from financing activities that include debt issuance.

The capital market is a market for a diversity of long-term financial instruments that can be traded such as stocks, bonds, and mutual funds, as well as it is a funding facility for organizations and a means of investing activities (Rahmawati et al., 2021). However, mutual funds may participate only in investing activities that may not keep short positions in securities or trade derivatives, as well as they may invest only in securities that may not invest in real estate or other assets (Krug, 2017). Bin Khidmat et al. (2019) showed that the competitive markets have more information content than the concentrated markets, where the organization's managers issue new shares and stocks that have efficient R&D investment, as well as the security market regulator formulates effective product market regulations for the policy implication perspective (Bin Khidmat et al., 2019). The studies discussed in this section are summarized in Table 21.

Table 21

Literature Summary of Annual Investing Activities

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Saj, 2013	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The finance committee evaluates the organizational financial performance through discussion of investment reviews and the annual

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Martins et al., 2021	Empirical	Commentary	Digital Libraries	financial performance. The most relevant cultural value for investment to be developed in a country is entrepreneurialism, which enables individuals to start a business and trust.
Bin Khidmat et al., 2019	Empirical	Commentary	Digital Libraries	Security market regulators should formulate effective product market regulations from the policy implication perspective.
Rahmawati et al., 2021	Empirical	Commentary	Digital Libraries	A capital market is a market for a diversity of long-term financial instruments and a funding facility for investing activities in organizations.
Lee & Park, 2018	Empirical	Commentary	Digital Libraries	Cash inflows from investing activities at an organization are the primary source of funding for capital expenditure.
Krug, 2017	Empirical	Commentary	Digital Libraries	Mutual funds may participate only in investing activities, and they may also invest only in securities.

Annual Financing Activities

Financing is used to finance different projects to enhance practices that will have a long-term positive impact on the projects (Julia et al., 2016). Harun and Raquela (2021)

showed that banks may face mismatch risk due to certain features of funding sources and financing activities, where deposits are the largest funding source in banks, which becomes essential due to its impact on bank lending as well as bank liquidity level. Also, financial institutions need to properly verify their customers by verifying the customer's identity before establishing a business relationship or transaction (Laurinaitis et al., 2021). If the institutions cannot verify their customers, it is recommended not to open business accounts for the customers or establish a business relationship that may negatively impact the institution's financing activities (Harun & Raquela, 2021; Laurinaitis et al., 2021). Financial institutions such as banks create information security policies and guidelines to protect their environments from data breaches by financing activities (Harun & Raquela, 2021; Julia et al., 2016). Julia et al. (2016) also added that studying IT security risks and data breaches in credit risk management, as well as creating climate risk funds may facilitate positive bank environment practices through bank financing activities.

Organizations that have been or will be close to registration under the former threshold of record-holders will no longer need to consider restricting financing activities, which might cause the organizations to exceed that threshold (Parrino & Romeo, 2012; Xie et al., 2020). Parrino and Romeo (2012) added that the new threshold may result in a significant increase in the trading of an organization's equity securities in the market, because many organizations can obtain a larger shareholder base than what was permitted under the former threshold. Application and initiation of various businesses, subsequent business acceptance and handling, management of various financing activities, as well as risk control quota management, and basic business support management functions can achieve various business management functions of supply chain financial business (Xie et al.,

2020). Similarly, sellers in organizations set up large amounts of accounts receivable by providing credit sales and instant payment services, whereas sellers' accounts receivable are relatively various and have different financing activities (Cheng-yong et al., 2022). The studies discussed in this section are summarized in Table 22.

Table 22

Literature Summary of Annual Financing Activities

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Julia et al., 2016	Quantitative Survey	24 SMEs	Surveys for SMEs	Studying IT security risks and creating climate risk funds facilitates positive organizational environment practices through financing activities.
Harun & Raquela, 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	Banks may face mismatch risk due to certain features of funding sources and financing activities in the organization.
Laurinaitis et al., 2021	Quantitative Survey	24 SMEs	Surveys for SMEs	It is recommended not to establish a business relationship with the customers that may negatively impact the institution's financing activities without verifying its customers.
Parrino & Romeo, 2012	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The new threshold may result in a significant increase in the trading of the organization's equity securities in the market due to

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Xie et al., 2020	Empirical	Commentary	Digital Libraries	obtaining a larger shareholder base. Business initiation, business handling, management of various financing activities, and basic business support management functions can achieve various business management functions of financial business.
Cheng-yong et al., 2022	Empirical	Commentary	Digital Libraries	Sellers set up large amounts of accounts receivable that have different financing activities by providing credit sales and instant payment services.

Challenges in Defining Organizational Financial Performance Indicators for

Mitigating Data Breaches

Organizational performance indicators are established to identify the business performance at an organization that shows the operational effectiveness at the organization's level (Bumblauskas et al., 2017; Juma'h & Alnsour, 2020). Bumblauskas et al. (2017) also added that fundamental to the effectiveness of the organizational financial performance indicators' approach is the existence of a cause-and-effect relationship between the indicators and financial performance. Karanja (2017) showed that reporting relationship represented by a hierarchical organizational structure, is considered as one of

the important indicators for making decisions and controlling resources in many organizations.

Ulven and Wangen (2021) defined organizational financial indicators as measurable values that explain the data breaches' impact on organizational financial performance, where IT security threats are considered harmful causes to organizational systems. The importance of cybersecurity risks, as well as data breach incidents, depends on their nature, range, and size (Skinner, 2019; Ulven & Wangen, 2021). Similarly, the importance of cybersecurity risks and data breach incidents depends on the harm range that data breach incidents may cause, where the harm includes the organization's reputation, financial performance, as well as customer and vendor relationships (Skinner, 2019).

Data breaches have a general impact on the organization's performance such as the impact on sales, revenue, liquidity, and profitability (Juma'h & Alnsour, 2020; Syed Emad et al., 2021). Juma'h and Alnsour (2020) added that announcements about data breaches can be used as an indicator in the organization, where data breaches have a significant negative impact on the organization's values. Similarly, the announcement about data breaches may lead to abnormality in organizational financial indicators that impact investors' confidence in the organizational market (Syed Emad et al., 2021). The impact of the organization's announcement about data breaches may have an impression on future cash flows, the required rate of return, financial distress, as well as credit rating (Karanja, 2017; Syed Emad et al., 2021). The studies discussed in this section are summarized in Table 23.

Table 23*Literature Summary of Challenges in Defining Organizational Financial Performance**Indicators*

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ulven & Wangen, 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizational financial indicators are defined as measurable values, which explain the data breaches' impact on organizational financial performance.
Juma'h & Alnsour, 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Data breaches have a significant negative impact on the organization's values and general impact on an organization's performance.
Bumblauskas et al., 2017	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The effectiveness of the organizational indicators approach is the existence of a cause-and-effect relationship between the organizational indicators and financial performance.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Syed Emad et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The impact of an organization's announcement about data breaches may have an impression on future cash flows, the required rate of return, financial distress, and credit rating.
Karanja, 2017	Empirical	Commentary	Digital Libraries	Reporting relationships in a hierarchical organizational structure is an important indicator for making decisions and controlling resources.
Skinner, 2019	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	The importance of data breach incidents depends on their nature, range, and size, besides the harm range caused by data breach incidents

Comparing Organizational Financial Performance Indicators Before and After

Data Breach Incidents

As organizations need asset management, capital control, production cost regulation, and increasing income, financial performance indicators are used to evaluate the organizations' performance, where organizational financial performance relies on cybersecurity efficiency in organizations (Chia-Nan et al., 2022). Thus, organizations

impacted by data breaches attempt to avoid financial loss, but the organizations need to adequately invest in cybersecurity to avoid IT security risks, where cyber attackers cause data breaches for monetary gain (Gupta et al., 2021). Bian et al. (2020) showed that although new technologies may have potential advantages, the organizational IT process still needs to be reviewed before implementation.

Information systems in organizations manage electronic data, automate communication and decision support, reduce misuse, as well as improve efficiency and effectiveness (Shrivastava et al., 2021). Bian et al. (2020) showed that organizations often move their data to the cloud quickly, but migration may cause issues if any organization's business does not adapt to the new environment quickly. However, organizations need to completely understand the basics of cloud computing before they migrate to it to avoid IT security risks such as data breaches in cloud SaaS platforms (Bian et al., 2020).

Financial service operations collect sensitive data that are related to protected financial information, as well as users have a great concern for the privacy of the sensitive data, because the users may be more likely to have data breaches and violations of privacy (Dzidzah et al., 2020). Shrivastava et al. (2021) gave an example of recent data breach incidents that impacted electronic patient data storage in medical organizations such as hospitals, where 18% of all data breaches occurred in the healthcare sector in 2019. Data breaches are usually associated with unauthorized access, alteration, destruction, or loss of data, where data loss could be the result of a cyber incident such as a malware attack or natural disasters such as earthquakes (Dzidzah et al., 2020; Shrivastava et al., 2021). Han et al. (2019) showed that as data breaches impact organizational financial performance, organizations must take action to reduce the data breaches, where the action will encourage

the organizations' customers to be confident, as well as the organizations will contribute a positive impact towards their financial performance. The studies discussed in this section are summarized in Table 24.

Table 24

Literature Summary of Comparing Organizational Financial Performance Indicators Before and After Data Breach Incidents

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Chia-Nan et al., 2022	Quantitative Survey	24 SMEs	Surveys for SMEs	Financial performance indicators are used to evaluate an organization's performance for increasing its income.
Gupta et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Organizations impacted by data breaches attempt to avoid financial loss by adequately investing in cybersecurity.
Bian et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations must understand the basics of cloud computing before using it to avoid data breaches in cloud SaaS platforms.
Shrivastava et al., 2021	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Digital research news (LexusNexis database)	Data breaches are usually associated with unauthorized access or loss of data, where data loss could be the result of a cyber event or natural disaster.

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Dzidzah et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Users have a great concern for the privacy of sensitive data because they might have data breaches and violations of privacy.
Han et al., 2019	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations must take action to reduce the data breaches that impact organizational financial performance.

Evaluating Past Cases of Data Breaches in Cloud SaaS Platforms in Organizations

Organizations must report data breaches to supervisory authorities, where implementing IT security solutions can help detect, alert, and report data breaches, as well as monitor and report any unauthorized or illegal access attempts (Georgiou & Lambrinouidakis, 2020). Similarly, risk assessments allow organizations to evaluate their cybersecurity controls to protect against future losses, where risk assessments include identifying system features, threat assessment, vulnerability analysis, impact analysis, as well as risk determination (David & Dhillon, 2019). Georgiou and Lambrinouidakis (2020) added that risk cases related to cloud SaaS platforms in the organization can be reported when the risks are identified using risk assessments.

Dinger and Wade (2019) evaluated 17 cases of public disclosures of data breaches in recent years, where the cases identified issues related to long-term financial damages caused by the data breaches. Palanisamy and Wu (2021) showed that perceived security in technology refers to the degree to which users believe that a certain technology or service is at a high level of security, while perceived security in organizational systems refers to

the degree to which users believe that the information is at a high level of security with less risk during the use of organizational systems. However, these studies measured perceived security in technology using self-assessment, which is questionable when it comes to its true impact on organizational performance (Zizic et al., 2022). Moudud-Ul-Huq et al. (2020) added that data security detection related to the security and insurance of customers' information may show unapproved access and device hacking in cloud computing.

Cloud service providers face direct obligations related to data processing activities under the general data protection regulation, where the cloud service providers will need to ensure that their product agreements with their customers comply with the data protection regulation (Georgiopolou et al., 2020). Similarly, the IT security level depends on customer service, where the organizations that use cloud computing must have better skills in giving a high level of IT security, which leads to greater dependability and security in the cloud computing framework (Moudud-Ul-Huq et al., 2020). However, failure to comply with the data protection regulation may result in the customers and local data protection authorities thrusting fines against the cloud service providers (Georgiopolou et al., 2020; Palanisamy & Wu, 2021). The studies discussed in this section are summarized in Table 25.

Table 25

Literature Summary of Evaluating Past Cases of Data Breaches in Cloud SaaS Platforms

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Georgiou & Lambrinouidakis, 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Organizations must report data breaches to supervisory authorities using implemented IT

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
David & Dhillon, 2019	Empirical	Commentary	Cloud SaaS Platforms	security solutions. Risk assessments allow organizations to evaluate their cybersecurity controls to protect against future losses.
Dinger & Wade, 2019	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	Around 17 cases of public disclosures of data breaches in recent years were evaluated to identify issues related to long-term financial damages caused by data breaches.
Georgiopoulou et al., 2020	Quantitative Survey	24 SMEs	Surveys for SMEs	Cloud SaaS providers need to ensure that their product agreements with their customers comply with the data protection regulation.
Palanisamy & Wu, 2021	Empirical	Commentary	Cloud SaaS Platforms	Perceived security in technology indicates that a certain technology or service is at a high level of security, while perceived security in organizational systems indicates that the

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Zizic et al., 2022	Empirical	Commentary	Cloud SaaS Platforms	information is at a high level of security. These studies measured perceived security in technology using self-assessment when it comes to the impact on organizational financial performances.
Moudud-UI-Huq et al., 2020	Multiple Case Study Analysis Method	100 Sample Cases of Data Breach Incidents	Cloud SaaS Platforms	A high IT security level leads to greater dependability and security in the cloud computing framework.

Summary of What Is Known and Unknown in Literature

It is known that organizations throughout the world create their Internet projects as enterprise applications based on cloud computing and SaaS technology, where these applications may suffer from IT security risks such as data breaches (Grubisic, 2014). It is known that data breaches are considered a high IT security risk in cloud SaaS platforms that organizations may face (Kaur & Bhardwaj, 2015; Singh & Malhotra, 2016). Data breaches still exist in cloud SaaS platforms which result in data leaks and data theft of customers (Akinbowale et al., 2020; Bhardwaj et al., 2016).

It is known that organizations make investments in IT security and another investment to train their employees (Eling & Schnell, 2016). IT security investments will never be sufficient if they are not associated with the necessary organizational financial performance

indicators (Hoppe et al., 2021). Organizations need to develop SETA programs to help their non-technical employees stay alert to help prevent data breaches, because non-technical employees are not aware of cybersecurity risks and how their actions may cause a data breach (Zhang et al., 2021).

This research aimed to empirically assess the investments in cybersecurity and financial performance before as well as after data breach incidents that impacted different organizations, address providing appropriate investment in organizations for IT security, as well as enhance cybersecurity posture in organizations. It appears that very little is known about organizations' investment in their IT security is associated with data breaches in their cloud SaaS platforms (He et al., 2020). Although the annual budget is provided by organizations to invest in IT security, cybersecurity prevention continuously changes to keep up with new methods that attackers use to cause data breaches (Chidinma et al., 2019; Zhang et al., 2021). Failure of organizational cybersecurity efforts to mitigate IT security risks and data breaches in organizations leads to damage to their business (Klamut, 2018).

It appears that very little is known about how organizations can reduce data breaches using their existing cybersecurity posture and without implementing strong security in the cloud with various solutions, which requires a high budget for cybersecurity (Harrison et al., 2015; Khayer et al., 2021). Thus, it appears that the existing gap in the literature can be reduced by assessing the investments in cybersecurity and financial performance in different organizations. Additional research can be done to address the organizational financial performance indicators that may reduce cybersecurity risks and data breaches in cloud SaaS platforms in organizations.

Chapter 3

Methodology

Overview of Research Design

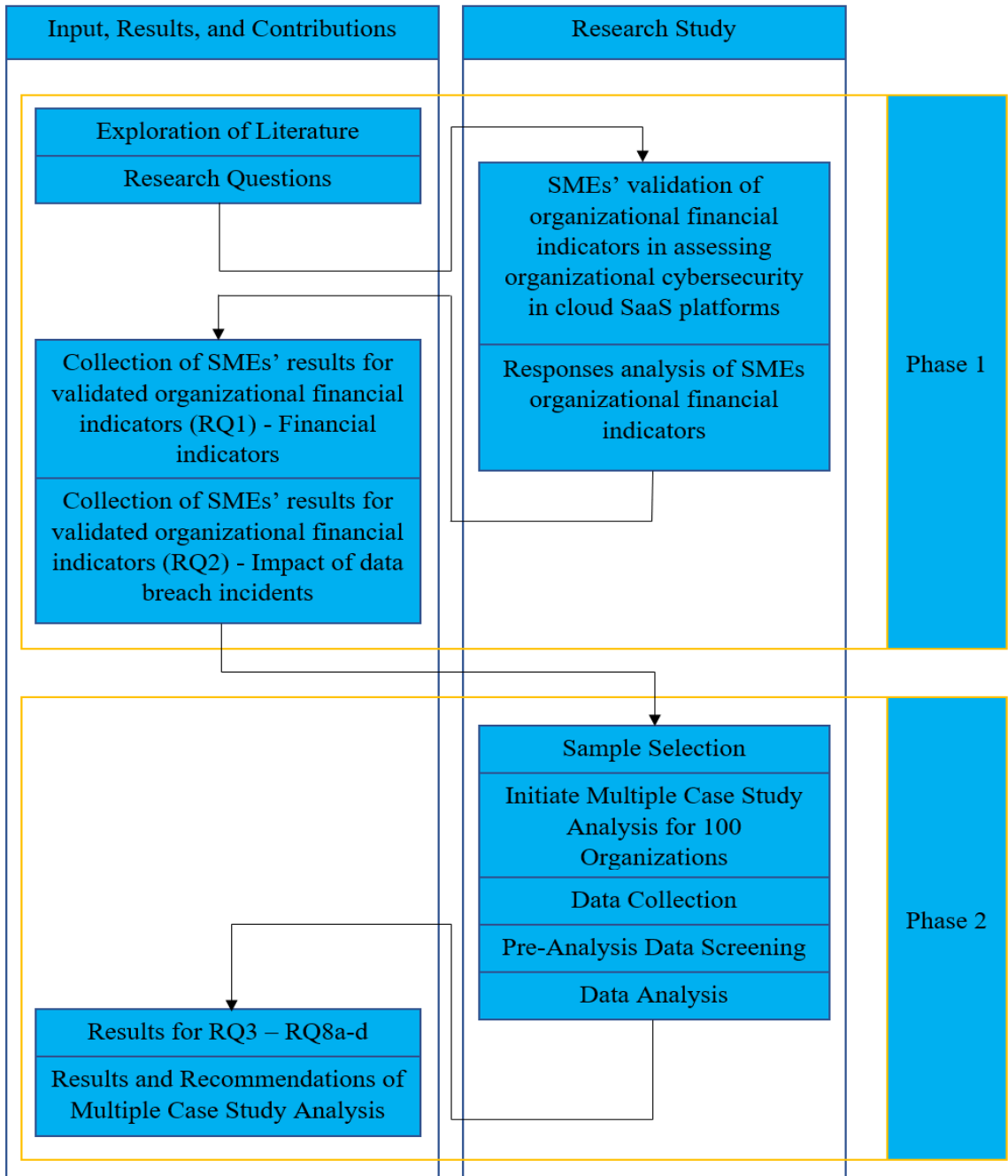
This research design was defined as a multiple case study analysis. A sequential quantitative-qualitative survey was used to collect opinions from SMEs, as well as case samples from the LexusNexis database. The qualitative data were derived from the open-ended questions in the SME survey. The open-ended questions included an assessment of the SMEs' opinion related to the possibility of any other financial performance indicators, which were valid components in assessing investment in cybersecurity in organizations that operate cloud SaaS platforms. This study answered the eight research questions that included assessing the relationships between the investigated variables. This research study empirically compared the organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations, which operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident.

This study also addressed the organizational financial performance indicators that may reduce cybersecurity risks and data breaches in cloud SaaS platforms in organizations. It appears that IT security issues continue to exist in platforms developed using SaaS and cloud computing. This research used an SME survey to first validate the organizational financial performance indicators relevant to the study of cybersecurity and then digital research news (LexusNexis database) to evaluate archived data of multiple past cases for

data breach incidents, which were reported between 2010 and 2023 in cloud SaaS platforms in different organizations. This research was conducted in two phases as shown in Figure 2.

Figure 2

Overview of Research Design Process



Phase I was based on a panel of several SMEs who have experience in organizational financial performance indicators and cybersecurity to assess organizational cybersecurity posture in cloud SaaS platforms. Phase II included the case analysis of the 100 organizations to empirically compare the organizational financial performance indicators before and after data breach incidents of 100 organizations that operate cloud SaaS platforms.

Measures

Phase I Measures: SMEs Assessment

Phase I of this research used an SME survey to obtain answers from SMEs using quantitative and qualitative questions (Wen-ai et al., 2012). The answers were collected from the first two sections of the given survey to empirically propose the approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity. The SME survey sections included organizational financial indicators evaluation, the impact of data breach incidents on organizational financial indicators, and demographics.

The first two sections of the SME survey evaluated the level of agreement from 1 = Strongly Disagree to 7 = Strongly Agree for the relevant organizational indicators as it pertains to assessing investment in cybersecurity in organizations that operate cloud SaaS platforms. The third section of the SME survey captured the SMEs' demographic information to assess their level of cybersecurity and/or financial experience in organizations.

The SME survey was sent to 100 SMEs using an invitation email that is included in Appendix A. The SMEs were asked to answer questions in the survey that are included in

Appendix B to evaluate the organizational financial performance indicators (Eitosa Jorge et al., 2022). Eitosa Jorge et al. (2022) noted that the SME survey collects information about the organizational financial performance indicators, as well as SMEs from different organizations who have experience in organizational financials and cybersecurity to assess organizational cybersecurity posture in cloud SaaS platforms.

Phase II Measures: The Case Analysis of the 100 Organizations

Phase II of this research followed the multiple case study analysis method to measure the research variables using the quantitative approach (Wen-ai et al., 2012). These variables were used to empirically compare the organizational financial performance indicators before and after data breach incidents of 100 organizations as shown in Figure 3. The research variables included Independent Variables (IVs), Dependent Variables (DVs), and Covariate Variables (CVs). IVs included the annual budget for cybersecurity, total expenses on IT, operating activities, investing activities, as well as financing activities. DVs included revenue, liabilities, as well as owners' equity accounts. CVs included total organizational assets, the number of total victims from a given organizational data breach, the size of the organization, as well as the U.S. state where the organization is located.

