

UNIVERSITY OF BAHRAIN

College of Information Technology



Examining The Impact Of Cyber Risk Insurance On Reducing Cybersecurity Risks

A Thesis Submitted in Partial Fulfilment of the Requirements for the
degree of M.Sc. in Cyber Security

Submitted By

Ahmed Ali Hasan Ahmed

20171166

Supervised By

Dr. Zakariya Issa

(Associate Professor)

University of Bahrain

June 2022



Dissertation Deposit Form

Author Name:	Ahmed Ali Hasan Ahmed		
Email:	20171166@stu.uob.edu.bh	Contact No:	36439390
College:	Information Technology		
Department:	Computer Science		
Thesis Title:	Examining the Impact of Cyber Risk Insurance On Reducing Cybersecurity Risks		
Year:	2022		

Author's Declaration: I agree to the following conditions:

The above thesis will be available (in the University of Bahrain library and externally) and reproduced as necessary at the discretion of the University of Bahrain. It may also be digitized by the University of Bahrain and made available via the university's repository or via other parties on the Internet.

This condition shall apply to ALL copies including electronic copies.

The above thesis has been provided on the understanding that it is copyright protected material and that no quotation from this thesis may be published without proper acknowledgement.

Signature of the Author:	Ahmed Ali Hasan Ahmed	Date:	21-May-22
--------------------------	-----------------------	-------	-----------

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.



Signed: -----

Date: 21/5/2