Figure 3

Organizational Financial Performance Indicators Before and After Data Breach Incidents

Organizational Indicators ▾	Before Incident ▾	After Incident ▾
Annual Budget for Cybersecurity	in USD Millions	in USD Millions
Total Annual Expenses on IT	in USD Millions	in USD Millions
Annual Operating Activities	in USD Millions	in USD Millions
Annual Investing Activities	in USD Millions	in USD Millions
Annual Financing Activities	in USD Millions	in USD Millions
Annual Revenue	in USD Millions	in USD Millions
Annual Liabilities	in USD Millions	in USD Millions
Annual Owner's Equity Account	in USD Millions	in USD Millions

The annual budget for cybersecurity was used as an IV. Organizational financial performance indicators have high predictions for employees' safety participation at an organization, which may use a measurement model to show the significant pathway from IT policy implementation to safety participation inside an organization (Adjekum, 2017). Adjekum (2017) noted that IT leadership makes the general rules for employees to complete their work successfully using the organizational information security policies, as well as SETA programs which are covered by the annual budget for cybersecurity.

Total annual expenses on IT were used as an IV. An organization should have employees with the necessary skills to adopt new technology, and the knowledge of IT is one of the factors for the adoption of technology in organizations (Trawnih et al., 2021). Trawnih et al. (2021) noted that the independent variables in this analysis may show technological and organizational financial performance indicators, whereas organizational financial performance indicators include employee experience and expense perception with management support. However, measuring perceptions in the cybersecurity field has provided misleading results, as well as it has recommended focusing on the facts rather than employee perceptions (Morawiec & Sołtysik-Piorunkiewicz, 2022; Vielberth et al., 2021).

Annual operating activities were used as an IV. Any organization works to achieve its main target of profit by enhancing sales volume, upward adjustment of the price, as well as cutting expenses due to the reduction of costs (Ismagilova Fairuza & Mirolyubova, 2012). Ismagilova Fairuza and Mirolyubova (2012) noted that the organization assesses the annual operating activities that the leadership is responsible for to achieve the organizational targets. Managers depend on economic and organizational financial

performance indicators when they assess annual operating activities, where these indicators are used by respondents when there is an orientation to support an organization's strategy (Ismagilova Fairuza & Mirolyubova, 2012).

Annual investing activities were used as an IV. Competition between organizations in an industry may depend on technology that results in the industry restructure, where these organizations implement technology under annual investing activities to achieve a competitive advantage (Trawnih et al., 2021). Trawnih et al. (2021) noted that organizations may use financial performance indicators to analyze their data to measure organizational financial performance, where the financial performance indicators are supported by the organization's top management.

Annual financing activities were used as an IV. Several organizations give credit to other businesses for participating in annual financing activities that are created by these organizations (Mehedi et al., 2020). Mehedi et al. (2020) noted that the organizations are responsible for credits through the institutional environment during developing economies, where these organizations can use pooled regression analysis to find out the association between the credits and organizational financial performance indicators.

Annual revenue was used as a DV. Performance assessment models may improve facility management functions in organizations, and key performance indicators may improve the performance of facilities with the annual revenue of these organizations to result in a successful business based on the focus on revenue (Yousefli et al., 2017). Yousefli et al. (2017) noted that integrated performance-based maintenance management develops methods to integrate indicators for the performance and efficiency of maintenance

in an organization, where these indicators are organizational financial performance indicators of the maintenance unit.

Annual liabilities were used as a DV. Organizational financial performance indicators are considered maintenance key performance indicators which can be used for integrating maintenance management, as well as manufacturing planning and control to result in successful operations at an organization to protect annual liabilities (Naji et al., 2020). The annual owners' equity account was used as a DV. Organizations may use pooled regression analysis to find the relationship between credits and organizational financial performance indicators, and the profitability of these organizations can be measured by return on equity (Mehedi et al., 2020).

Total organizational assets were used as a CV. The sector of the economy is linked to factors determined by using expert methods, where these methods cover different indicators such as indicators of the financial conditions and organizational financial performance indicators (Lukashevich & Garanin, 2016). Lukashevich and Garanin (2016) noted that using traditional models based on ratio analysis for estimating the probability of default for an organization may not help monitor financial issues for this organization, and some key factors for these financial issues are the return on assets and the structure of current assets.

The organization's size, the U.S. state where the organization is located, and the number of total victims from a given organizational data breach were used as CVs too. The security quality in cloud SaaS platforms can reduce the risks related to data breaches that may affect the organizational financial performance indicators (Ana Paula Beck da et al., 2018). Ana Paula Beck da et al. (2018) also noted that data breaches have an impact on

annual revenue, liabilities, and owner's equity accounts after controlling for the non-financial performance indicators. The non-financial performance indicators included total organizational assets, the number of total victims from a given organizational data breach, the size of the organization, and the U.S. state where the organization is located (Ana Paula Beck da et al., 2018). This study measured IVs, DVs, and CVs that are involved in data breach incidents, as well as determined the relationships between these variables as shown in Table 26 and Figure 4 (Ongaki, 2019; Su, 2018).

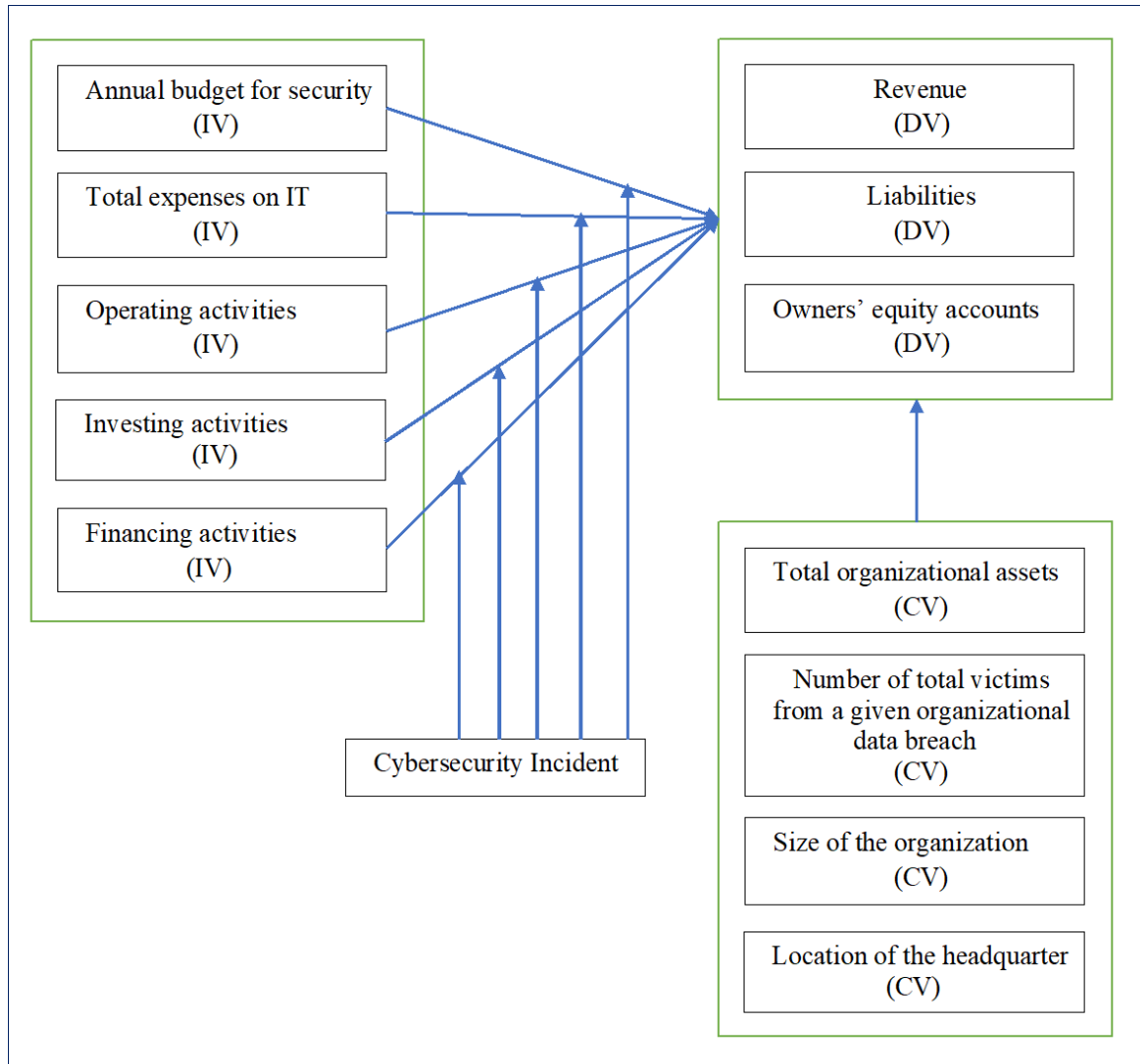
Table 26

Research Variables for Research Questions

Independent Variables (IVs)	Covariate Variables (CVs)	Dependent Variables (DVs)
Annual budget for cybersecurity	Total organizational assets	Revenue
Total expenses on IT	Number of total victims from a given organizational data breach	Liabilities
Operating activities	Size of the organization	Owners' equity accounts
Investing activities	U.S. state where the organization is located	
Financing activities		

Figure 4

Conceptual Model for the Role of Organizational Financial Performance Indicators on Overall Organizational Financial Performances Before and After a Data Breach

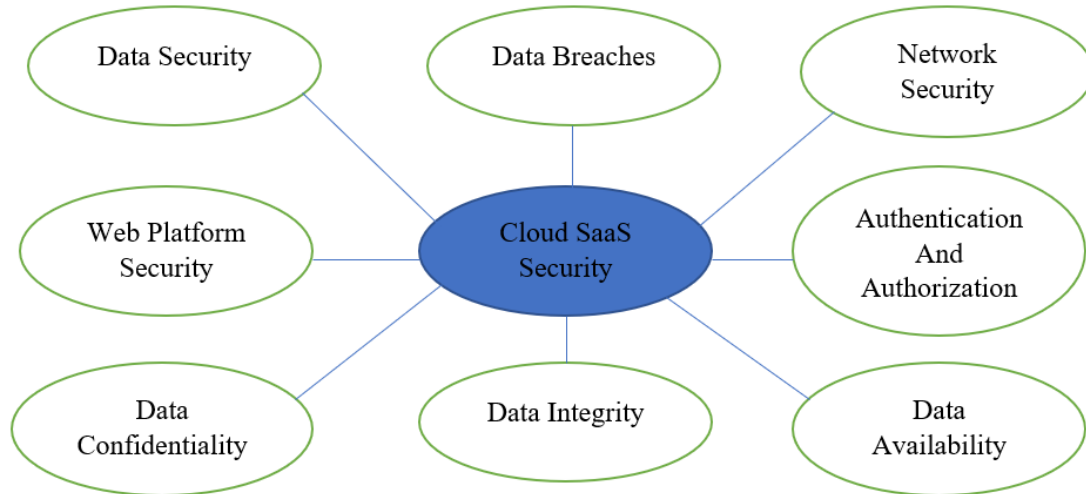


Validity and Reliability

All case samples were selected from the organizations that suffered from data breach incidents in their cloud SaaS platforms to identify the validity and reliability of these case samples, as well as how these incidents impacted the organizational financial performance indicators (research variables) (Su, 2018). The descriptive statistics selected from the sample included the selection of the mean, standard deviations, and other statistical outputs to evaluate the results of this study (Ongaki, 2019; Su, 2018). Ongaki (2019) also noted that the validity is evaluated based on the research study and instruments.

Threats to internal validity may include data quality such as missing or incomplete data, selection bias, as well as unmeasured confusion that exists in collected data (Price-Haywood, 2018). Price-Haywood et al. (2018) also noted that minimizing threats to internal validity can be done by providing a prior specification of research questions, targeting specific populations impacted by data breach incidents in organizations, selecting a research design that is conducted to answer the research questions, and using analytic research methods such as regression.

Threats to external validity may include the sample in this research study that does not represent all U.S. organizations (Ava Clare Marie, 2017). The results can only be generalized to populations where organizations use cloud SaaS platforms (Khamprapai et al., 2021). The sample needs to include organizations from different sectors such as banking and hospitals for higher population validity (Koul & Eydgahi, 2018). Minimizing threats to external validity can be done by selecting 100 organizations within the U.S., which could help in generalizing across a wider population when selecting various organizations impacted by data breach incidents (Ava Clare Marie, 2017; Koul & Eydgahi, 2018). Each one of these organizations has at least one cloud SaaS platform that had a data breach incident between 2010 and 2023 due to the lack of investment in cybersecurity as shown in Figure 5 (Khamprapai et al., 2021).

Figure 5*Cloud SaaS Security*

Threats to reliability may include threats to data stability over time and in different cases at an organization (Sarti et al., 2015). Sarti et al. (2015) also noted that the research assessed the organizational investment for minimizing threats to reliability to ensure consistency in the concept of data breaches. This research also defined the criteria to provide the organizational financial performance indicators, which may reduce data breaches in cloud SaaS platforms to minimize threats to reliability (Bishop et al., 2015).

Proposed Sample*Phase I: SMEs' Assessment*

In Phase I of this study, the sample was chosen by sampling from SMEs in some organizations who have experience in organizational financial indicators and/or cybersecurity experts. This study plan was to contact 100 SMEs to participate in the SME survey. The sample of SMEs included 24 participants in this study. Results from this study were anticipated to be a 24% response rate. SMEs were chosen based on their experience

in organizational financial indicators and cybersecurity to assess the cybersecurity posture in cloud SaaS platforms in organizations (Špaček, 2021).

The SMEs were asked to evaluate the organizational financial indicators using the 7-point Likert scale questions in the SME survey (See Appendix B). The SME survey items assess the impact of data breach incidents on the financial indicators in organizations that operate cloud SaaS platforms (Lucianetti et al., 2019). The SMEs were asked to evaluate the impact of data breach incidents on the financial indicators too using the 7-point Likert scale questions in the SME survey (See Appendix B).

Gallagher et al. (2012) noted that organizations may utilize SMEs from the business units based on their knowledge of business processes and IT systems, which helps collect information in the SME survey. Some of the SMEs who take the survey may have experience in quality measurement, where they may work together in the organization, work in different departments in the same organization, or work in different organizations (Gallagher et al., 2012; Reed et al., 2020). The SME survey consisted of different sections that may include Likert scale questions, multiple choice questions, as well as open-ended questions, which were used to empirically propose the approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity (Khatibian et al., 2010; Reed et al., 2020).

Open-ended questions were used in this study to collect qualitative data (Khatibian et al., 2010). The SME survey listed the answers to the open-ended questions when answering other financial performance indicators. There was an option if there are any other financial performance indicators that are valid components in assessing investment in cybersecurity in organizations that operate cloud SaaS platforms (Kirkness, 2021; Wu et al., 2019).

Phase II: The Case Analysis of the 100 Organizations

In Phase II of this study, the sample was chosen by sampling from the LexusNexis database which provides over 15,000 credible news, business, and legal sources. The sample of LexusNexis database included 100 organizations in the U.S. that reported data breach incidents between 2010 and 2023. These organizations disclosed their data breaches that may have compromised the personal data of their employees or customers. The data breaches impacted cloud SaaS platforms in these organizations.

The sample included organizations that were reported between 2010 and 2023 to suffer from data breach incidents. These years are examples of when data breaches happened and impacted organizations. Different cyber-attacks have increased rapidly during using new technologies in recent years, where data breaches have been an example of cyber-attacks (Zwilling, 2022). Zwilling (2022) also noted that the increase in data breaches needs advanced detecting and defending procedures. Employees and customers in different organizations have been subject to the impact of data breaches (Xu et al., 2022; Zwilling, 2022). Xu et al. (2022) also noted that traditional ways to identify cyber-attacks and data breaches in organizations are not efficient, which may lead to cybersecurity risks.

In recent years, people have heard from the news that many organizations suffered from data breaches that impacted their cloud SaaS platforms (Teng, 2022). Teng (2022) also noted that the organizations may have lost millions of dollars due to data breaches and cybersecurity issues. Teng (2022) stated, "In 2016, the LinkedIn network platform spread to nearly 500 million users. The economic losses caused by data breaches averaged 3.6 million U.S. dollars each year, according to the report released by IBM in 2020" (p. 1). Cyber adversaries can blackmail organizations by demanding millions of dollars as ransom

when they steal their data (Murtaza et al., 2022). Murtaza et al. (2022) also noted that some organizations lost millions of dollars after falling victim to different types of cyber-attacks such as BEC and phishing emails.

Alaoui and El (2022) noted that web vulnerabilities are continuously growing due to the large use of web applications such as cloud SaaS platforms. Many cloud SaaS platforms can be vulnerable and subject to data breaches if there is an intrusion caused by unauthorized access to the platforms (Alaoui & El, 2022; Nagarajan & Kumar, 2021). Cybersecurity threats caused by data breaches in cloud computing may include poor identity and authentication, insecure user interfaces, cloud system vulnerabilities, as well as malicious use of cloud services (Cho et al., 2021).

Kude et al. (2017) noted that data were collected from U.S. customers who were affected by Target's data breach using a market research firm that contacted these customers. The sample consisted of 2,500 customers who covered a variety of income levels, as well as an average age of 31.4 years in the respondent group (Kude et al., 2017). Kude et al. (2017) also noted that 212 customers (58% of them are males) provided responses with a response rate of 8.5%, as well as all responses were collected after Target had announced compensation due to the data breach. The data breach incident that impacted Target is one of the 100 sample cases to be presented in this research study, where its financial performance indicators on annual revenue, liabilities, and owner's equity account showed different results on Target's annual financial reports before and after reporting the data breach incident in its cloud SaaS platforms (Kude et al., 2017).

Adonis and Ngcamu (2016) noted that some managers in a financial institution contacted their employees who were affected by a data breach incident in this institution,

where the location of the institution is in South Africa. Their purpose was to collect information about the data breach impact on their employees, but some of their employees ignored the response of collecting information about the data breach impact (Adonis & Ngcamu, 2016). Adonis and Ngcamu (2016) also noted that it is estimated that approximately 500 employees were contacted, as well as 81 employees replied with a response rate of 16.2%. The data breach incident that impacted the financial institution is also an example presented in this research study, where its financial performance indicators on annual revenue, liabilities, and owner's equity account showed different results on the annual financial reports for this institution before and after reporting the data breach incident in its cloud SaaS platforms (Adonis & Ngcamu, 2016).

Pre-Analysis Data Screening

This research required data accuracy, assessing incomplete data for organizational financial performance indicators, as well as assessing outliers (Mertler & Vannatta, 2016). Mertler and Vannatta (2016) also noted that all fields for these indicators are required to avoid incomplete data. This research screened the data to identify missing data, outliers, and keying errors, as well as to evaluate the fulfillment of test assumptions of normality, linearity, and homoscedasticity (Tyler et al., 2016). Descriptive statistics were used for pre-analysis data screening, as well as for exploring the features and distribution of the variables (Mertler & Venetta, 2016; Secret et al., 2011). Tyler et al. (2016) noted that descriptive statistics of all demographic items were run, and the results were visually checked to verify the accuracy of data entry.

Data Analysis

Phase I: SMEs' Assessment

In Phase I of this study, a panel of several SMEs who may represent some organizations was chosen based on their experience in organizational financial indicators and cybersecurity, which are valid in assessing organizational investment in cybersecurity in cloud SaaS platforms (Špaček, 2021). This study plan was to acquire 24 SMEs by contacting 100 SMEs. An example of an invitation email to SMEs can be found in Appendix A. A target response rate of 24% is anticipated for participation. The SMEs were asked to evaluate the financial indicators using scale questions in the given survey. An example of an SME survey can be found in Appendix B. Špaček (2021) also noted that after receiving the answers from the SMEs, the survey results were calculated to find the validity score for the indicators. This process was used to answer RQ1.

The survey items for SMEs were also built based on the review of the literature for organizational financial indicators to evaluate the impact of data breach incidents on the financial indicators in organizations that operate cloud SaaS platforms (Lucianetti et al., 2019). The SMEs were asked to evaluate the impact of data breach incidents using scale questions in the given survey too. Lucianetti et al. (2019) also noted that the survey answers obtained from SMEs helped improve the clarity, validity, and comprehensiveness of the financial indicators. This process was used to answer RQ2.

Phase II: The Case Analysis of the 100 Organizations

In Phase II of this study, RQ3 has one IV (annual budget for cybersecurity) and three quantitative DVs (annual revenue, liabilities, and owner's equity account). One-way MANOVA was used to answer RQ3 (Mertler & Vannatta, 2016). RQ4 has one IV (total

annual expenses on IT) and three quantitative DVs (annual revenue, liabilities, as well as owners' equity account). One-way MANOVA was used to answer RQ4 (Mertler & Vannatta, 2016). RQ5 has one IV (annual operating activities) and three quantitative DVs (annual revenue, liabilities, as well as owners' equity account). One-way MANOVA was used to answer RQ5 (Mertler & Vannatta, 2016).

RQ6 has one IV (annual investing activities) and three quantitative DVs (annual revenue, liabilities, and owner's equity account). One-way MANOVA was used to answer RQ6 (Mertler & Vannatta, 2016). RQ7 has one IV (annual financing activities) and three quantitative DVs (annual revenue, liabilities, as well as owners' equity account). One-way MANOVA was used to answer RQ7 (Mertler & Vannatta, 2016). RQ8 has three DVs (annual revenue, liabilities, as well as owners' equity account) and four CVs (number of total victims from a given organizational data breach, total organizational assets, size of the organization, and the U.S. state where the organization is located). One-way ANCOVA was used to answer RQ8 (Mertler & Vannatta, 2016). A summary of research phases with proposed samples can be shown in Table 27.

Table 27

Summary of Research Phases with Proposed Samples

Research Question	Phase	Sample	Methodology	Analysis
RQ1	Phase I	24 SMEs	Quantitative-Qualitative Survey	Using quantitative and qualitative approaches to compare organizational indicators
RQ2	Phase I	24 SMEs	Quantitative-Qualitative Survey	Using quantitative and

Research Question	Phase	Sample	Methodology	Analysis
				qualitative approaches to compare organizational indicators
RQ3	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way MANOVA
RQ4	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way MANOVA
RQ5	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way MANOVA
RQ6	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way MANOVA
RQ7	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way MANOVA
RQ8	Phase II	100 Sample Cases	Multiple Case Study Analysis Method	One-way ANCOVA

Formats for Presenting Results

SME survey included Likert-type scale questions using the level of agreement of a 7-point scale with options from 1 – Strongly Disagree to 7 - Strongly Agree. Level of agreement had scale options such as 1 – Strongly Disagree, 2 – Somewhat Disagree, 3 – Disagree, 4 – Neither Agree nor Disagree, 5 – Agree, 6 – Somewhat Agree, and 7 - Strongly Agree.

Sample cases of data breach incidents for 100 organizations had different organizational financial performance indicators that can be amounts of millions or billions in U.S. dollars. The organizational financial performance indicators included the annual budget for cybersecurity, assets, liabilities, owners' equity accounts, revenue, total expenses on IT, operating activities, investing activities, and financing activities. The amount in U.S. dollars for each organizational financial performance indicator was shown before and after the data breach incident in this research study.

Resources

LexusNexis database via Alvin Sherman Library at Nova Southeastern University was used to find 100 sample cases for data breach incidents in cloud SaaS platforms. Hardware was used during the research. It may have included desktops and laptops. Cloud SaaS platforms were used in organizations as a target for this research study, where these platforms are web applications used as services and deployed within cloud computing. MS Excel and SPSS were also used as statistical analysis tools to complete statistics and calculations. Lists and graphs were created in spreadsheets using Excel and SPSS to analyze and compile the results.

Summary

The overall research methodology was presented in this chapter. A research design of multiple case study analysis using a quantitative approach was used to validate, test, collect, and analyze research data. The quantitative approach was also used in this research study to collect and process the data provided as a sequential quantitative-qualitative survey to collect opinions from SMEs. The goal of this research was to answer the following research questions:

The main research question that this study addressed was: What is the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

- RQ1: What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms?
- RQ2: What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms?
- RQ3: Are there any statistically significant mean differences for *the annual budget for cybersecurity* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ4: Are there any statistically significant mean differences for *total annual expenses on IT* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ5: Are there any statistically significant mean differences for *annual operating activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ6: Are there any statistically significant mean differences for *annual investing activities* on annual revenue, liabilities, as well as owners' equity accounts

before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ7: Are there any statistically significant mean differences for *annual financing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ8: Are there any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from data breach incidents after controlling for: (a) number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located?

The RQs were addressed in two phases. Phase I was based on a panel of several SMEs who have experience in organizational financial performance indicators and cybersecurity to assess organizational cybersecurity posture in cloud SaaS platforms. Phase II was based on the case analysis of the 100 organizations to empirically compare the organizational financial performance indicators before and after data breach incidents of the organizations that operate cloud SaaS platforms.

Chapter 4

Results

Overview

This chapter presents the results of the data collection and analysis from this research study. The main goal was to empirically compare the role of organizational financial performance indicators on annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations. The organizations operated cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. For Phase I, 100 SMEs were contacted to participate in the SME survey. The SME survey was answered by 24 participants, and the results from this study were anticipated to be a 24% response rate. The participants completed the SME survey, and a level of agreement was used to determine the minimum SMEs' consensus as 70% (Lucianetti et al., 2019; Su & Jang, 2020). The SMEs validated the organizational financial performance indicators relevant to the study of cybersecurity. Phase II used digital research news (LexusNexis database) to evaluate archived data of multiple past cases for data breach incidents in cloud SaaS platforms in different organizations. SPSS version 28 was used to calculate one-way MANOVA and one-way ANCOVA which were used to analyze the data collected in Phase II.

Phase I – SME Survey Feedback and Findings

RQ1 and RQ2 were answered using the findings from the SME survey. An invitation was sent as a message on LinkedIn to request participation from experts in organizational financial indicators, as well as cybersecurity experts. From the initial 100 SMEs invited to participate, 24 SMEs have responded. However, a few participants did not answer

questions about demographics and opened questions to add any additional organizational indicators via the SME survey. If a participant did not answer a demographic question in the SME survey (None selected), the non-selected answer was not included in calculating the mean, standard deviation, and level of agreement. The non-selected answers were included in the count of demographics. Frequency and percentage were calculated for the answers in the demographic descriptive statistics. The level of agreement and its percentage were calculated for the questions about organizational indicators.

Table 28 provides descriptive statistics of the 24 SMEs. The SMEs included finance administrators (4%), finance managers (8%), financial analysts (8%), and other professional roles (75%). The SMEs' years of professional experience included the range from 11 to 15 years (25%), from 16 to 20 years (17%), and over 20 years (54%). Three SMEs did not have professional certifications (13%). Eight SMEs had one professional certification (33%). One SME had three professional certifications (4%). Eight SMEs had two professional certifications (33%). Three SMEs had four or more professional certifications (13%). SMEs' professional certifications included accounting (4%), cybersecurity (21%), finance (17%), IT (13%), and other professional certifications (38%).

Table 28

Summary of SME Demographics (N=24)

Demographics Indicator	Indicator Item	Frequency (N)	Percentage
Age Group	30-39	8	33%
	40-49	3	13%
	50-59	10	42%
	60-67	2	8%
	(None selected)	1	4%
Gender	Female	5	21%
	Male	18	75%
	(None selected)	1	4%

Demographics Indicator	Indicator Item	Frequency (N)	Percentage
Highest Degree	Bachelor's degree	5	21%
	Doctorate (PhD, JD, MD, etc.) degree	7	29%
	Master's degree	11	46%
	(None selected)	1	4%
Current Employment Status	Full-time employment	21	88%
	Self-employed	2	8%
	(None selected)	1	4%
Main Work Industry	Critical manufacturing	1	4%
	Data processing	1	4%
	Education	3	13%
	Emergency services	1	4%
	Finance	5	21%
	Food services	1	4%
	Government facilities	3	13%
	Healthcare	4	17%
	IT / Communication	3	13%
	Transportation systems	1	4%
	(None selected)	1	4%
	Main Professional Role	Finance Administrator	1
Finance Manager		2	8%
Financial Analyst		2	8%
Other		18	75%
(None selected)		1	4%
Years of Professional Experience	From 11 to 15 years	6	25%
	From 16 to 20 years	4	17%
	Over 20 years	13	54%
	(None selected)	1	4%
Number of Professional Certifications	Four or more	3	13%
	None	3	13%
	One	8	33%
	Three	1	4%
	Two	8	33%
	(None selected)	1	4%
Professional Certifications	Accounting	1	4%

Demographics Indicator	Indicator Item	Frequency (N)	Percentage
	Cybersecurity	5	21%
	Finance	4	17%
	IT	3	13%
	Other	9	38%
	(None selected)	2	8%

Phase I - RQ1

Phase I addressed RQ1: What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms? This research question was answered with data from section A (Organizational Financial Indicators Evaluation) in the SME survey. For SMEs' responses in section A, level of agreement for annual budget for cybersecurity was 100%, level of agreement for total annual expenses on IT was 96%, level of agreement for annual financing activities was 92%, level of agreement for annual revenue was 92%, level of agreement for annual operating activities was 83%, level of agreement for annual liabilities was 83%, level of agreement for annual investing activities was 75%, and level of agreement for annual owners' equity account was 63%. A summary of the level of agreement in section A is shown in Table 29.

Table 29

Summary of Level of Agreement in Section A (N=24)

Section In SME Survey	Organizational Indicator	Level of Agreement (%)	SMEs Approved
A	Annual budget for cybersecurity	100%	Yes
A	Total annual expenses on IT	96%	Yes
A	Annual financing activities	92%	Yes
A	Annual revenue	92%	Yes
A	Annual operating activities	83%	Yes
A	Annual liabilities	83%	Yes
A	Annual investing activities	75%	Yes

Section In SME Survey	Organizational Indicator	Level of Agreement (%)	SMEs Approved
A	Annual owners' equity account	63%	No

Phase I – RQ2

Phase I also addressed RQ2: What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms? This research question was answered with data from section B (Impact of Data Breach Incidents on Organizational Financial Indicators) in the SME survey. For SMEs' responses in section B, level of agreement for annual budget for cybersecurity was 100%, level of agreement for total annual expenses on IT was 100%, level of agreement for annual operating activities was 88%, level of agreement for annual financing activities was 83%, level of agreement for annual revenue was 83%, level of agreement for annual liabilities was 83%, level of agreement for annual investing activities was 79%, and level of agreement for annual owners' equity account was 71%. A summary of the level of agreement in section B is shown in Table 30.

Table 30

Summary of Level of Agreement in Section B (N=24)

Section In SME Survey	Organizational Indicator	Level of Agreement (%)	SMEs Approved
B	Annual budget for cybersecurity	100%	Yes
B	Total annual expenses on IT	100%	Yes
B	Annual operating activities	88%	Yes
B	Annual financing activities	83%	Yes
B	Annual revenue	83%	Yes
B	Annual liabilities	83%	Yes
B	Annual investing activities	79%	Yes
B	Annual owners' equity account	71%	Yes

Phase I – Mean and Standard Deviation of Organizational Indicators

The mean and standard deviation of organizational indicators were calculated. OrgFinInd was used for the organizational financial indicators' evaluation in section A. IDBI-FI was also used for the impact of data breach incidents on organizational financial indicators in section B. The annual budget for cybersecurity (IDBI-FI) was found to have the highest mean (6.167). Annual owners' equity account (OrgFinInd) was found to have the lowest mean (4.133). Annual owners' equity account (OrgFinInd) was found to have the highest standard deviation (2.167). Annual budget for cybersecurity (IDBI-FI) was found to have the lowest standard deviation (1.020). The mean and standard deviation of organizational indicators are shown in Table 31, Figure 6, and Figure 7.

Table 31

Mean and Standard Deviation of Organizational Indicators of SMEs Feedback (N=24)

Organizational Indicator	Mean	Standard Deviation
Annual budget for cybersecurity (OrgFinInd)	6.292	0.859
Total annual expenses on IT (OrgFinInd)	5.833	1.090
Annual operating activities (OrgFinInd)	5.542	1.103
Annual investing activities (OrgFinInd)	5.375	1.056
Annual financing activities (OrgFinInd)	5.542	1.141
Annual revenue (OrgFinInd)	5.792	0.977
Annual liabilities (OrgFinInd)	5.750	1.189
Annual owners' equity account (OrgFinInd)	5.292	1.429
Annual budget for cybersecurity (IDBI-FI)	6.375	0.770
Total annual expenses on IT (IDBI-FI)	6.125	0.900
Annual operating activities (IDBI-FI)	5.667	1.308
Annual investing activities (IDBI-FI)	5.542	1.141
Annual financing activities (IDBI-FI)	5.625	1.096
Annual revenue (IDBI-FI)	5.542	1.021
Annual liabilities (IDBI-FI)	5.583	1.100
Annual owners' equity account (IDBI-FI)	5.417	1.381

Figure 6

Mean and Standard Deviation of Organizational Financial Indicators of SMEs Feedback

Related to RQ1 (N=24)

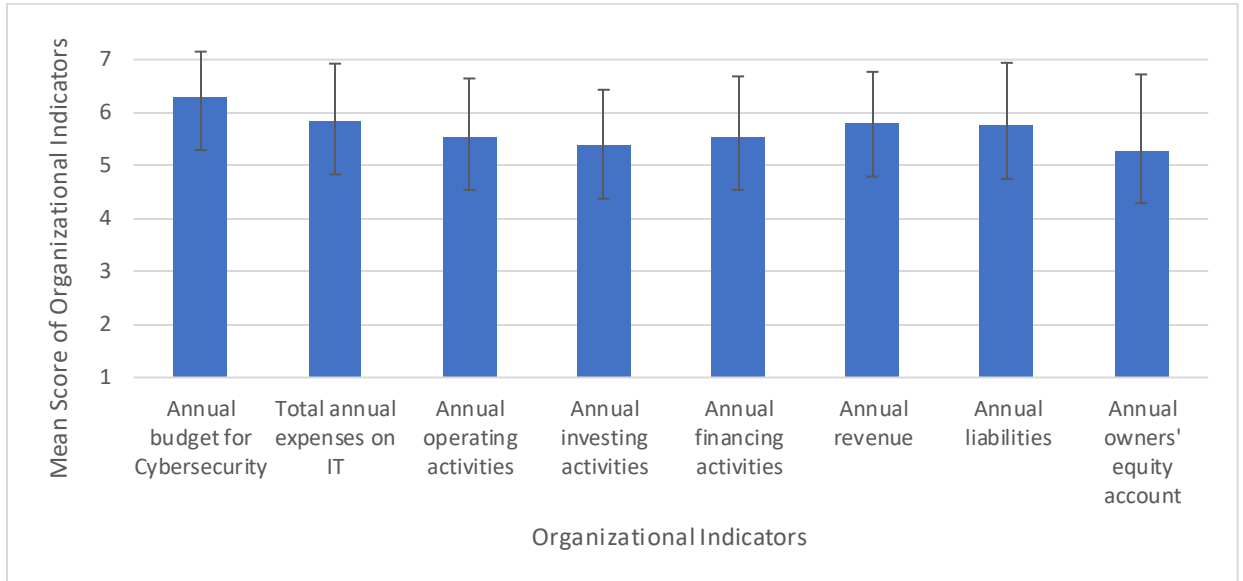
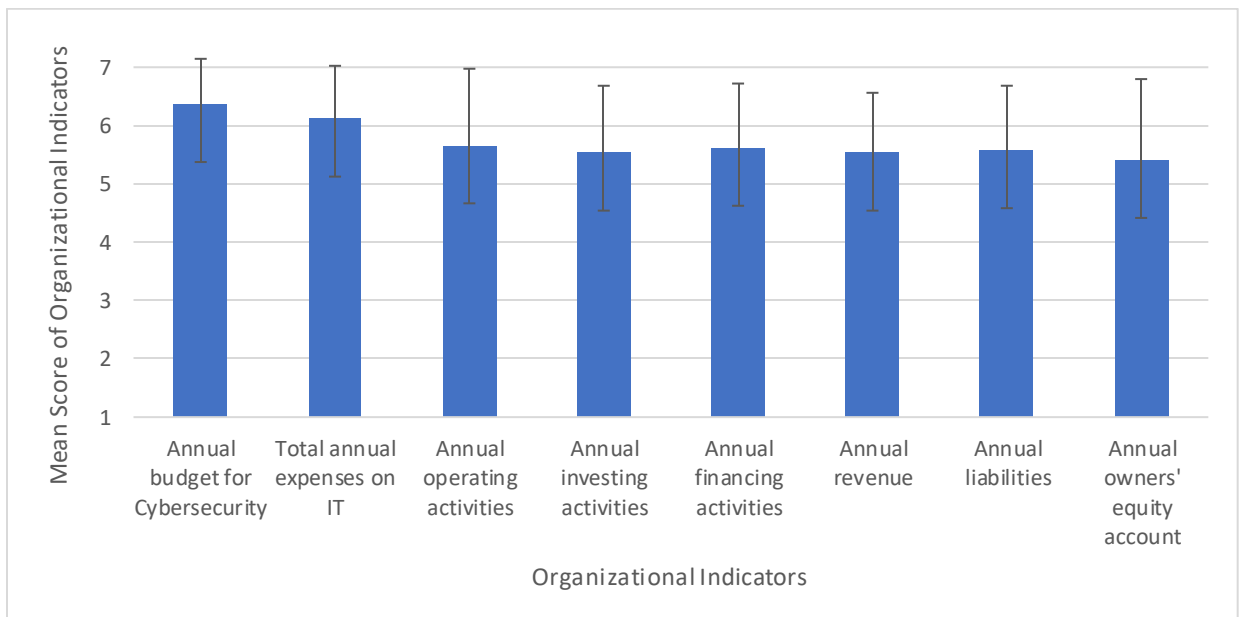


Figure 7

Mean and Standard Deviation of Organizational Financial Indicators of SMEs Feedback

Related to RQ2 (N=24)



Phase I – SMEs Level of Agreement for Organizational Indicators (N=24)

SMEs level of agreement for organizational indicators was calculated by finding (sum of the SME survey answers when the answer is Somewhat agree = 5 divided by 5 + sum of the SME survey answers when the answer is Agree = 6 divided by 6 + sum of the SME survey answers when the answer is Strongly agree = 7 divided by 7), then the total sum of all three was divided by the number of SMEs (24). The outcome of the calculation results in the total percentage agreement across all 24 SMEs ranging from 0% to 100%.

The target value of 70% was used to create the cut-off line for the minimum SMEs' consensus as shown in Figures 8, 9, and 10. Annual owners' equity account (OrgFinInd) was the only financial indicator that had less than 70% of the level of agreement. The other financial indicators that belong to Section A (OrgFinInd) and Section B (IDBI-FI) had more than 70% of the level of agreement. There is strong evidence that owners' equity accounts appear to have little impact on evaluating the organizational financial indicators from the SMEs' perspective. It was found that the level of agreement is above 70% when it comes to mitigating data breaches. The level of agreement for organizational indicators is also shown in Table 32 as well as Figures 8, 9, and 10.

Table 32

SMEs Level of Agreement for Organizational Indicators (N=24)

Organizational Indicator	Level of Agreement (%)	SMEs Approved
Annual budget for cybersecurity (OrgFinInd)	100%	Yes
Annual budget for cybersecurity (IDBI-FI)	100%	Yes
Total annual expenses on IT (IDBI-FI)	100%	Yes
Total annual expenses on IT (OrgFinInd)	96%	Yes
Annual financing activities (OrgFinInd)	92%	Yes
Annual revenue (OrgFinInd)	92%	Yes
Annual operating activities (IDBI-FI)	88%	Yes
Annual operating activities (OrgFinInd)	83%	Yes

Organizational Indicator	Level of Agreement (%)	SMEs Approved
Annual liabilities (OrgFinInd)	83%	Yes
Annual financing activities (IDBI-FI)	83%	Yes
Annual revenue (IDBI-FI)	83%	Yes
Annual liabilities (IDBI-FI)	83%	Yes
Annual investing activities (IDBI-FI)	79%	Yes
Annual investing activities (OrgFinInd)	75%	Yes
Annual owners' equity account (IDBI-FI)	71%	Yes
Annual owners' equity account (OrgFinInd)	63%	No

Figure 8

SMEs Level of Agreement for Organizational Indicators (OrgFinInd) with Cut-off Line

for Minimum SMEs Consensus (N=24)

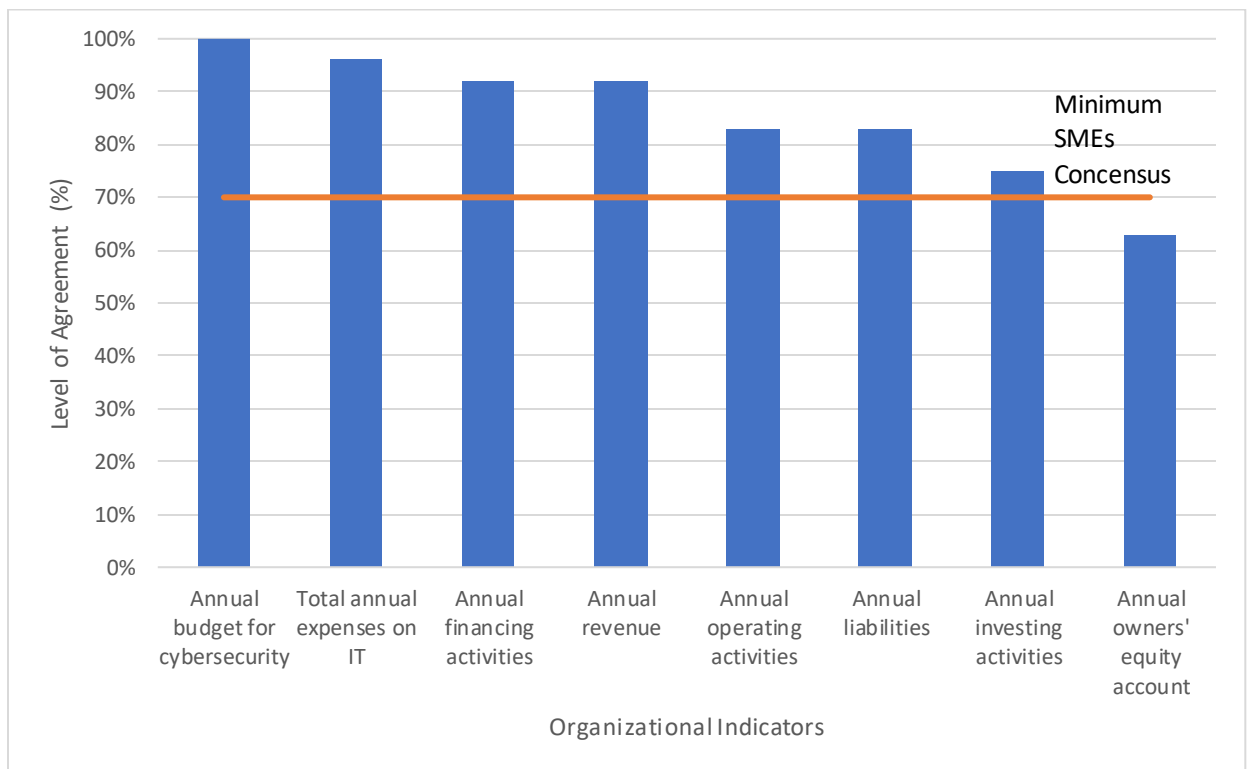


Figure 9

SMEs Level of Agreement for Organizational Indicators (IDBI-FI) with Cut-off Line for Minimum SMEs Consensus (N=24)

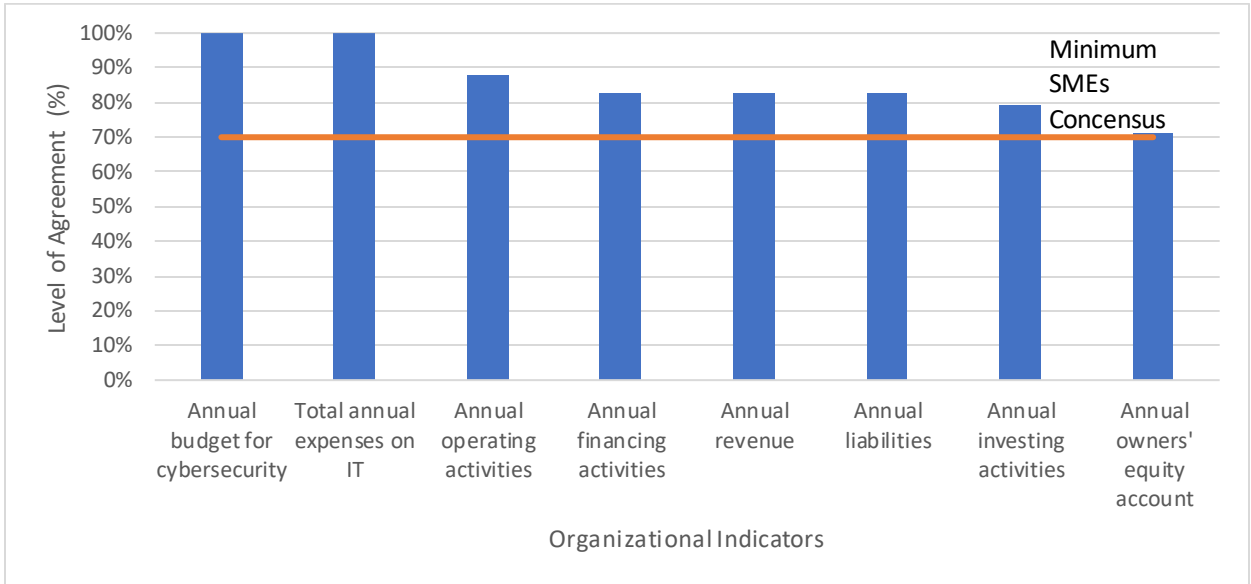
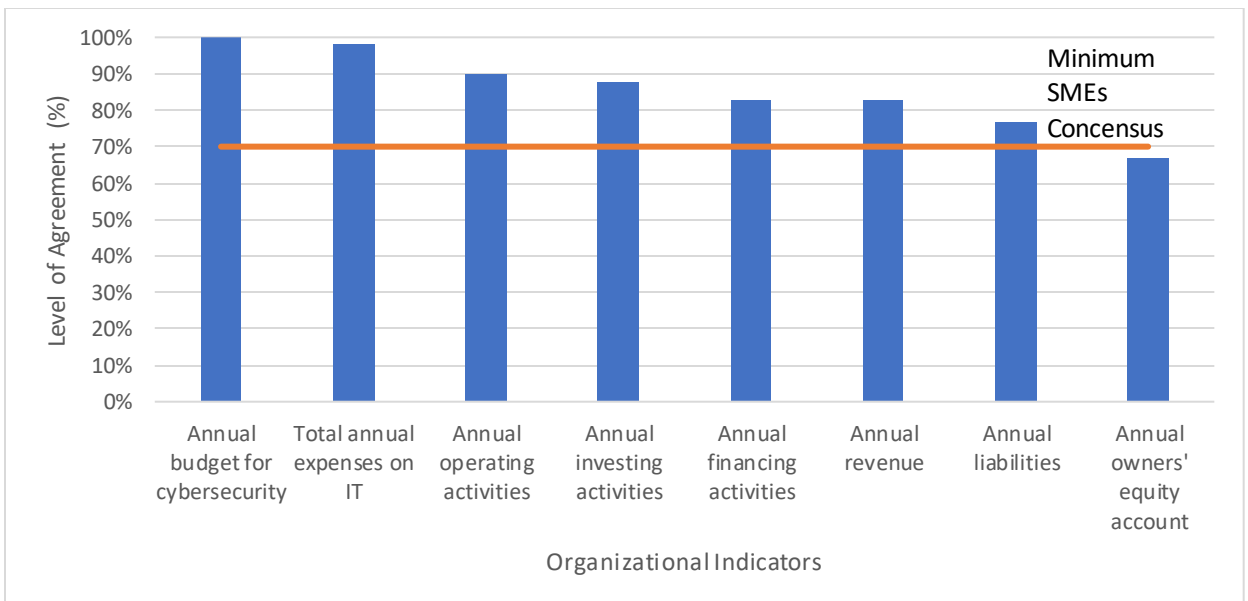


Figure 10

SMEs Level of Agreement for Organizational Indicators (Average of OrgFinInd and IDBI-FI) with Cut-off Line for Minimum SMEs Consensus (N=24)



Phase II – The Case Analysis of 100 Organizations

Phase II included the case analysis of the 100 organizations to empirically compare organizational financial performance indicators before and after data breach incidents of the organizations that operate cloud SaaS platforms. This research study was defined as a multiple case study analysis where the case samples were obtained from the LexusNexis database. Revenue, liabilities, owner's equity accounts, assets, operating activities, investing activities, and financing activities are organizational indicators that were added from the web in the annual financial reports.

Phase II – RQ3

Phase II addressed RQ3: Are there any statistically significant mean differences in *the annual budget for cybersecurity* on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? To answer RQ3, the annual budget for cybersecurity, annual revenue, liabilities, and owner's equity account before and after data breach incidents of 100 organizations were collected in millions of U.S. dollars. One-way MANOVA was used to test the significant differences in the annual budget for cybersecurity on revenue, liabilities, and owner's equity account before and after a data breach incident.

The results of the One-way MANOVA showed there was not a significant difference in the annual budget for cybersecurity on revenue ($F(df, err\ df)=1; p = 0.319$) before and after a data breach incident. There were significant differences in the annual budget for cybersecurity on liabilities ($F(df, err\ df)= 23.806; p < .001$) and owner's equity account ($F(df, err\ df)= 310.336; p < .001$) before and after a data breach incident. The results of the

One-way MANOVA to answer RQ3 are shown in Table 33. The estimated marginal means of revenue increased from Group 1 (before the incident) to Group 2 (after the incident) as shown in Figure 11. The estimated marginal means of liabilities increased from Group 1 (before the incident) to Group 2 (after the incident) as shown in Figure 12. The estimated marginal means of the owner's equity account increased from Group 1 (before the incident) to Group 2 (after the incident) as shown in Figure 13. Appendix C shows all organizational indicators with their description.

Table 33

One-Way MANOVA Results of Difference in Annual Budget for Cybersecurity on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
ANN_BUDGET _SEC	REVENUE	1	2,630,586,303	1	0.319
	LIABIL	1	1,169,246,307,912	23.806	<.001***
	OWN_EQUITY _ACC	1	4,701,967,533,221	310.336	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Figure 11

One-Way MANOVA Results of Difference in Estimated Marginal Means of Revenue Before and After Data Breach Incident (N=100)

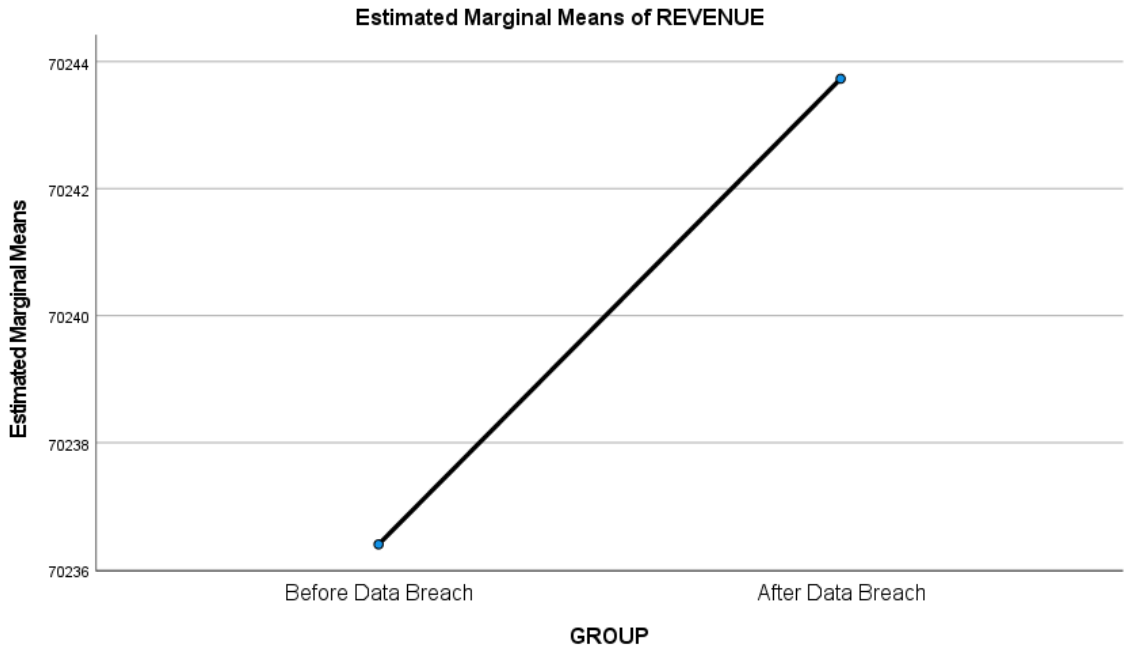


Figure 12

One-Way MANOVA Results of Difference in Estimated Marginal Means of Liabilities Before and After Data Breach Incident (N=100)

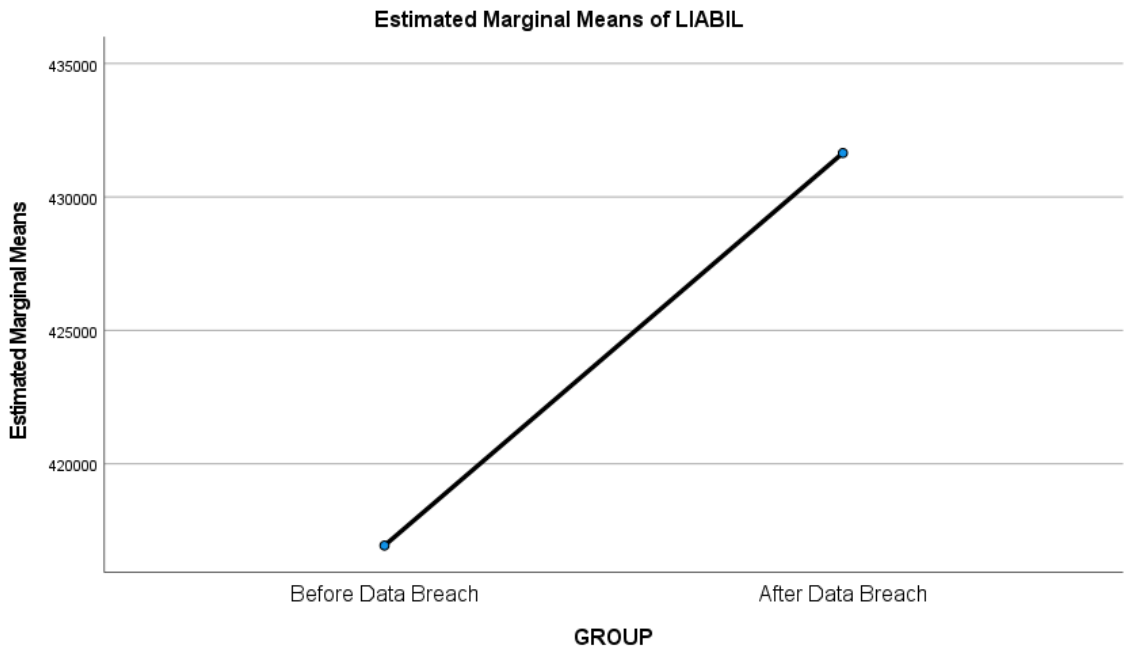
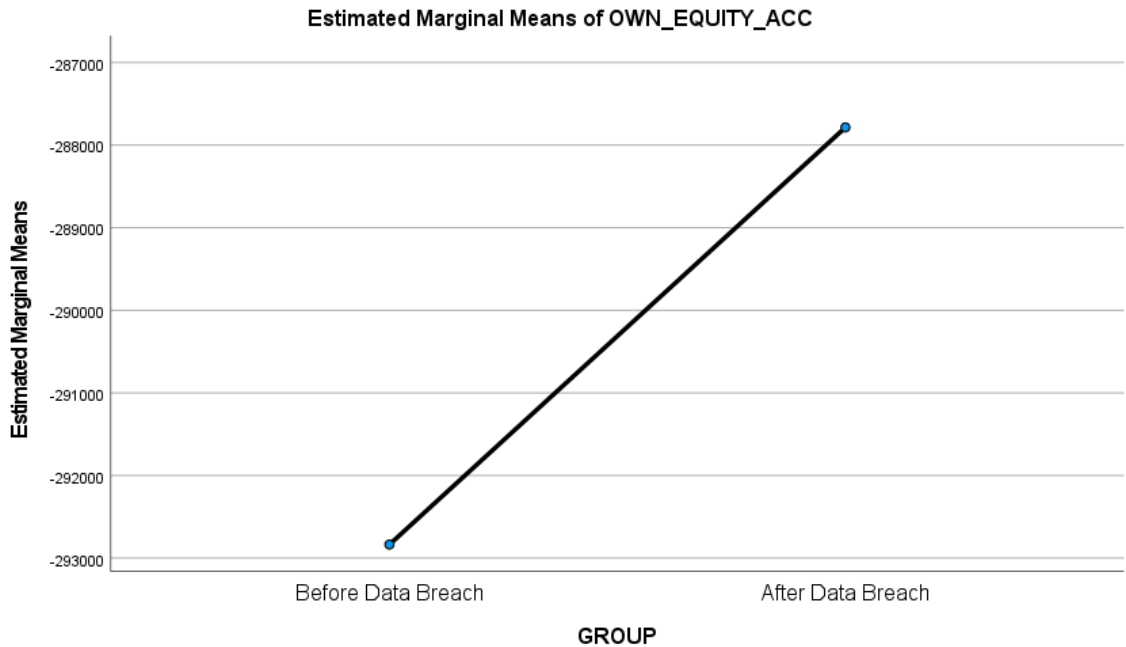


Figure 13

One-Way MANOVA Results of Difference in Estimated Marginal Means of Owner's Equity Account Before and After Data Breach Incident (N=100)



Phase II – RQ4

Phase II addressed RQ4: Are there any statistically significant mean differences for *total expenses on IT* on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? To answer RQ4, total expenses on IT, annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations were collected in millions of U.S. dollars. One-way MANOVA was used to test the significant differences in total expenses on IT on revenue, liabilities, and owner's equity account before and after a data breach incident.

The results of the One-way MANOVA showed there was not a significant difference in total expenses on IT on liabilities ($F(df, err df) = 1.047; p = 0.307$) before and after a data breach incident. There were significant differences in total expenses on IT on revenue ($F(df, err df) = 16.784; p < .001$) and owner's equity account ($F(df, err df) = 18.374; p < .001$) before and after a data breach incident. The results of the One-way MANOVA to answer RQ4 are shown in Table 34.

Table 34

One-Way MANOVA Results of Difference in Total Expenses on IT on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
TOTAL_EXPEN _IT	REVENUE	1	44,170,222,053	16.784	<.001***
	LIABIL	1	51,420,167,606	1.047	0.307
	OWN_EQUITY _ACC	1	278,393,841,668	18.374	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Phase II – RQ5

Phase II addressed RQ5: Are there any statistically significant mean differences for *operating activities* on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? To answer RQ5, operating activities, annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations were collected in millions of U.S. dollars. One-way MANOVA was used to test the significant differences in operating

activities on revenue, liabilities, and owner's equity account before and after a data breach incident.

The results of the One-way MANOVA showed there were significant differences in operating activities on revenue ($F(df, err df) = 239; p < .001$), liabilities ($F(df, err df) = 535.677; p < .001$), and owner's equity account ($F(df, err df) = 2919.414; p < .001$) before and after a data breach incident. The results of the One-way MANOVA to answer RQ5 are shown in Table 35.

Table 35

One-Way MANOVA Results of Difference in Operating Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
OPER_ACTIV	REVENUE	1	628,955,796,645	239	<.001***
	LIABIL	1	26,309,837,758,595	535.677	<.001***
	OWN_EQUITY _ACC	1	44,232,698,030,642	2919.414	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Phase II – RQ6

Phase II addressed RQ6: Are there any statistically significant mean differences for *investing activities* on annual revenue, liabilities, as well as owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? To answer RQ6, investing activities, annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations were collected in millions of U.S. dollars. One-way MANOVA was used to test the significant differences in investing

activities on revenue, liabilities, and owner's equity account before and after a data breach incident.

The results of the One-way MANOVA showed there were significant differences in investing activities on revenue ($F(df, \text{err } df) = 10.996; p = 0.001$), liabilities ($F(df, \text{err } df) = 128.986; p < .001$), and owner's equity account ($F(df, \text{err } df) = 365.381; p < .001$) before and after a data breach incident. The results of the One-way MANOVA to answer RQ6 are shown in Table 36.

Table 36

One-Way MANOVA Results of Difference in Investing Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
INVEST_ACTIV	REVENUE	1	28,936,981,917	10.996	0.001**
	LIABIL	1	6,335,141,510,483	128.986	<.001***
	OWN_EQUITY _ACC	1	5,535,976,806,221	365.381	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Phase II – RQ7

Phase II addressed RQ7: Are there any statistically significant mean differences for *financing activities* on annual revenue, liabilities, as well as owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? To answer RQ7, financing activities, annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations were collected in millions of U.S. dollars. One-way MANOVA was used to test the significant differences in financing

activities on revenue, liabilities, and owner's equity account before and after a data breach incident.

The results of the One-way MANOVA showed there were significant differences in financing activities on revenue ($F(df, \text{err } df) = 4.087; p = 0.045$), liabilities ($F(df, \text{err } df) = 327.763; p < .001$), and owner's equity account ($F(df, \text{err } df) = 27.633; p < .001$) before and after a data breach incident. The results of the One-way MANOVA to answer RQ7 are shown in Table 37.

Table 37

One-Way MANOVA Results of Difference in Financing Activities on Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
FINANC_ACTIV	REVENUE	1	10,754,112,121	4.087	0.045*
	LIABIL	1	16,098,082,656,353	327.763	<.001***
	OWN_EQUITY _ACC	1	418,676,783,130	27.633	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Phase II – RQ8

Phase II addressed RQ8: Are there any statistically significant mean differences for annual revenue, liabilities, as well as owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for: (a) the number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located? To answer RQ8, annual revenue, liabilities, owners' equity

account, total organizational assets, and size of the organization before and after data breach incidents of 100 organizations were collected. One-way ANCOVA was used to test the significant differences in annual revenue, liabilities, and owner's equity accounts before and after a data breach incident.

The results of the One-way ANCOVA showed there were significant differences in revenue ($F(df, err\ df) = 7.656; p = 0.006$), liabilities ($F(df, err\ df) = 6.257; p = 0.013$), and owner's equity account ($F(df, err\ df) = 6.257; p = 0.013$) before and after data breach incident after controlling for number of total victims from a given organizational data breach. The results of the One-way ANCOVA showed there were significant differences in revenue ($F(df, err\ df) = 246.583; p < .001$), liabilities ($F(df, err\ df) = 338.545; p < .001$), and owners' equity account ($F(df, err\ df) = 212.524; p < .001$) before and after data breach incident after controlling for total organizational assets.

The results of the One-way ANCOVA showed there were significant differences in revenue ($F(df, err\ df) = 56.641; p < .001$), liabilities ($F(df, err\ df) = 17.883; p < .001$), and owners' equity account ($F(df, err\ df) = 17.883; p < .001$) before and after data breach incident after controlling for the size of the organization. The results of the One-way ANCOVA showed there were no significant differences in revenue ($F(df, err\ df) = 0.608; p = 0.436$), liabilities ($F(df, err\ df) = 0.107; p = 0.744$), and owner's equity account ($F(df, err\ df) = 0.107; p = 0.744$) before and after data breach incident after controlling for the U.S. state where the organization is located. The results of the One-way ANCOVA to answer RQ8 are shown in Table 38.

Table 38

One-Way ANCOVA Results of Difference in Revenue, Liabilities, and Owner's Equity Account Before and After Data Breach Incident (N=100)

Source	Dependent Variable	df (df, error df)	Mean Square	F	Sig.
LOCATION_NUM	REVENUE	1	29,747,651,327	0.608	0.436
	LIABIL	1	331,512,884,015	0.107	0.744
	OWN_EQUITY_ACC	1	331,512,884,015	0.107	0.744
COMP_SIZE	REVENUE	1	2,769,241,643,846	56.641	<.001***
	LIABIL	1	55,305,860,843,074	17.883	<.001***
	OWN_EQUITY_ACC	1	55,305,860,843,074	17.883	<.001***
NUM_TOTAL_VICT	REVENUE	1	374,322,229,288	7.656	0.006**
	LIABIL	1	19,349,171,232,234	6.257	0.013*
	OWN_EQUITY_ACC	1	19,349,171,232,234	6.257	0.013*
ASSETS	REVENUE	1	12,055,782,368,554	246.583	<.001***
	LIABIL	1	1,046,973,738,184,170	338.545	<.001***
	OWN_EQUITY_ACC	1	657,245,277,146,166	212.524	<.001***

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Phase II – Mean and Standard Deviation of Organizational Indicators Before and After Data Breach Incident

The mean and standard deviation of organizational indicators were calculated before and after a data breach incident. The statistical mean of assets before the incident (132,286) is less than the statistical mean of assets after the incident (135,680). The statistical mean of the annual budget for cybersecurity before the incident (1,223) is less than the statistical

mean of the annual budget for cybersecurity after the incident (3,229). The statistical mean of total expenses on IT before the incident (8,284) is less than the statistical mean of total expenses on IT after the incident (41,594).

The statistical mean of revenue before the incident (66,496) is less than the statistical mean of revenue after the incident (427,098). The statistical mean of liabilities before the incident (402,651) is less than the statistical mean of liabilities after the incident (3,485,045). The statistical mean of the owner's equity account before the incident (-270,364) is less than the statistical mean of the owner's equity account after the incident (2,992,187).

The statistical mean of operating activities before the incident (36,666) is less than the statistical mean of operating activities after the incident (309,245). The statistical mean of investing activities before the incident (16,195) is less than the statistical mean of investing activities after the incident (98,162). The statistical mean of financing activities before the incident (20,071) is less than the statistical mean of financing activities after the incident (135,720). The mean and standard deviation of the organizational indicators before and after a data breach incident are shown in Table 39. The mean and standard deviation of the organizational indicators for each organization before and after a data breach incident are also shown in Table 40.

Table 39

Mean and Standard Deviation of Organizational Indicators Before and After Data Breach Incident (N=100)

Organizational Indicator	Before Incident		After Incident	
	Mean	Standard Deviation	Mean	Standard Deviation
ASSETS	132,286	585,038	135,680	585,813

Organizational Indicator	Before Incident		After Incident	
	Mean	Standard Deviation	Mean	Standard Deviation
ANN_BUDGET_SEC	1,223	1,333	3,230	3,428
TOTAL_EXPEN_IT	8,285	6,818	41,594	25,444
REVENUE	66,496	73,984	427,099	493,611
LIABIL	402,651	445,936	3,485,045	3,907,287
OWN_EQUITY_ACC	-270,365	-310,256	2,992,188	3,409,907
OPER_ACTIV	36,666	47,617	309,246	416,789
INVEST_ACTIV	16,195	30,964	98,163	262,211
FINANC_ACTIV	20,071	20,333	135,721	152,636

Table 40

Mean and Standard Deviation of Organizational Indicators for Each Organization Before and After Data Breach Incident (N=100)

Number	Organization Name	Year	Before Incident		After Incident	
			Mean	Standard Deviation	Mean	Standard Deviation
1	AT&T	2010	86,605	99,924	87,311	101,432
2	Colorado government	2010	9,005	11,331	9,346	11,753
3	Federal Reserve Bank of Cleveland	2010	20,976	35,845	20,825	36,441
4	Ohio State University	2010	2,141	2,521	2,454	2,901
5	Yale University	2010	6,592	9,781	7,337	11,342
6	Eisenhower Medical Center	2011	202	217	210	213
7	Memorial Hermann Health System	2011	1,454	1,422	1,590	1,368
8	Health Net	2011	2,304	3,716	2,307	3,832
9	Massachusetts Government	2011	30,540	40,923	30,066	39,989
10	Nemours Foundation	2011	640	496	620	501
11	LinkedIn	2012	390	254	543	447
12	Verizon	2012	71,680	87,646	73,620	84,822

Number	Organization Name	Year	Before Incident		After Incident	
			Mean	Standard Deviation	Mean	Standard Deviation
13	Barnes & Noble	2012	1,254	1,458	1,224	1,394
14	TD Bank, N.A.	2012	92,558	141,805	99,114	151,990
15	Emory Healthcare	2012	3,019	4,059	3,208	4,348
16	Global Payments	2012	939	1,041	1,073	1,101
17	Adobe	2013	3,192	3,330	3,300	3,353
18	LivingSocial	2013	187	221	189	218
19	Myspace	2013	17	21	24	24
20	Target	2013	21,957	25,381	20,613	24,610
21	Yahoo	2013	5,368	6,592	15,695	25,650
22	JP Morgan Chase	2014	51,777	66,066	46,137	52,934
23	NASDAQ	2014	3,617	4,310	3,408	3,910
24	Neiman Marcus	2014	1,912	2,203	2,796	3,424
25	Sony Pictures	2014	6,870	12,658	8,089	7,716
26	SuperValu	2014	1,721	1,601	1,688	2,192
27	Trump Hotels	2014	36	57	79	133
28	UPS	2014	21,627	21,020	22,354	22,111
29	Anthem Inc.	2015	22,898	28,787	24,494	32,180
30	CVS	2015	35,841	46,337	44,946	59,260
31	CareFirst databases	2015	3,054	4,486	3,567	5,224
32	Hyatt Hotels	2015	2,012	2,587	2,001	2,803
33	Landry's, Inc.	2015	604	609	587	662
34	Natural Grocers	2015	139	227	182	270
35	Premiera	2015	1,335	1,699	1,448	1,761
36	Scottrade	2015	5,869	9,054	6,379	10,160
37	Slack	2015	298	250	433	371
38	Starwood Hotel	2015	2,883	3,385	2,909	3,194
39	Twitch	2015	14,596	18,211	18,032	21,666
40	Walmart	2015	105,604	158,680	104,202	157,352
41	Wendy's	2015	1,252	1,547	1,167	1,543
42	Century Oncology	2016	467	525	414	555
43	Cox Communications	2016	6,602	8,598	6,621	8,313
44	University of California, Berkeley	2016	2,267	2,762	2,225	2,737

Number	Organization Name	Year	Before Incident		After Incident	
			Mean	Standard Deviation	Mean	Standard Deviation
45	University of Central Florida	2016	514	575	553	591
46	Friend Finder Networks	2016	180	269	169	244
47	Funimation	2016	110	119	78	73
48	Uber	2016	1,932	2,275	4,213	5,380
49	Alteryx	2017	56	40	123	79
50	Arby's	2017	1,127	1,358	1,049	1,250
51	Chipotle	2017	1,140	1,409	1,081	1,235
52	Dun & Bradstreet	2017	791	1,372	761	1,319
53	Equifax	2017	1,934	2,439	1,925	2,401
54	UNC Health Care	2017	712	722	727	778
55	Verifone	2017	854	949	804	879
56	Bethesda Game Studios	2018	114	103	128	111
57	BMO Harris Bank, N.A., U.S.	2018	161,260	298,836	175,738	326,774
58	Saks and Lord & Taylor	2018	8,511	12,402	8,425	11,705
59	US Centers for Medicare & Medicaid Services	2018	13,129	18,410	14,001	18,991
60	Earl Enterprises	2018	4,490	4,033	5,556	4,725
61	HauteLook	2018	3,909	5,065	3,927	5,123
62	Marriott International	2018	8,215	9,362	8,375	9,729
63	Orbitz	2018	5,946	6,239	5,980	6,434
64	State Farm	2018	6,824	16,914	7,162	17,749
65	Under Armour	2018	1,681	1,910	1,803	2,070
66	USPS	2018	14,559	42,672	14,707	44,271
67	Adobe Inc.	2019	7,488	6,307	8,154	7,848
68	Capital One	2019	95,109	149,837	103,271	163,179
69	DoorDash	2019	629	528	1,717	2,259
70	ElasticSearch	2019	63	57	83	59
71	Facebook	2019	35,521	35,066	34,623	48,538

Number	Organization Name	Year	Before Incident		After Incident	
			Mean	Standard Deviation	Mean	Standard Deviation
72	First American Corporation	2019	3,189	4,224	3,443	4,517
73	Microsoft	2019	80,324	89,391	89,175	96,716
74	Quest Diagnostics	2019	3,841	4,163	4,577	5,001
75	StockX	2019	632	673	564	580
76	Zynga	2019	1,177	1,148	1,795	2,052
77	United States federal government	2020	2,203,500	16,253,130	2,600,644	18,362,564
78	FireEye	2020	838	1,130	922	1,257
79	Office of Washington State Auditor (SAO)	2020	19,713	31,870	20,744	33,383
80	SolarWinds	2020	1,469	1,947	1,235	1,638
81	Verizon	2020	92,321	118,730	109,718	135,355
82	Wawa	2020	3,184	3,924	3,120	3,885
83	Accenture	2021	18,994	16,956	22,060	19,169
84	Ancestry.com	2021	507	595	494	596
85	Apple	2021	109,672	124,880	116,121	126,945
86	UScellular	2021	775	728	786	510
87	Kaseya	2021	471	805	480	817
88	LinkedIn	2021	1,839	2,425	2,069	2,578
89	Appliance Maker Whirlpool	2021	7,012	8,426	7,287	8,961
90	T-Mobile	2021	50,999	74,140	50,085	72,828
91	Amazon Web Services	2022	18,797	20,666	16,614	15,828
92	American Airlines	2022	15,057	18,486	16,783	19,229
93	North Face	2022	3,967	4,472	3,812	4,535
94	Rockstar	2022	1,062	1,230	1,251	1,359
95	Slack	2022	275	230	396	390
96	Consumer Financial Protection Bureau	2023	374	465	437	527

Number	Organization Name	Year	Before Incident		After Incident	
			Mean	Standard Deviation	Mean	Standard Deviation
97	AT&T	2023	151,860	200,356	156,492	206,786
98	Bank of America	2023	768,362	1,291,303	702,505	1,259,096
99	KFC	2023	2,701	2,918	2,624	2,960
100	PharMerica	2023	541	720	583	769

Summary

The results and data collection were presented in this chapter. Phase I utilized data from the SME survey to answer RQ1 and RQ2. Phase II included the main study which answered RQs 3 to 8. One-way MANOVA was performed on the main study data to answer RQ3 to RQ7. One-way ANCOVA was performed on the main study data to answer RQ8.

The results of Phase I indicated that the level of agreement for organizational financial indicators evaluation was 100% for the annual budget for cybersecurity, 96% for total annual expenses on IT, 92% for annual financing activities, 92% for annual revenue, 83% for annual operating activities, 83% for annual liabilities, 75% for annual investing activities, and 63% for annual owners' equity account. The result of the annual owners' equity account was only below the minimum SMEs' consensus at 70%. The results of the other financial indicators were above the minimum SMEs' consensus at 70%.

The results of Phase I also indicated that the level of agreement for the impact of data breach incidents on organizational financial indicators was 100% for annual budget for cybersecurity, 100% for total annual expenses on IT, 88% for annual operating activities, 83% for annual financing activities, 83% for annual revenue, 83% for annual liabilities, 79% for annual investing activities, and 71% for annual owners' equity account. These results were above the minimum SMEs' consensus at 70%.

Phase II found that the estimated marginal means of revenue increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal means of liabilities also increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal means of the owner's equity account increased from Group 1 (before the incident) to Group 2 (after the incident) too.

Phase II also indicated that the mean and standard deviation of organizational indicators were calculated before and after a data breach incident. The statistical mean of assets before the incident (132,286) is less than the statistical mean of assets after the incident (135,680). The statistical mean of the annual budget for cybersecurity before the incident (1,223) is less than the statistical mean of the annual budget for cybersecurity after the incident (3,229). The statistical mean of total expenses on IT before the incident (8,284) is less than the statistical mean of total expenses on IT after the incident (41,594). The statistical mean of revenue before the incident (66,496) is less than the statistical mean of revenue after the incident (427,098). The statistical mean of liabilities before the incident (402,651) is less than the statistical mean of liabilities after the incident (3,485,045). The statistical mean of the owner's equity account before the incident (-270,364) is less than the statistical mean of the owner's equity account after the incident (2,992,187). The statistical mean of operating activities before the incident (36,666) is less than the statistical mean of operating activities after the incident (309,245). The statistical mean of investing activities before the incident (16,195) is less than the statistical mean of investing activities after the incident (98,162). The statistical mean of financing activities before the incident (20,071) is less than the statistical mean of financing activities after the incident (135,720). The values were calculated in millions of U.S. dollars. Most values of significance of p in

Phase II were recorded to be less than .001, but one value of significance of p was recorded to be less than .01. A summary of the research question results is shown in Table 41.

Table 41

Summary of Research Question Results

No.	Research Question	Result
RQ1	What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms?	<ul style="list-style-type: none"> • This study had 24 SMEs. • The annual budget for cybersecurity had 24 SMEs in agreement. Total annual expenses on IT had 23 SMEs in agreement, and one SME was not in agreement. Annual financing activities had 22 SMEs in agreement, and two SMEs were not in agreement. Annual revenue had 22 SMEs in agreement, and two SMEs were not in agreement. Annual operating activities had 20 SMEs in agreement, and four SMEs were not in agreement. Annual liabilities had 20 SMEs in agreement, and four SMEs were not in agreement. Annual investing activities had 18 SMEs in agreement, and six SMEs were not in agreement. The annual owners' equity account had 15 SMEs in agreement, and nine SMEs were not in agreement. • The level of the agreement for organizational financial indicators evaluation was from 63% to 100%.
RQ2	What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms?	<ul style="list-style-type: none"> • This study had 24 SMEs. • The annual budget for cybersecurity had 24 SMEs in agreement. Total annual expenses on IT had 24 SMEs in agreement. Annual financing activities had 21 SMEs in agreement, and three SMEs were not in agreement. Annual revenue had 20 SMEs in agreement, and four SMEs were not in agreement. Annual operating activities had 20 SMEs in agreement, and four SMEs were not in agreement. Annual liabilities had 20 SMEs in agreement, and four

No.	Research Question	Result
RQ3	<p>Are there any statistically significant mean differences in <i>the annual budget for cybersecurity</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?</p>	<p>SMEs were not in agreement. Annual investing activities had 19 SMEs in agreement, and five SMEs were not in agreement. The annual owners' equity account had 17 SMEs in agreement, and seven SMEs were not in agreement.</p> <ul style="list-style-type: none"> • The level of agreement for the impact of data breach incidents on organizational financial indicators was from 71% to 100%. • There was not a significant difference in the annual budget for cybersecurity on revenue before and after a data breach incident. • There were significant differences in the annual budget for cybersecurity on liabilities and owner's equity account before and after a data breach incident.
RQ4	<p>Are there any statistically significant mean differences for <i>total annual expenses on IT</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?</p>	<ul style="list-style-type: none"> • There was not a significant difference in total expenses on IT on liabilities before and after a data breach incident. • There were significant differences in total expenses on IT on revenue and owner's equity account before and after a data breach incident.
RQ5	<p>Are there any statistically significant mean differences for <i>annual operating activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?</p>	<ul style="list-style-type: none"> • There were significant differences in operating activities on revenue, liabilities, and owner's equity account before and after a data breach incident.

No.	Research Question	Result
RQ6	Are there any statistically significant mean differences for <i>annual investing activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	<ul style="list-style-type: none"> • There were significant differences in investing activities on revenue, liabilities, and owner's equity account before and after a data breach incident.
RQ7	Are there any statistically significant mean differences for <i>annual financing activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	<ul style="list-style-type: none"> • There were significant differences in financing activities on revenue, liabilities, and owner's equity account before and after a data breach incident.
RQ8	Are there any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for: (a) the number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located?	<ul style="list-style-type: none"> • There were significant differences in revenue, liabilities, and owner's equity account before and after data breach incident after controlling for number of total victims from a given organizational data breach. • There were significant differences in revenue, liabilities, and owners' equity account before and after data breach incident after controlling for total organizational assets. • There were significant differences in revenue, liabilities, and owners' equity account before and after data breach incident after controlling for the size of the organization. • There were no significant differences in revenue, liabilities, and owner's equity account before and after data breach incident after controlling for the U.S. state where the organization is located.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

This study assessed the perceived security in technology using the SME survey as a self-assessment to assess the impact of financial indicators on organizational performance, which follows the studies related to cloud SaaS platforms (Zizic et al., 2022). The SME survey questions were answered by participants from different age groups from 30 to 67 years. Most of these participants are males. The participants have different academic degrees such as bachelor's degrees, master's degrees, and doctorate (Ph.D.) degrees. The work industries where the most participants work included education, finance, government facilities, healthcare, as well as IT and communication. The participants' years of professional experience included the range from 11 to 15 years (25%), from 16 to 20 years (17%), and over 20 years (54%). The summary of SME demographics follows the studies related to quantitative and qualitative approaches (Wen-ai et al., 2012). This study also compared the role of organizational financial performance indicators on annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms. The cases of public disclosures of data breaches in the recent years were evaluated to identify issues related to long-term financial damages caused by data breaches, which follow the studies related to sample cases of data breach incidents in cloud SaaS platforms (Dinger & Wade, 2019).

Organizations make investments in cybersecurity and another investment in training their employees. Cybersecurity investments will never be sufficient if they are not associated with the necessary organizational financial performance indicators.

Organizations need to develop IT security education and training programs to help their non-technical employees avoid data breaches because non-technical employees are not cybersecurity experts, which follow the studies related to investments in cybersecurity (Eling & Schnell, 2016; Hoppe et al., 2021; Zhang et al., 2021). Risk assessments allow organizations to evaluate their cybersecurity controls to protect against future losses that include financial losses, which follow the studies related to cloud SaaS platforms (David & Dhillon, 2019).

The main goal of this research study was to empirically compare the role of organizational financial performance indicators on annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations. The organizations operate cloud SaaS platforms, and they reported in media between 2010 and 2023 that suffered from a data breach incident. This study empirically assessed the investments in cybersecurity as well as financial performance before and after data breach incidents that impacted different organizations. The data shows that providing appropriate investment in organizations for IT security helps reduce cybersecurity issues that cause data breach incidents.

Discussion

There are several implications for providing appropriate investment in organizations for IT security, which reduces cybersecurity issues that cause data breach incidents. IT security risks and vulnerabilities may lead to financial loss. In addition, defining the organizational financial performance indicators that impact the risk of falling victim to such cybersecurity incidents may help mitigate data breaches in organizational systems.

Implications for Practice

Implications for practice indicate that IT security risks and vulnerabilities cost organizations millions of dollars a year, as well as exploiting information through data breaches, which may lead to financial loss and failure of business. Data breaches impact organizational financial performance. Organizations have non-technical employees who do not have experience in cybersecurity. Organizations need to develop IT security education and training programs such as SETA to help their employees avoid data breaches.

Implications for Research

The results of this study provided further understanding for mitigating data breaches by defining the organizational financial performance indicators that impact the risk of falling victim to such cybersecurity incidents. Future research could investigate organizations that are located outside of the U.S. too. Future research could also investigate more cases of data breaches in cloud SaaS platforms in organizations that may happen after 2023.

Limitations

This study had several limitations. In Phase I, some invalid responses were received, possibly due to the lack of experience with some organizational financial indicators, as well as the different time allocations spent by the participants answering the SME survey. Some of these time allocations were 1, 5, 10, 30, 40, and 60 minutes. However, the average time to complete the SME survey was 28 minutes and 50 seconds. The SME survey contained demographic questions that asked the SMEs if they had a good level of expertise in both cybersecurity and finance. The third section of the SME survey captured the SMEs'

demographic information to assess their level of cybersecurity and financial experience in organizations that operate cloud SaaS platforms. Some participants also did not answer questions about demographics.

In Phase II, there was a limitation for the 100 organizations in finding all their annual financial reports online for the years before and after the data breach incidents that were reported between 2010 and 2023. The annual financial reports listed the financial performance indicators that included the annual budget for cybersecurity, revenue, liabilities, owners' equity accounts, operating activities, investing activities, financing activities, as well as total expenses on IT. Most of these financial reports were obtained from the sec.gov site or the organization's website. There was a difficulty in finding the other financial reports, and different websites were used.

On the first few days of the main study data collection, interaction was low. This was mitigated by sending them individual messages again on LinkedIn. A few participants did not know exactly what they were to do despite the directions given. It also seemed that few participants did not read the directions as they asked questions that were answered in the directions. A few participants also stated that they could not answer the survey questions as they did not have any experience with the financial performance indicators. This limitation can be mitigated in future studies by providing brief descriptions for both financial and non-financial performance indicators. Future research is recommended for developing the SME survey to be more valid for SMEs, where the survey contains questions which cover all aspects of the research. Also, there was an issue where this study only had one participant from the finance sector. This issue was resolved by adding and

contacting new LinkedIn connections who are in the business field and have experience in the finance sector.

Recommendations and Future Research

A future study may include more organizations that are located inside and outside of the U.S., where the same level of censorship in the U.S. does not exist in other countries. Reporters can report data breach incidents if they get approval from the government in other countries. The future study may also include evaluating more past cases of data breaches and after 2023 in cloud SaaS platforms in organizations, which suffered from data breach incidents. Future study may assess the organizational investment in cybersecurity and financial performance by comparing different organizations with the annual budget for cybersecurity, where the U.S. Cybersecurity and Critical Infrastructure Agency recommended in 2018 that organizations should assign at least 8% of their annual budget for their cybersecurity posture, which follows the studies related to Cloud SaaS Platforms (Shihan & Radif, 2022).

Future research may provide brief descriptions for both financial and non-financial performance indicators to help the participant understand the financial and non-financial performance indicators. The SME survey can also be developed to be clear for SMEs about the definition of the organizational indicators. The future study may include SMEs who speak languages other than English in U.S. organizations. SMEs may also access cloud SaaS platforms on devices other than desktops and laptops in their organizations such as tablets as well as mobiles.

Summary

In summary, IT security risks and vulnerabilities may lead to financial loss and failure of business. The results of this study indicated that the level of agreement for organizational financial indicators evaluation in Phase I was 100% for annual budget for cybersecurity, 96% for total annual expenses on IT, 92% for annual financing activities, 92% for annual revenue, 83% for annual operating activities, 83% for annual liabilities, 75% for annual investing activities, and 63% for annual owners' equity account. The result of the annual owners' equity account was only below the minimum SMEs' consensus at 70%. The results of the other financial indicators were above the minimum SMEs' consensus at 70%.

Results from this study also indicated that the level of agreement for the impact of data breach incidents on organizational financial indicators in Phase I was 100% for annual budget for cybersecurity, 100% for total annual expenses on IT, 88% for annual operating activities, 83% for annual financing activities, 83% for annual revenue, 83% for annual liabilities, 79% for annual investing activities, and 71% for annual owners' equity account. These results were above the minimum SMEs' consensus at 70%.

This study found that the estimated marginal means of revenue in Phase II increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal means of liabilities also increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal means of the owner's equity account increased from Group 1 (before the incident) to Group 2 (after the incident) too.

This study indicated that there were significant differences in the annual budget for cybersecurity on liabilities and owner's equity account before and after a data breach incident. There were significant differences in total expenses on IT on revenue and owner's

equity account before and after a data breach incident. There were significant differences in operating activities on revenue, liabilities, and owner's equity account before and after a data breach incident. There were significant differences in investing activities on revenue, liabilities, and owner's equity account before and after a data breach incident. There were significant differences in financing activities on revenue, liabilities, and owner's equity account before and after a data breach incident.

This study also indicated that there were significant differences in revenue, liabilities, and owner's equity account before and after data breach incident after controlling for number of total victims from a given organizational data breach. There were significant differences in revenue, liabilities, and owners' equity account before and after data breach incident after controlling for total organizational assets. There were significant differences in revenue, liabilities, and owners' equity account before and after data breach incident after controlling for the size of the organization. In addition, this study found that defining the organizational financial performance indicators may help mitigate data breaches in organizational systems.

The main research question that this study addressed is: What is the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, as well as owners' equity account before and after data breach incidents of organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident? The eight specific research questions that this study addressed were:

- RQ1: What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms?
- RQ2: What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms?
- RQ3: Are there any statistically significant mean differences for *the annual budget for cybersecurity* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ4: Are there any statistically significant mean differences for *total annual expenses on IT* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ5: Are there any statistically significant mean differences for *annual operating activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?
- RQ6: Are there any statistically significant mean differences for *annual investing activities* on annual revenue, liabilities, as well as owners' equity accounts

before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ7: Are there any statistically significant mean differences for *annual financing activities* on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?

RQ8: Are there any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from data breach incidents after controlling for: (a) number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located?

Phase I answered RQ1 and RQ2 in the main study. The results of Phase I indicated that the level of the agreement for organizational financial indicators evaluation was from 63% to 100%. The results of Phase I also indicated that the level of agreement for the impact of data breach incidents on organizational financial indicators was from 71% to 100%. Phase II answered RQ3-8 in the main study. Phase II found that the estimated marginal means of revenue in Phase II increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal means of liabilities also increased from Group 1 (before the incident) to Group 2 (after the incident). The estimated marginal

means of the owner's equity account increased from Group 1 (before the incident) to Group 2 (after the incident) too. Phase II indicated that the mean and standard deviation of organizational indicators were calculated before and after a data breach incident.

This study used the SME survey as a self-assessment to assess the impact of financial indicators on organizational performance. The most participants worked in education, finance, government facilities, healthcare, and IT. The participants have had professional experience for more than 10 years. This study compared the role of organizational financial performance indicators on annual revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms. The 100 past cases for data breach incidents were reported between 2010 and 2023 in cloud SaaS platforms in different U.S. organizations.

Cybersecurity investments can be sufficient if they are associated with the organizational financial performance indicators. Defining the organizational financial performance indicators may help mitigate data breaches in organizational systems. This study empirically assessed the investments in cybersecurity as well as financial performance before and after data breach incidents that impacted different organizations, where providing appropriate investment in organizations for cybersecurity helps reduce IT security issues that include data breach incidents.

Organizations may lose millions of dollars every year due to IT security risks, vulnerabilities, and data breaches. Loss of millions of dollars may lead to financial loss and failure of business. Financial performance would be impacted in the organizations that suffered from data breach incidents. The results of this study provided further

understanding for mitigating data breaches by defining the organizational financial performance indicators.

Overall, this study used SMEs' feedback to calculate the frequency and percentage of the answers in the demographic descriptive statistics, as well as the level of agreement and its percentage for the questions about organizational indicators. Participants were able to assess the impact of financial indicators on organizational performance using the SME survey. The results of this study showed that there were no statistically significant mean differences in the annual budget for cybersecurity on revenue and total expenses on IT on liabilities before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident.

There were statistically significant mean differences in the annual budget for cybersecurity on liabilities and owner's equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. There were statistically significant mean differences in total expenses on IT on revenue and owner's equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident. There were statistically significant mean differences in operating activities, investing activities, and financing activities on revenue, liabilities, and owner's equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident.

The results of this study also showed statistically significant mean differences in revenue, liabilities, and owner's equity account before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for number of total victims from a given organizational data breach, total organizational assets, and the size of the organization. There were statistically no mean significant differences in revenue, liabilities, and owner's equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for the U.S. state where the organization is located.

Appendix A

Example of SMEs' Invitation Email

Dear Security Subject Matter Expert (SME),

I am a PhD candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My dissertation is chaired by Dr. Yair Levy. This work is part of the Levy CyLab Projects (<https://infosec.nova.edu/cylab/>). My research study seeks to empirically propose to the Subject Matter Experts (SMEs) approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms.

The goal of my research study is to empirically compare the role of organizational financial performance indicators (annual budget for cybersecurity, total annual expenses on IT, annual operating activities, annual investing activities, and annual financing activities) on annual revenue, liabilities, and owner's equity account before and after data breach incidents of 100 organizations. The organizations operate cloud SaaS platforms, and they reported in media between 2010 and 2023 that suffered from a data breach incident.

I am requesting your help to provide your feedback on the organizational financial indicators that are listed as part of their relations to assessing organizational cybersecurity posture.

By participating in this research study, you agree and understand that your responses are voluntary. All responses are anonymous and no personally identifiable information will be collected or traced back to anyone. Of course, you may stop your participation at any time.

I appreciate your assistance and contribution to this research study. If you wish to receive the findings of this study, feel free to contact me via email and I will be more than happy to provide you with the information about the academic research publication resulting from this study.

Please let me know if you would like to participate in this SME survey.

Best Regards,
Munther Ghazawneh
Doctoral Candidate in Information Systems
College of Computing and Engineering
Nova Southeastern University
mg1269@mysu.nova.edu

Appendix B

Example of SME Survey

Dear Financial and/or Cybersecurity Expert,

My name is Munther Ghazawneh. I am a Ph.D. candidate in Information Systems at the College of Engineering and Computing of Nova Southeastern University. My research study seeks to empirically propose to the Subject Matter Experts (SMEs) approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms.

I am requesting your help to provide your feedback on the organizational financial indicators that are listed as part of their relations to assessing organizational cybersecurity posture.

Below you will find three sections:

- A. Organizational Financial Indicators Evaluation
- B. Impact of Data Breach Incidents on Organizational Financial Indicators
- C. Demographics

You will be asked in sections A and B to evaluate the level of agreement from 1 = Strongly Disagree to 7 = Strongly Agree for the relevant organizational indicators as it pertains to assessing investment in cybersecurity in organizations that operate cloud SaaS platforms.

You will be asked in Section C to answer Demographics' questions about you as a subject matter expert to assess cybersecurity posture in organizations that operate cloud SaaS platforms.

A. Organizational Financial Indicators Evaluation

Please evaluate the organizational financial indicators indicated below on a scale from 1 = Strongly Disagree to 7 = Strongly Agree by providing your expert opinion on the level of agreement of financial indicators *are relevant in assessing investment in cybersecurity* in organizations that operate cloud SaaS platforms.

Scale:

- 1 = Strongly disagree
- 2 = Somewhat disagree
- 3 = Disagree
- 4 = Neither agree nor disagree
- 5 = Agree
- 6 = Somewhat agree

7 = Strongly agree

A1. Financial Indicators:

ID	Indicator	←	→
		Strongly Disagree	Strongly Agree
F01	Annual budget for cybersecurity	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F02	Total annual expenses on IT	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F03	Annual operating activities	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F04	Annual investing activities	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F05	Annual financing activities	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F06	Annual revenue	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F07	Annual liabilities	<input type="checkbox"/> 1	<input type="checkbox"/> 7
F08	Annual owners' equity account	<input type="checkbox"/> 1	<input type="checkbox"/> 7

A2. Are there any other financial performance indicators that are valid components in assessing investment in cybersecurity in organizations that operate cloud SaaS platforms?

B. Impact of Data Breach Incidents on Organizational Financial Indicators

Please indicate your expert opinion on the level of agreement, from 1 = Strongly Disagree to 7 = Strongly Agree, *about the impact of data breach incidents* on each of the organizational financial indicators noted below in organizations that operate cloud SaaS platforms.

Scale:

- 1 = Strongly disagree
- 2 = Somewhat disagree
- 3 = Disagree
- 4 = Neither agree nor disagree
- 5 = Agree
- 6 = Somewhat agree
- 7 = Strongly agree

B1. Financial Indicators:

ID	Indicator	←	→
		Strongly Disagree	Strongly Agree

FI01	Annual budget for cybersecurity	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI02	Total annual expenses on IT	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI03	Annual operating activities	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI04	Annual investing activities	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI05	Annual financing activities	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI06	Annual revenue	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI07	Annual liabilities	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7
FI08	Annual owners' equity account	<input type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input type="checkbox"/> 6	<input type="checkbox"/> 7

C. Demographics

- What is your age group?
 - 18-29
 - 30-39
 - 40-49
 - 50-59
 - 60-67
 - Above 67
- What is your gender?
 - Male
 - Female
 - Other
 - Prefer not to say
- What is your highest degree?
 - High school diploma
 - Associate degree
 - Bachelor's degree
 - Master's degree
 - Doctorate (PhD, JD, MD, etc.) degree
 - Other
- What is your current employment status?
 - Full-time employment
 - Part-time employment
 - Unemployed
 - Self-employed
 - Retired
- What is your main work industry?
 - Agriculture
 - Chemical industry

- Commercial facilities
- Communications
- Critical manufacturing
- Dams industry
- Data processing
- Defense industry
- Education
- Emergency services
- Energy industry
- Finance
- Food services
- Government facilities
- Healthcare
- IT / Communication
- Legal services
- Military
- Nuclear industry
- Transportation systems
- Water and wastewater systems

6. What is your main professional role?

- Accountant
- Auditor
- Budget Analyst
- Chief Finance Officer
- Finance Administrator
- Financial Analyst
- Finance Manager
- Financial Planner
- Investment Banker
- Loan Officer
- Portfolio Manager
- Securities Trader

7. How many years of professional experience do you have in the industry (related to IT/cybersecurity, finance, and/or accounting)?

- No experience
- Less than one year
- From 1 to 5 years
- From 6 to 10 years
- From 11 to 15 years
- From 16 to 20 years

Over 20 years

8. How many professional certifications do you have (related to IT/cybersecurity, finance, and/or accounting)?

None

One

Two

Three

Four or more

9. Which professional certifications do you possess?

IT

Cybersecurity

Finance

Accounting

Other

Appendix C

Organizational Indicators with Description

Organizational Indicator	Description
ANN_BUDGET_SEC	Annual budget for cybersecurity
ASSETS_B	Assets before data breach incident
ASSETS_A	Assets after data breach incident
LIABIL_B	Liabilities before data breach incident
LIABIL_A	Liabilities after data breach incident
OWN_EQUITY_ACC_B	Owner's equity account before data breach incident
OWN_EQUITY_ACC_A	Owner's equity account after data breach incident
REVENUE_B	Revenue before data breach incident
REVENUE_A	Revenue after data breach incident
OPER_ACTIV_B	Operating activities before data breach incident
OPER_ACTIV_A	Operating activities after data breach incident
INVEST_ACTIV_B	Investing activities before data breach incident
INVEST_ACTIV_A	Investing activities after data breach incident
FINANC_ACTIV_B	Financing activities before data breach incident
FINANC_ACTIV_A	Financing activities after data breach incident
TOTAL_EXPEN_IT_B	Total expenses on IT before data breach incident
TOTAL_EXPEN_IT_A	Total expenses on IT after data breach incident
COMP_SIZE	Company size

Appendix D

Data Collection Details

Phase	No.	Research Question	Methodology	Analysis
Phase I	RQ1	What are the SMEs' approved organizational financial indicators that are valid in assessing organizational investment in cybersecurity for those that operate cloud SaaS platforms?	Sequential Quantitative-Qualitative Survey	Using quantitative and qualitative approaches to compare organizational indicators
Phase I	RQ2	What are the SMEs' approved organizational financial indicators relevant to mitigating data breach incidents in organizations that operate cloud SaaS platforms?	Sequential Quantitative-Qualitative Survey	Using quantitative and qualitative approaches to compare organizational indicators
Phase II	RQ3	Are there any statistically significant mean differences in <i>the annual budget for cybersecurity</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	Multiple Case Study Analysis Method	One-way MANOVA

Phase	No.	Research Question	Methodology	Analysis
Phase II	RQ4	Are there any statistically significant mean differences for <i>total annual expenses on IT</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	Multiple Case Study Analysis Method	One-way MANOVA
Phase II	RQ5	Are there any statistically significant mean differences for <i>annual operating activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	Multiple Case Study Analysis Method	One-way MANOVA
Phase II	RQ6	Are there any statistically significant mean differences for <i>annual investing activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	Multiple Case Study Analysis Method	One-way MANOVA

Phase	No.	Research Question	Methodology	Analysis
Phase II	RQ7	Are there any statistically significant mean differences for <i>annual financing activities</i> on annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident?	Multiple Case Study Analysis Method	One-way MANOVA
Phase II	RQ8	Are there any statistically significant mean differences for annual revenue, liabilities, as well as owners' equity accounts before and after data breach incidents of 100 organizations that operate cloud SaaS platforms and reported in media between 2010 and 2023 that suffered from a data breach incident after controlling for: (a) the number of total victims from a given organizational data breach; (b) total organizational assets; (c) size of the organization; and (d) the U.S. state where the organization is located?	Multiple Case Study Analysis Method	One-way ANCOVA

Appendix E

Institutional Review Board (IRB) Approval Letter



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

MEMORANDUM

To: MUNTHER GHAZAWNEH
College of Engineering and Computing

From: Ling Wang, Ph.D.
College Representative, College of Engineering and Computing

Date: April 27, 2023

Subject: IRB Exempt Initial Approval Memo

TITLE: Assessing Organizational Investments in Cybersecurity and Financial Performance Before and After Data Breach Incidents of Cloud SaaS Platforms. – NSU IRB Protocol Number 2023-207

Dear Principal Investigator,

Your submission has been reviewed and Exempted by your IRB College Representative or their Alternate on **April 27, 2023**. You may proceed with your study.

NOTE: Exempt studies do not require approval stamped documents. If your study site requires stamped copies of consent forms, recruiting materials, etc., contact the IRB Office.

Level of Review: Exempt

Type of Approval: Initial Approval

Exempt Review Category: Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies.

Annual Status of Research Update: You are required to notify the IRB Office annually if your research study is still ongoing via the *Exempt Research Status Update xForm*.

Changes: Any changes in the study (e.g., procedures, consent forms, investigators, etc.) must be approved by the IRB prior to implementation using the *Amendment xForm*.



INSTITUTIONAL REVIEW BOARD
3301 College Avenue
Fort Lauderdale, Florida 33314-7796
PHONE: (954) 262-5369

Post-Approval Monitoring: The IRB Office conducts post-approval review and monitoring of all studies involving human participants under the purview of the NSU IRB. The Post-Approval Monitor may randomly select any active study for a Not-for-Cause Evaluation.

Final Report: You are required to notify the IRB Office within 30 days of the conclusion of the research that the study has ended using the *Exempt Research Status Update xForm*.

Translated Documents: No

Retain this document in your IRB correspondence file.

CC: Ling Wang, Ph.D.

Yair Levy, Ph.D.

References

- Abbas, M. A., Ajayi, S. O., Oyegoke, A. S., & Alaka, H. (2022). A cloud-based collaborative ecosystem for the automation of BIM execution plan (BEP). *Journal of Engineering, Design and Technology*. <https://doi.org/10.1108/JEDT-02-2022-0128>
- Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, 22(3), 1109. <https://doi.org/10.3390/s22031109>
- Adjekum, D. K. (2017). An evaluation of the relationships between collegiate aviation safety management system initiative, self-efficacy, transformational safety leadership and safety behavior mediated by safety motivation. *International Journal of Aviation, Aeronautics and Aerospace*, 4(2), 4.
- Adonis, R., & Ngcamu, B. S. (2016). An empirical investigation into the information management systems at a South African financial institution. *Banks and Bank Systems*, 11(3), 58-65. [https://doi.org/10.21511/bbs.11\(3\).2016.06](https://doi.org/10.21511/bbs.11(3).2016.06)
- Algarni, A. M., Thayanathan, V., & Malaiya, Y. K. (2021). Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. *Applied Sciences*, 11(8), 3678. <https://doi.org/10.3390/app11083678>
- Ahmad, W., Rasool, A., Abdul, R. J., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, 11(1), 16. <https://doi.org/10.3390/electronics11010016>
- Akinbowale, O. E., Heinz Eckart Klingelhöfer, & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: A survey of literature. *Journal of Financial Crime*, 27(3), 945-958. <https://doi.org/10.1108/JFC-03-2020-0037>
- Al-Marsy, A., Chaudhary, P., & James, A. R. (2021). A model for examining challenges and opportunities in use of cloud computing for health information systems. *Applied System Innovation*, 4(1), 1-20. <https://doi.org/10.3390/asi4010015>
- Alaoui, R. L., & El, H. N. (2022). Deep learning for vulnerability and attack detection on web applications: A systematic literature review. *Future Internet*, 14(4), 118. <https://doi.org/10.3390/fi14040118>
- Aldossary, S., & Allen, W. (2016). Data security, privacy, availability, and integrity in cloud computing: Issues and current solutions. *International Journal of Advanced Computer Science and Applications*, 7(4), 485-498. <https://doi.org/10.14569/IJACSA.2016.070464>

- Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., & Bander Ali Saleh Al-rimy. (2021). Secure cloud infrastructure: A survey on issues, current solutions, and open challenges. *Applied Sciences*, *11*(19), 9005. <https://doi.org/10.3390/app11199005>
- Aleem, A., & Ryan Spratt, C. (2013). Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime*, *20*(1), 6-24. <https://doi.org/10.1108/13590791311287337>
- Ana Paula Beck da, Silva Etges, Grenon, V., Lu, M., Ricardo, B. C., Joana Siqueira, d. S., Francisco José, K. N., & Elaine, A. F. (2018). Development of an enterprise risk inventory for healthcare. *BMC Health Services Research*, *18*. <https://doi.org/10.1186/s12913-018-3400-7>
- Anago, J. C. (2022). How do adoption choices influence public private partnership outcomes? Lessons from Spain and Portugal transport infrastructure. *International Journal of Managing Projects in Business*, *15*(3), 469-493. <https://doi.org/10.1108/IJMPB-03-2021-0077>
- Aslam, M., Muhammad Abbas, K. A., Khalid, T., Rafi, u. S., Ullah, S., Tahir, A., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting smarter about smart cities: Improving data security and privacy through compliance. *Sensors*, *22*(23), 9338. <https://doi.org/10.3390/s22239338>
- Ava Clare Marie, O. R. (2017). Evaluating the use of Toondoo for collaborative E-learning of selected pre-service teachers. *International Journal of Modern Education and Computer Science*, *09*(11), 25. <https://doi.org/10.5815/ijmeecs.2017.11.03>
- Avery, A. (2021). After the disclosure: measuring the short-term and long-term impacts of data breach disclosures on the financial performance of organizations. *Information and Computer Security*, *29*(3), 500-525. <https://doi.org/10.1108/ICS-10-2020-0161>
- Bella, G. (2020). Out to explore the cybersecurity planet. *Journal of Intellectual Capital*, *21*(2), 291-307. <https://doi.org/10.1108/JIC-05-2019-0127>
- Ben-Abdallah, E., Boukadi, K., Hammami, M., & Karray, M. H. (2020). Personalized cloud service review analysis based on modularized ontology. *Online Information Review*, *44*(5), 953-975. <https://doi.org/10.1108/OIR-06-2019-0207>
- Bennet Simon, v. S., Dreißigacker, A., & Teuteberg, F. (2022). Toward enhancing the information base on costs of cyber incidents: Implications from literature and a large-scale survey conducted in Germany. *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(2), 79-112. <https://doi.org/10.1108/OCJ-08-2021-0020>

- Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization benefits as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability*, 13(24), 13761. <https://doi.org/10.3390/su132413761>
- Bhardwaj, A., Subramanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Review of solutions for securing end user data over cloud applications. *International Journal of Advanced Computer Research*, 6(27), 222-229. <https://doi.org/10.19101/IJACR.2016.626005>
- Bian, Y., Kang, L., & Zhao, J. L. (2020). Dual decision-making with discontinuance and acceptance of information technology: The case of cloud computing. *Internet Research*, 30(5), 1521-1546. <https://doi.org/10.1108/INTR-05-2019-0187>
- Bin Khidmat, W., Wang, M., & Awan, S. (2019). The value relevance of R&D and free cash flow in an efficient investment setup: Evidence from Chinese A-listed firms. *Asian Journal of Accounting Research*, 4(1), 95-111. <https://doi.org/10.1108/AJAR-10-2018-0035>
- Bishop, A. E., Sawyer, M., Alber-Morgan, S., & Boggs, M. (2015). Effects of a graphic organizer training package on the persuasive writing of middle school students with autism. *Education and Training in Autism and Developmental Disabilities*, 50(3), 290-302.
- Biswas, B., & Mukhopadhyay, A. (2018). G-RAM framework for software risk assessment and mitigation strategies in organizations. *Journal of Enterprise Information Management*, 31(2), 276-299. <https://doi.org/10.1108/JEIM-05-2017-0069>
- Boulton, R. E. S., Libert, B. D., & Samek, S. M. (2000). A business model for the new economy. *The Journal of Business Strategy*, 21(4), 29-35. <https://doi.org/10.1108/eb040102>
- Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360-376. <https://doi.org/10.1108/MAJ-02-2018-1804>
- Brody, R. G., Chang, H. U., & Schoenberg, E. S. (2018). Malware at its worst: Death and destruction. *International Journal of Accounting & Information Management*, 26(4), 527-540. <https://doi.org/10.1108/IJAIM-04-2018-0046>
- Brumă, L. M. (2020). Data security methods in cloud computing. *Informatica Economica*, 24(1), 48-60. <https://doi.org/10.24818/issn14531305/24.1.2020.05>

- Bumblauskas, D., Nold, H., Bumblauskas, P., & Igou, A. (2017). Big data analytics: Transforming data to action. *Business Process Management Journal*, 23(3), 703-720. <https://doi.org/10.1108/BPMJ-03-2016-0056>
- Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber-attacks through the measurement of non-IT professionals' cybersecurity skills. *Information and Computer Security*, 27(1), 101-121. <https://doi.org/10.1108/ICS-11-2016-0088>
- Chang, V., Golightly, L., Modesti, P., Xu, Q. A., Le Minh, T. D., Hall, K., Boddu, S., & Kobusińska, A. (2022). A survey on intrusion detection systems for fog and cloud computing. *Future Internet*, 14(3), 89. <https://doi.org/10.3390/fi14030089>
- Cheng-yong, L., Tian-yu, D., & Ling-xing, M. (2022). The prevention of financial legal risks of B2B e-commerce supply chain. *Wireless Communications & Mobile Computing*, 2022, 1-15. <https://doi.org/10.1155/2022/6154011>
- Chia-Nan, W., Fu-Chiang, Y., Vo, N. T. M., & Van Thanh, T. N. (2022). Wireless communications for data security: Efficiency assessment of cybersecurity industry – A promising application for UAVs. *Drones*, 6(11), 363. <https://doi.org/10.3390/drones6110363>
- Chidinma, E. E., Yusuff, F. A., Adekunle Oluyemi, O. A., & Sodeinde, G. M. (2019). Security spending and foreign direct investment inflows in Nigeria: An autoregressive distribution lag model approach. *Acta Universitatis Danubius. Oeconomica*, 15(7), 164-173.
- Cho, S., Hwang, S., Shin, W., Kim, N., & In, H. P. (2021). Design of military service framework for enabling migration to military SaaS cloud environment. *Electronics*, 10(5), 572. <https://doi.org/10.3390/electronics10050572>
- Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: Insights from an exploratory analysis. *Supply Chain Management*, 24(2), 215-240. <https://doi.org/10.1108/SCM-09-2017-0289>
- Cope, J., Siewe, F., Chen, F., Maglaras, L., & Janicke, H. (2017). On data leakage from non-production systems. *Information and Computer Security*, 25(4), 454-474. <https://doi.org/10.1108/ICS-02-2017-0004>
- Coss, D. L., & Dhillon, G. (2019). Cloud privacy objectives a value-based approach. *Information and Computer Security*, 27(2), 189-220. <https://doi.org/10.1108/ICS-05-2017-0034>
- Couture, J. (2017). Reconciling operational and financial planning views in a customer-funded organization: Making customer-funding work for NC3A. *Information & Security*, 38, 63-69. <https://doi.org/10.11610/isij.3804>

- Creado, Y., & Ramteke, V. (2020). Active cyber defense strategies and techniques for banks and financial institutions. *Journal of Financial Crime*, 27(3), 771-780. <https://doi.org/10.1108/JFC-01-2020-0008>
- Dandapani, K. (2017). Electronic finance – recent developments. *Managerial Finance*, 43(5), 614-626. <https://doi.org/10.1108/MF-02-2017-0028>
- David, L. C., & Dhillon, G. (2019). Cloud privacy objectives a value-based approach. *Information and Computer Security*, 27(2), 189-220. <https://doi.org/10.1108/ICS-05-2017-0034>
- Deflorin, P., Scherrer, M., & Schillo, K. (2021). The influence of IoT on manufacturing network coordination. *Journal of Manufacturing Technology Management*, 32(6), 1144-1166. <https://doi.org/10.1108/JMTM-09-2019-0346>
- Diers-Lawson, A., Symons, A., & Zeng, C. (2021). Building crisis capacity with data breaches: The role of stakeholder relationship management and strategic communication. *Corporate Communications*, 26(4), 675-699. <https://doi.org/10.1108/CCIJ-02-2021-0024>
- Diez, F., Bussin, M., & Lee, V. (2019). Tools for HR analytics. *Fundamentals of HR Analytics*, Emerald Publishing Limited, Bingley, 37-46. <https://doi.org/10.1108/978-1-78973-961-920191002>
- Dinger, M., & Wade, J. T. (2019). The strategic problem of information security and data breaches. *The Coastal Business Journal*, 17(1), 1-25.
- Donner, H., & Steep, M. (2021). Monetizing the IoT revolution. *Sustainability*, 13(4), 2195. <https://doi.org/10.3390/su13042195>
- Dzidzah, E., Owusu Kwateng, K., & Asante, B. K. (2020). Security behavior of mobile financial service users. *Information and Computer Security*, 28(5), 719-741. <https://doi.org/10.1108/ICS-02-2020-0021>
- Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., Dee, A., Bajaj, R., V-J Jaeger, Katz, D., Meghen, P., Silley, M., Nasser-Probert, S., Pikinska, J., Rubin, R., & Ang, K. (2019). Cyber operational risk scenarios for insurance companies. *British Actuarial Journal*, 24. <https://doi.org/10.1017/S1357321718000284>
- Eitosa Jorge, L., Mosconi, E., & Santa-Eulalia, L. A. (2022). Enterprise social media platforms for coping with an accelerated digital transformation. *Journal of Systems and Information Technology*, 24(3), 221-245. <https://doi.org/10.1108/JSIT-08-2021-0154>

- Eling, M., & Schnell, W. (2016). What do we know about cyber risk and cyber risk insurance? *Journal of Risk Finance*, 17(5), 474-491. <https://doi.org/10.1108/JRF-09-2016-0122>
- Ermicioi, N., & Liu, X. M. (2021). An interdisciplinary study of cybersecurity investment in the nonprofit sector. *American Journal of Management*, 21(5), 39-50.
- Fabio, R. B., & Samara, B. S. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, 28(2), 359-374. <https://doi.org/10.1108/JFC-07-2020-0149>
- Fan, B., Ji, H., Wei, J., & Lambert, S. (2018). Development of tactical solutions for the e-credit card issuing industry. *International Journal of Accounting and Information Management*, 26(1), 115-131. <https://doi.org/10.1108/IJAIM-02-2017-0014>
- Feghali, K., Matta, J., & Moussa, S. (2022). Digital transformation of accounting practices and behavior during COVID-19: MENA evidence. *Accounting and Management Information Systems*, 21(2), 236-269. <https://doi.org/10.24818/jamis.2022.02005>
- Fehér, D. J., & Sándor, B. (2019). Cloud SaaS security issues and challenges. *Proceedings of the 2019 IEEE 13th International Symposium on Applied Computational Intelligence and Informatics*, 131-134. <https://doi.org/10.1109/SACI46893.2019.9111529>
- Frøystad, C., Tøndel, I. A., & Martin, G. J. (2018). Security incident information exchange for cloud service provisioning chains. *Cryptography*, 2(4), 41. <https://doi.org/10.3390/cryptography2040041>
- Gallagher, K. P., Jamey Worrell, J. L., & Mason, R. M. (2012). The negotiation and selection of horizontal mechanisms to support post-implementation ERP organizations. *Information Technology & People*, 25(1), 4-30. <https://doi.org/10.1108/09593841211204326>
- Ganda, F. (2019). The relationship between corporate sustainability disclosure and firm financial performance in Johannesburg Stock Exchange (JSE) Listed Mining Companies. *Sustainability*, 11(16), 4496. <https://doi.org/10.3390/su11164496>
- Gashami, J. P. G., Libaque-Saenz, C. F., & Chang, Y. (2020). Social-media-based risk communication for data co-security on the cloud. *Industrial Management & Data Systems*, 120(3), 442-463. <https://doi.org/10.1108/IMDS-03-2019-0131>
- Georgiou, D., & Lambrinoudakis, C. (2020). Compatibility of a security policy for a cloud-based healthcare system with the EU general data protection regulation (GDPR). *Information*, 11, 586. <https://doi.org/10.3390/info11120586>

- Georgiopoulou, Z., Makri, E. L., & Lambrinouidakis, C. (2020). GDPR compliance: Proposed technical and organizational measures for cloud provider. *Information and Computer Security*, 28(5), 665-680. <https://doi.org/10.1108/ICS-01-2020-0009>
- Granneman, J. (2018). The business guide to improving information security. *The Journal of Equipment Lease Financing (Online)*, 36(3), 1-9.
- Griffy-Brown, C., Lazarikos, D., & Chun, M. (2017). Cybercrime business models: Developing an approach for effective security against better organized criminals. *The Journal of Applied Business and Economics*, 19(8), 22-34.
- Gromis di Trana, M., Fiandrino, S., & Yahiaoui, D. (2022). Stakeholder engagement, flexible proactiveness and democratic durability as CSR strategic postures to overcome periods of crisis. *Management Decision*, 60(10), 2719-2742. <https://doi.org/10.1108/MD-08-2021-1012>
- Grubisic, I. (2014). ERP in clouds or still below. *Journal of Systems and Information Technology*, 16(1), 62-76. <https://doi.org/10.1108/JSIT-05-2013-0016>
- Gunawan, H., & Lina, E. O. (2015). Mandatory and voluntary disclosure of annual report on investor reaction. *International Journal of Economics and Financial Issues*, 5(1), 311-314.
- Gupta, R., Biswas, B., Biswas, I., & Sana, S. S. (2021). Firm investment decisions for information security under a fuzzy environment: A game-theoretic approach. *Information and Computer Security*, 29(1), 73-104. <https://doi.org/10.1108/ICS-02-2020-0028>
- Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: Is the industry different? *Journal of Hospitality and Tourism Technology*, 11(3), 511-527. <https://doi.org/10.1108/JHTT-11-2019-013>
- Han, L. Y., Arokiasamy, L., & Marn, J. T. K. (2019). A study on ethical customer management and organizational sustainability in pharmaceutical industry in Malaysia. *Global Business and Management Research*, 11(1), 593-606.
- Harmandeep, S. B., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, 2018, 11. <https://doi.org/10.1155/2018/1798659>
- Harris, M., & Patten, K. (2014). Mobile device security considerations for small and medium-sized enterprise business mobility. *Information Management & Computer Security*, 22(1), 97-114. <https://doi.org/10.1108/IMCS-03-2013-0019>

- Harrison, R., Parker, A., Brosas, G., Chiong, R., & Tian, X. (2015). The role of technology in the management and exploitation of internal business intelligence. *Journal of Systems and Information Technology*, 17(3), 247-262. <https://doi.org/10.1108/JSIT-04-2015-0030>
- Harun, C. A., & Raquela, R. N. (2021). Non-core deposit of Indonesian banking. *Studies in Economics and Finance*, 38(2), 207-226. <https://doi.org/10.1108/SEF-10-2018-0311>
- He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21(2), 203-213. <https://doi.org/10.1108/JIC-05-2019-0112>
- Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: Insights from industry surveys. *Journal of Risk Finance*, 22(3/4), 240-260. <https://doi.org/10.1108/JRF-02-2020-0024>
- Hua, N., Huang, A., Medeiros, M., & DeFranco, A. (2020). The moderating effect of operator type: The impact of information technology (IT) expenditures on hotels' operating performance. *International Journal of Contemporary Hospitality Management*, 32(8), 2519-2541. <https://doi.org/10.1108/IJCHM-09-2019-0753>
- Hubbs, T., & Kuethe, T. (2017). A disequilibrium evaluation of public intervention in agricultural credit markets. *Agricultural Finance Review*, 77(1), 37-49. <https://doi.org/10.1108/AFR-04-2016-0032>
- Humayun, M., Niazi, M., Almufareh, M. F., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Software-as-a-service security challenges and best practices: A multivocal literature review. *Applied Sciences*, 12(8), 3953. <https://doi.org/10.3390/app12083953>
- Ismagilova Fairuza, S., & Mirolyubova, G. S. (2012). Subjective preferences of criterion-oriented support of professional activities of managers. *Psychology in Russia*, 5, 359-368. <https://doi.org/10.11621/pir.2012.0022>
- Jamieson, K. H. (2019). How Russian hackers and trolls exploited U.S. media in 2016 1. *Proceedings of the American Philosophical Society*, 163(2), 122-135.
- Javidi, M. M., Mansouri, N., & Asadi, A. (2014). Data management challenges in cloud environments. *Computer Engineering and Applications Journal*, 3(3), 157-171.
- Jeletic, T. (2012). Cash flow and company valuation analysis: Practical approach to INA PLC, the biggest Croatian oil company. *International Journal of Arts & Sciences*, 5(7), 319-337.

- Jia, P., & Stan, C. (2021). Artificial intelligence factory, data risk, and VCs' mediation: The case of ByteDance, an AI-powered startup. *Journal of Risk and Financial Management*, 14(5), 203. <https://doi.org/10.3390/jrfm14050203>
- Jiang, Y., & Wang, N. (2022). Impact of biased technological change on high-quality economic development of China's forestry: Based on mediating effect of industrial structure upgrading. *Sustainability*, 14(16), 10348. <https://doi.org/10.3390/su141610348>
- Johnston, A. C. (2022). A closer look at organizational cybersecurity research trending topics and limitations. *Organizational Cybersecurity Journal: Practice, Process and People*, 2(2), 124-133. <https://doi.org/10.1108/OCJ-07-2022-0013>
- Joia, L. A., & Marchisotti, G. (2020). It is so! (If you think so!) – IT professionals' social representation of cloud computing. *Internet Research*, 30(3), 889-923. <https://doi.org/10.1108/INTR-10-2018-0463>
- Jouini, M., & Ben Arfa Rabai, L. (2014). Surveying and analyzing security problems in cloud computing environments. *Proceedings of the 2014 10th International Conference on Computational Intelligence and Security*, 689-693. <https://doi.org/10.1109/CIS.2014.169>
- Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting & Information Management*, 28(2), 275-301. <https://doi.org/10.1108/IJAIM-01-2019-000>
- Julia, T., Rahman, M. P., & Kassim, S. (2016). Shariah compliance of green banking policy in Bangladesh. *Humanomics*, 32(4), 390-404. <https://doi.org/10.1108/H-02-2016-0015>
- Kamariah, A. S., Aziz, N., Said, J. A., Noor, H. H., & Aziz, I. A. (2018). Data governance cloud security checklist at infrastructure as a service (IaaS). *International Journal of Advanced Computer Science and Applications*, 9(10) <https://doi.org/10.14569/IJACSA.2018.091036>
- Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information and Computer Security*, 25(3), 300-329. <https://doi.org/10.1108/ICS-02-2016-0013>
- Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, 26(2), 23-47.
- Kaur, H., & Bhardwaj, N. (2015). A review on security issues in cloud computing. *International Journal of Advanced Research in Computer Science*, 6(2). 178-182.

- Kayes, A., Kalaria, R., Sarker, I. H., Islam, M. S., Watters, P., Ng, A., Hammoudeh, M., Badsha, S., & Kumara, I. (2020). A survey of context-aware access control mechanisms for cloud and fog networks: Taxonomy and open research issues. *Sensors*, 20(9), 1-34. <https://doi.org/10.3390/s20092464>
- Khamprapai, W., Cheng-Fa, T., Wang, P., & Tsai, C. (2021). Multiple-searching genetic algorithm for whole test suites. *Electronics*, 10(16), 2011. <https://doi.org/10.3390/electronics10162011>
- Khatibian, N., Hasan gholi pour, T., & Abedi Jafari, H. (2010). Measurement of knowledge management maturity level within organizations. *Business Strategy Series*, 11(1), 54-70. <https://doi.org/10.1108/17515631011013113>
- Khayer, A., Jahan, N., Hossain, M. N., & Hossain, M. Y. (2021). The adoption of cloud computing in small and medium enterprises: A developing country perspective. *VINE Journal of Information and Knowledge Management Systems*, 51(1), 64-91. <https://doi.org/10.1108/VJIKMS-05-2019-0064>
- Khey, D. N., & Sainato, V. A. (2013). Examining the correlates and spatial distribution of organizational data breaches in the United States. *Security Journal*, 26(4), 367-382. <https://doi.org/10.1057/sj.2013.24>
- Kirkness, A. (2021). Feasibility review of a start-up full-service freelance ICT firm in NZ. *Journal of Asia Entrepreneurship and Sustainability*, 17(5), 50-92.
- Klamut, E. (2018). Internal audit tool for minimizing the risk of fraud. *E-Finanse*, 14(1), 49-68.
- Kolouch, J. (2018). Evolution of phishing and business email compromise campaigns in the Czech Republic. *Academic and Applied Research in Military and Public Management Science*, 17(3), 83-100.
- Kosseff, J. (2018). Defining cybersecurity law. *Iowa Law Review*, 103(3), 985-1031.
- Kouatli, I. (2014). A comparative study of the evolution of vulnerabilities in IT systems and its relation to the new concept of cloud computing. *Journal of Management History*, 20(4), 409-433. <https://doi.org/10.1108/JMH-02-2014-0018>
- Koul, S., & Eydgahi, A. (2018). Utilizing technology acceptance model (TAM) for driverless car technology. *Journal of Technology Management & Innovation*, 13(4), 37-46. <https://doi.org/10.4067/S0718-27242018000400037>
- Kramer, B., & van Welie, T. (2001). An asset liability management model for housing associations. *Journal of Property Investment & Finance*, 19(6), 453-471. <https://doi.org/10.1108/EUM00000000006186>

- Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., & Bizon, N. (2021). State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability*, *13*(16), 9463. <https://doi.org/10.3390/su13169463>
- Krug, A. K. (2017). Investors' paradox. *Journal of Corporation Law*, *43*(2), 245-288.
- Kude, T., Hoehle, H., & Sykes, T. A. (2017). Big data breaches and customer compensation strategies: Personality traits and social influence as antecedents of perceived compensation. *International Journal of Operations & Production Management*, *37*(1), 56-74. <https://doi.org/10.1108/IJOPM-03-2015-0156>
- Kulkarni, P., & Cauvery, N. K. (2021). Personally identifiable information (PII) detection in the unstructured large text corpus using natural language processing and unsupervised learning technique. *International Journal of Advanced Computer Science and Applications*, *12*(9), 508-517. <https://doi.org/10.14569/IJACSA.2021.0120957>
- Kumar, P. R., Wan, A. T., & Suhaili, W. S. H. (2020). Exploring data security and privacy issues in Internet of Things based on five-layer architecture. *International Journal of Communication Networks and Information Security*, *12*(1), 108-121.
- Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organizations. *Journal of Enterprise Information Management*, *34*(6), 1597-1629. <https://doi.org/10.1108/JEIM-06-2020-0240>
- Kuo-Chung, C., Yu-Kai, G., & Shih-Cheng, L. (2020). The effect of data theft on a firm's short-term and long-term market value. *Mathematics*, *8*(5), 808. <https://doi.org/10.3390/math8050808>
- Lamarca, B. I. (2020). Cybersecurity risk assessment of the university of northern Philippines using PRISM approach. *IOP Conference Series. Materials Science and Engineering*, *769*(1), 1-8. <https://doi.org/10.1088/1757-899X/769/1/012066>
- Laurinaitis, M., Štītīlis, D., & Verenius, E. (2021). Implementation of the personal data minimization principle in financial institutions: Lithuania's case. *Journal of Money Laundering Control*, *24*(4), 664-680. <https://doi.org/10.1108/JMLC-11-2020-0128>
- Lee, H., & Park, K. (2018). Advances in the corporate finance literature: A survey of recent studies on Korea. *Managerial Finance*, *44*(1), 5-25. <https://doi.org/10.1108/MF-10-2017-0390>
- Lee, I. (2022). Analysis of insider threats in the healthcare industry: A text mining approach. *Information*, *13*(9), 404. <https://doi.org/10.3390/info13090404>

- Levy, Y., & Gafni, R. (2021). Introducing the concept of cybersecurity footprint. *Information and Computer Security*, 29(5), 724-736. <https://doi.org/10.1108/ICS-04-2020-0054>
- Lu, Y., Wang, Y., & Chen, R. (2022). Design of enterprise financial information management system based on blockchain technology. *Security and Communication Networks*, 2022. <https://doi.org/10.1155/2022/2566615>
- Lucianetti, L., Battista, V., & Koufteros, X. (2019). Comprehensive performance measurement systems design and organizational effectiveness. *International Journal of Operations & Production Management*, 39(2), 326-356. <https://doi.org/10.1108/IJOPM-07-2017-0412>
- Lukashevich, N. S., & Garanin, D. A. (2016). Analytic decision support system for small business crediting. *St. Petersburg State Polytechnical University Journal. Economics*, (5) <https://doi.org/10.5862/JE.251.8>
- Maitlo, A., Ameen, N., Peikari, H. R., & Shah, M. (2019). Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organizations. *Information Technology & People*, 32(5), 1184-1214. <https://doi.org/10.1108/ITP-05-2018-0255>
- Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information and Computer Security*, 27(2), 233-272. <https://doi.org/10.1108/ICS-03-2018-0031>
- Mani, D., Kim-Kwang, R., & Mubarak, S. (2014). Information security in the South Australian real estate industry: A study of 40 real estate organizations. *Information Management & Computer Security*, 22(1), 24-41. <https://doi.org/10.1108/IMCS-10-2012-0060>
- Marcus, J. (2017). Competency-based education, put to the test: An inside look at learning and assessment at Western Governors University. *Education Next*, 17(4), 26.
- Martins, I., Romaní, G., & Atienza, M. (2021). An institutional approach to the development of business angel networks in Latin American emerging countries. *European Business Review*, 33(6), 918-941. <https://doi.org/10.1108/EBR-11-2020-0261>
- Massingham, P. R., & Massingham, R. K. (2014). Does knowledge management produce practical outcomes? *Journal of Knowledge Management*, 18(2), 221-254. <https://doi.org/10.1108/JKM-10-2013-0390>

- Mattessich, R., & Küpper, H. (2003). Accounting research in the German language area – first half of the 20th century. *Review of Accounting and Finance*, 2(3), 106-137. <https://doi.org/10.1108/eb027015>
- Max, v. H., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., Dumitru, D., Răcățăian, A., Brinkhuis, M., & Spruit, M. (2021). A shared cyber threat intelligence solution for SMEs. *Electronics*, 10(23), 2913. <https://doi.org/10.3390/electronics10232913>
- Mehedi, S., Rahman, H., & Jalaludin, D. (2020). The relationship between corporate governance, corporate characteristics, and agricultural credit supply: Evidence from Bangladesh. *International Journal of Social Economics*, 47(7), 867-885. <https://doi.org/10.1108/IJSE-02-2020-0085>
- Mertler, C. A., & Vannatta, R. A. (2016). *Advanced and multivariate statistical methods: Practical application and interpretation* (6th ed.). Pyrczak.
- Mohammed, Z. (2022). Data breach recovery areas: An exploration of organization's recovery strategies for surviving data breaches. *Organizational Cybersecurity Journal: Practice, Process and People*, 2(1), 41-59. <https://doi.org/10.1108/O CJ-05-2021-0014>
- Mohd Aizuddin, Z. A., Nawawi, A., & Ahmad Saiful Azlin, P. S. (2019). Customer data security and theft: A Malaysian organization's experience. *Information and Computer Security*, 27(1), 81-100. <https://doi.org/10.1108/ICS-04-2018-0043>
- Moorthy, S., & Polley, D. E. (2010). Technological knowledge breadth and depth: Performance impacts. *Journal of Knowledge Management*, 14(3), 359-377. <https://doi.org/10.1108/13673271011050102>
- Morawiec, P., & Sołtysik-Piorunkiewicz, A. (2022). Cloud computing, big data, and blockchain technology adoption in ERP implementation methodology. *Sustainability*, 14(7), 3714. <https://doi.org/10.3390/su14073714>
- Moudud-Ul-Huq, S., Asaduzzaman, M., & Biswas, T. (2020). Role of cloud computing in global accounting information systems. *The Bottom Line*, 33(3), 231-250. <https://doi.org/10.1108/BL-01-2020-0010>
- Muda, I., Sidauruk, S. H., Siregar, H. S., & Nurzaimah. (2018). The effect of corporate social responsibility on company's value with Common Effects Model (CEM), Fixed Effects Model (FEM) and Random Effects Model (REM) approaches (empirical evidence in Indonesia stock exchange): Access la success. *Calitatea*, 19(165), 79-90.
- Murtaza, A. S., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, 12(12), 6042. <https://doi.org/10.3390/app12126042>

- Murumba, J. W., Kwanya, T., & Maina, J. C. (2020). Effects of tacit knowledge on the performance of selected universities in Kenya. *Management Dynamics in the Knowledge Economy*, 8(2), 125-144. <https://doi.org/10.2478/mdke-2020-0009>
- Nagarajan, G., & Kumar, K. S. (2021). Comparative analysis of public cloud security-based schemes and cryptographic algorithms. *Turkish Journal of Computer and Mathematics Education*, 12(13), 2114-2127.
- Naji, A., Oumami, M. E., Bouksour, O., & Beidouri, Z. (2020). Mixed methods research toward a framework of a maintenance management model: A survey in Moroccan industries. *Journal of Quality in Maintenance Engineering*, 26(2), 260-289. <https://doi.org/10.1108/JQME-10-2018-0079>
- Nguyen, T. A., & Park, M. (2022). DoH tunneling detection system for enterprise network using deep learning technique. *Applied Sciences*, 12(5), 2416. <https://doi.org/10.3390/app12052416>
- Nie, D. and Xu, C. (2021). Non-GAAP earnings quality in firms with data breach incident. *Asian Review of Accounting*, 29(3), 383-398. <https://doi.org/10.1108/ARA-10-2020-0169>
- Nield, J., Scanlan, J., & Roehrer, E. (2020). Exploring consumer information-security awareness and preparedness of data-breach events. *Library Trends*, 68(4), 611-635. <https://doi.org/10.1353/lib.2020.0014>
- Ogu, E. C., Ojesanmi, O. A., Awodele, O., & Shade Kuyoro. (2019). A botnets circumspection: The current threat landscape, and what we know so far. *Information*, 10(11), 337. <https://doi.org/10.3390/info10110337>
- Ongaki, J. (2019). An examination of the relationship between flexible work arrangements, work-family conflict, organizational commitment, and job performance. *Management*, 23(2), 169-187. <https://doi.org/10.2478/manment-2019-0025>
- Orlando, A. (2021). Cyber risk quantification: Investigating the role of cyber value at risk. *Risks*, 9(10), 184. <https://doi.org/10.3390/risks9100184>
- Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. *Proceedings of the 2015 International Conference on Cyberspace*, 91-100. <https://doi.org/10.1109/CYBER-Abuja.2015.7360515>
- Ozkaya, H. (2018). Effect of mandatory IFRS adoption on cost of debt in Turkey. *Business and Economics Research Journal*, 9(3), 579-588. <https://doi.org/10.20409/berj.2018.124>

- Palanisamy, R., & Wu, Y. (2021). Users' attitude on perceived security of enterprise systems mobility: An empirical study. *Information and Computer Security*, 29(1), 159-186. <https://doi.org/10.1108/ICS-05-2020-0069>
- Parrino, R. J., & Romeo, P. J. (2012). JOBS Act eases securities-law regulation of smaller companies. *Journal of Investment Compliance*, 13(3), 27-35. <https://doi.org/10.1108/15285811211266083>
- Patel, A. S., & Patel, K. M. (2021). Critical review of literature on Lean Six Sigma methodology. *International Journal of Lean Six Sigma*, 12(3), 627-674. <https://doi.org/10.1108/IJLSS-04-2020-0043>
- Pathak, S., Krishnaswamy, V., & Sharma, M. (2020). Impact of IT practices and business value of IT measurement. *International Journal of Productivity and Performance Management*, 69(4), 774-793. <https://doi.org/10.1108/IJPPM-08-2018-0283>
- Patwary, A., Naha, R., Garg, S., Battula, S., Patwary, Md A., Aghasian, E., Amin, M., Mahanti, A., & Gong, M. (2021). Towards secure fog computing: A survey on trust management, privacy, authentication, threats, and access control. *Electronics*, 10, 1171. <https://doi.org/10.3390/electronics10101171>
- Perry, P. M. (2021). Establishing a cybersecurity program for my size entity. *Journal of Pension Benefits*, 29(1), 4-9.
- Peruško, T., & Šestan, V. (2020). Accounting information for improvement of cost planning in accident insurance 1. *Journal of Economic and Social Development*, 7(1), 39-48.
- Pevnick, J. M., Claver, M., Dobalian, A., Asch, S. M., Stutman, H. R., Tomines, A., & Fu, P., Jr. (2012). Provider stakeholders' perceived benefit from a Nascent Health Information Exchange: A qualitative analysis. *Journal of Medical Systems*, 36(2), 601-13. <https://doi.org/10.1007/s10916-010-9524-x>
- Pietro, C. D., Antonio Carlos Gastaud Maçada, & Grant, G. G. (2014). IT investment management and Information Technology Portfolio Management (ITPM). *Journal of Enterprise Information Management*, 27(6), 802-816. <https://doi.org/10.1108/JEIM-06-2013-0035>
- Plave, L. J., & Edson, J. W. (2018). First steps in data privacy cases: Article III standing. *Franchise Law Journal*, 37(4), 485-506.
- Poritskiy, N., Oliveira, F., & Almeida, F. (2019). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, 21(5), 510-524. <https://doi.org/10.1108/DPRG-05-2019-0039>

- Posey Garrison, C., & Ncube, M. (2011). A longitudinal analysis of data breaches. *Information Management & Computer Security*, 19(4), 216-230. <https://doi.org/10.1108/09685221111173049>
- Prasad, M. R., Naik, R. L., & Bapuji, V. (2013). Cloud computing: Research issues and implications. *International Journal of Cloud Computing and Services Science*, 2(2), 134-140. <https://doi.org/10.11591/closer.v2i2.1963>
- Price-Haywood, E., Robinson, W., Harden-Barrios, J., Burton, J., & Burstain, T. (2018). Intelligent clinical decision support to improve safe opioid management of chronic noncancer pain in primary care. *The Ochsner Journal*, 18(1), 30-35.
- Qin, Z., Hassan, A., & Adhikariparajuli, M. (2022). Direct and indirect implications of the COVID-19 pandemic on Amazon's financial situation. *Journal of Risk and Financial Management*, 15(9), 414. <https://doi.org/10.3390/jrfm15090414>
- Rahmawati, E., Abubakar, L., & Fakhriah, E. L. (2021). Re-conceptualizing the legal standing claim by Financial Services Authority (FSA): Its challenge in Indonesian capital market. *Journal of Legal, Ethical and Regulatory Issues*, 24, 1-10.
- Ramakic, A., & Bundalo, Z. (2014). Data protection in microcomputer systems and networks. *Acta Technica Corviniensis - Bulletin of Engineering*, 7(2), 137-140.
- Ramluckan, T., & van Niekerk, B. (2014). Security requirements for cloud computing in crisis management. *Journal of Information Warfare*, 13(1), 33-46.
- Raslan, I., Hegazy, M., & Eldawla, N. K. (2016). Quality control elements and auditor fraud risk assessment: An experimental study. *Journal of Accounting and Finance*, 16(2), 151-176.
- Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2021). Cost benefits of using machine learning features in NIDS for cyber security in UK Small Medium Enterprises (SME). *Future Internet*, 13(8), 186. <https://doi.org/10.3390/fi13080186>
- Renwick, S. L., & Martin, K. M. (2017). Practical architectures for deployment of searchable encryption in a cloud environment. *Cryptography*, 1(3). <https://doi.org/10.3390/cryptography1030019>
- Reed, N. J., Wilson, N., & Hayes, K. J. (2020). Identifying contextually relevant improvement measures, illustrated by a case of executive walk rounds. *International Journal of Health Care Quality Assurance*, 33(5), 345-361. <https://doi.org/10.1108/IJHCQA-08-2019-0140>

- Reilly, R. F. (2018). The asset-based approach to business valuation in family law (part III of III): The ANAV method. *American Journal of Family Law*, 31(4), 181-192.
- Rigg, T. (2018). The ethical considerations of storing client information online. *Professional Psychology: Research and Practice*, 49(5-6), 332-335. <https://doi.org/10.1037/pro0000217>
- Saj, P. (2013). Charity performance reporting: comparing board and executive roles. *Qualitative Research in Accounting & Management*, 10(3/4), 347-368. <https://doi.org/10.1108/QRAM-05-2013-0018>
- Sarti, A. J., Bourbonnais, F. F., Landriault, A., Sutherland, S., & Cardinal, P. (2015). An interhospital, interdisciplinary needs assessment to palliative care in a community critical care context. *Journal of Palliative Care*, 31(4), 234-242. <https://doi.org/10.1177/082585971503100405>
- Saxena, N., Hayes, E., Bertino, E., Ojo, P., Kim-Kwang, R., & Burnap, P. (2020). Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, 9(9), 1460. <https://doi.org/10.3390/electronics9091460>
- Schniederjans, D. G., Ozpolat, K., & Chen, Y. (2016). Humanitarian supply chain use of cloud computing. *Supply Chain Management*, 21(5), 569-588. <https://doi.org/10.1108/SCM-01-2016-0024>
- Secret, M., Leisey, M., Lanning, S., Polich, S., & Schaub, J. (2011). Faculty perceptions of the scholarship of teaching and learning: Definition, activity level and merit considerations at one university. *Journal of the Scholarship of Teaching and Learning*, 11(3), 1-20.
- Senyo, P. K., Effah, J., & Addae, E. (2016). Preliminary insight into cloud computing adoption in a developing country. *Journal of Enterprise Information Management*, 29(4), 505-524. <https://doi.org/10.1108/JEIM-09-2014-0094>
- Sezer, B. K., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, 33(4), 360-376. <https://doi.org/10.1108/MAJ-02-2018-1804>
- Shahzadi, S., Khaliq, B., Rizwan, M., & Ahmad, F. (2020). Security of cloud computing using adaptive neural fuzzy inference system. *Security and Communication Networks*, 2020, 15. <https://doi.org/10.1155/2020/5352108>
- Shammar, E. A., & Zahary, A. T. (2020). The Internet of Things (IoT): A survey of techniques, operating systems, and trends. *Library Hi Tech*, 38(1), 5-66. <https://doi.org/10.1108/LHT-12-2018-0200>

- Sharma, M., & Sehrawat, R. (2020). Quantifying SWOT analysis for cloud adoption using FAHP-DEMATEL approach: Evidence from the manufacturing sector. *Journal of Enterprise Information Management*, 33(5), 1111-1152. <https://doi.org/10.1108/JEIM-09-2019-0276>
- Shihan, K. H., & Radif, M. J. (2022). Internal and external factors to adopt a cyber security strategy in Iraqi organizations. *Webology*, 19(1), 5181-5198. <https://doi.org/10.14704/WEB/V19I1/WEB19349>
- Shrivastava, U., Hazarika, B., & Rea, A. (2021). Restoring clinical information system operations post data disaster: The role of IT investment, integration, and interoperability. *Industrial Management & Data Systems*, 121(12), 2672-2696. <https://doi.org/10.1108/IMDS-03-2021-0128>
- Simon, J. P. (2021). APIs, the glue under the hood. Looking for the “API economy”. *Digital Policy, Regulation and Governance*, 23(5), 489-508. <https://doi.org/10.1108/DPRG-10-2020-0147>
- Singh, A., & Malhotra, M. (2016). Hybrid two-tier framework for improved security in cloud environment. *Proceedings of the 3rd International Conference on Computing for Sustainable Global Development*, 955-960.
- Singh, V. K., & Dutta, M. (2014). Analyzing cryptographic algorithms for secure cloud network. *International Journal of Advanced Studies in Computers, Science and Engineering*, 3(6), 1-9.
- Sizov, A., Tretyakov, K., Boyarko, G., & Shenderova, I. (2015). Liability of the supervisor under petroleum drilling contract. *Proceedings of the IOP Conference Series. Earth and Environmental Science*, 24(1), 1-5. <https://doi.org/10.1088/1755-1315/24/1/012029>
- Skinner, C. P. (2019). Bank disclosures of cyber exposure. *Iowa Law Review*, 105(1), 239-281.
- Smit, R., Hagedoorn, J. M. J. v. Y., Versteeg, P., & Ravesteijn, P. (2021). The soft skills business demands of the chief information security officer. *Journal of International Technology and Information Management*, 30(4), 41-61.
- Solove, D. J., & Citron, D. K. (2018). Risk and anxiety: A theory of data-breach harms. *Texas Law Review*, 96(4), 737-786.
- Špaček, M. (2021). Sustainable HRM practices in corporate reporting. *Economies*, 9(2), 75. <https://doi.org/10.3390/economies9020075>

- Spasic, B., Boucart, N., & Thiran, P. (2019). Security pattern for cloud SaaS: From system and data security to privacy case study in AWS and Azure. *Computers*, 8(2), 34. <https://doi.org/10.3390/computers8020034>
- Spinello, R. A. (2021). Corporate data breaches: A moral and legal analysis. *Journal of Information Ethics*, 30(1), 12-32. <https://doi.org/10.2307/JIE.30.1.12>
- Stewart, H. (2022). The hindrance of cloud computing acceptance within the financial sectors in Germany. *Information and Computer Security*, 30(2), 206-224. <https://doi.org/10.1108/ICS-01-2021-0002>
- Stojkovic, M., & Butt, J. (2022). Industry 4.0 implementation framework for the composite manufacturing industry. *Journal of Composites Science*, 6(9), 258. <https://doi.org/10.3390/jcs6090258>
- Su, J. Y., & Jang, S. (2020). How does corporate sustainability increase financial performance for small-and medium-sized fashion companies: Roles of organizational values and business model innovation. *Sustainability*, 12(24), 10322. <https://doi.org/10.3390/su122410322>
- Su, K. D. (2018). Enhancing students' corresponding reasoning of cognitive performances by animated concept mapping in electrochemistry. *Journal of Baltic Science Education*, 17(4), 662-673.
- Sukumar, A., Jafari-Sadeghi, V., Garcia-Perez, A., & Dutta, D. K. (2020). The potential link between corporate innovations and corporate competitiveness: Evidence from IT firms in the UK. *Journal of Knowledge Management*, 24(5), 965-983. <https://doi.org/10.1108/JKM-10-2019-0590>
- Sun, M., & Lu, Y. (2022). A generalized linear mixed model for data breaches and its application in cyber insurance. *Risks*, 10(12), 224. <https://doi.org/10.3390/risks10120224>
- Syed Emad, A. A., Fong-Woon, L., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, 13(3), 1066. <https://doi.org/10.3390/su13031066>
- Tahir, R. (2018). A study on malware and malware detection techniques. *International Journal of Education and Management Engineering*, 8(2), 20. <https://doi.org/10.5815/ijeme.2018.02.03>
- Thamik, H., & Wu, J. (2022). The impact of artificial intelligence on sustainable development in electronic markets. *Sustainability*, 14(6), 3568. <https://doi.org/10.3390/su14063568>

- Teng, D. (2022). Industrial Internet of Things anti-intrusion detection system by neural network in the context of Internet of Things for privacy law security protection. *Wireless Communications & Mobile Computing (Online)*, 2022, 1-17. <https://doi.org/10.1155/2022/7182989>
- Thottoli, M. M., & Ahmed, E. R. (2022). Information technology and e-accounting: Some determinants among SMEs. *Journal of Money and Business*, 2(1), 1-15. <https://doi.org/10.1108/JMB-05-2021-0018>
- Torre, M. L., Dumay, J., & Rea, M. A. (2018). Breaching intellectual capital: Critical reflections on big data security. *Meditari Accountancy Research*, 26(3), 463-482. <https://doi.org/10.1108/MEDAR-06-2017-0154>
- Trawnih, A., Yaseen, H., Al-Adwan, A., Alsoud, R., & Jaber, O. A. (2021). Factors influencing social media adoption among SMEs during COVID-19 crisis. *Journal of Management Information and Decision Sciences*, 24(6), 1-18.
- Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573. <https://doi.org/10.3390/jcp2030029>
- Türkössy, A. (2013). The rules for the cash flow statement in the international financial reporting standard. *Analecta Technica Szegedinensia*, 7(1-2), 71-73. <https://doi.org/10.14232/analecta.2013.1-2.71-73>
- Tyler, K. M., Stevens-Morgan, R., & Brown-Wright, L. (2016). Home-school dissonance and student-teacher interaction as predictors of school attachment among urban middle level students. *RMLE Online*, 39(7), 1-22.
- Uddin, M. H., Hakim, A. M., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, 22(4), 239-309. <https://doi.org/10.1057/s41283-020-00063-2>
- Uddin, M., Khalique, A., Awais, K. J., Syed, S. U., & Hussain, S. (2021). Next-generation blockchain-enabled virtualized cloud security solutions: Review and open challenges. *Electronics*, 10(20), 2493. <https://doi.org/10.3390/electronics10202493>
- Upadhyay, A., Ayodele, J. O., Kumar, A., & Garza-Reyes, J. A. (2021). A review of challenges and opportunities of blockchain adoption for operational excellence in the UK automotive industry. *Journal of Global Operations and Strategic Sourcing*, 14(1), 7-60. <https://doi.org/10.1108/JGOSS-05-2020-0024>
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>

- Verstraete, M., & Zarsky, T. (2022). Cybersecurity spillovers. *Brigham Young University Law Review*, 47(3), 929-999.
- Vida, A. M., Arlos, P., & Casalicchio, E. (2022). Automated context-aware vulnerability risk management for patch prioritization. *Electronics*, 11(21), 3580. <https://doi.org/10.3390/electronics11213580>
- Vielberth, M., Englbrecht, L., & Pernul, G. (2021). Improving data quality for human-as-a-security-sensor. A process driven quality improvement approach for user-provided incident information. *Information and Computer Security*, 29(2), 332-349. <https://doi.org/10.1108/ICS-06-2020-0100>
- Wang, W., & Yongchareon, S. (2020). Security-as-a-service: A literature review. *International Journal of Web Information Systems*, 16(5), 493-517. <https://doi.org/10.1108/IJWIS-06-2020-0031>
- Webb, J., & Aly, O. (2020). Relationship between acceptance of Virtual Private Cloud (VPC) and Adoption of VPC: An empirical study. *IUP Journal of Information Technology*, 16(1), 19-76.
- Wei, W., Zhang, L., & Hua, N. (2019). Error management in service security breaches. *Journal of Services Marketing*, 33(7), 783-797. <https://doi.org/10.1108/JSM-04-2018-0114>
- Wen-ai, S., Lei, Y., Hu, L., & Wang, Y. (2012). Feasibility of output-only modal identification using wireless sensor network: A quantitative field experimental study. *International Journal of Distributed Sensor Networks*, 8, 1-17. <https://doi.org/10.1155/2012/560161>
- Wibowo, S., Nada, N. Q., Novita, M., & Budirahardjo, S. (2019). Exploratory research on green information technology knowledge. *Journal of Physics: Conference Series*, 1179(1). <https://doi.org/10.1088/1742-6596/1179/1/012109>
- Wirth, A. (2017). The economics of cybersecurity. *Biomedical Instrumentation & Technology*, 51(s6), 52-59. <https://doi.org/10.2345/0899-8205-51.s6.52>
- Wu, X., Zhao, W., & Ma, T. (2019). Improving the impact of green construction management on the quality of highway engineering projects. *Sustainability*, 11(7). <https://doi.org/10.3390/su11071895>
- Xie, P., Chen, Q., Qu, P., Fan, J., & Tang, Z. (2020). Research on financial platform of railway freight supply chain based on blockchain. *Smart and Resilient Transportation*, 2(2), 69-84. <https://doi.org/10.1108/SRT-09-2020-0007>

- Xing, J., & Zhang, Z. (2022). Hierarchical network security measurement and optimal proactive defense in cloud computing environments. *Security and Communication Networks*, 2022. <https://doi.org/10.1155/2022/6783223>
- Xu, C., Hsu, C., & Tawei (David) Wang. (2022). Talk too much? The impact of cybersecurity disclosures on investment decisions. *Communications of the Association for Information Systems*, 50. <https://doi.org/10.17705/1CAIS.05022>
- Xue, X., Wang, S., & Chao, H. (2015). Autonomous evolution of service system in cluster supply chain. *Kybernetes*, 44(1), 139-158. <https://doi.org/10.1108/K-01-2014-0005>
- Yadav, J., Misra, M., Rana, N. P., & Singh, K. (2022). Exploring the synergy between nano-influencers and sports community: Behavior mapping through machine learning. *Information Technology & People*, 35(7), 1829-1854. <https://doi.org/10.1108/ITP-03-2021-0219>
- Yousefli, Z., Nasiri, F., & Moselhi, O. (2017). Healthcare facilities maintenance management: A literature review. *Journal of Facilities Management*, 15(4), 352-375. <https://doi.org/10.1108/JFM-10-2016-0040>
- Yu, H., & Wang, D. (2012). Mass log data processing and mining based on Hadoop and cloud computing. *Proceedings of the 2012 7th International Conference on Computer Science & Education*, 197-202. <https://doi.org/10.1109/ICCSE.2012.6295056>
- Zhao, H., Wang, Y., & Liu, X. (2022). The assessment of smart city information security risk in China based on zGT2FSs and IAA method. *Scientific Reports (Nature Publisher Group)*, 12(1), 2045-2322. <https://doi.org/10.1038/s41598-022-07197-1>
- Zhang, Y., Zhang, J., & Zhang, C. (2021). Stock market liberalization and corporate green innovation: Evidence from China. *International Journal of Environmental Research and Public Health*, 18(7), 3412. <https://doi.org/10.3390/ijerph18073412>
- Zhang, Z.(J)., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management & Data Systems*, 121(3), 613-636. <https://doi.org/10.1108/IMDS-08-2020-0462>
- Zimba, A., & Chama, V. (2018). Cyber-attacks in cloud computing: Modelling multi-stage attacks using probability density curves. *International Journal of Computer Network and Information Security*, 11(3), 25. <https://doi.org/10.5815/ijcnis.2018.03.04>
- Zizic, M. C., Mladineo, M., Gjeldum, N., & Celent, L. (2022). From industry 4.0 towards industry 5.0: A review and analysis of paradigm shift for the people, organization, and technology. *Energies*, 15(14), 5221. <https://doi.org/10.3390/en15145221>

Zwilling, M. (2022). Trends and challenges regarding cyber risk mitigation by CISOs – A systematic literature and experts' opinion review based on text analytics. *Sustainability*, 14(3), 1311. <https://doi.org/10.3390/su14031311>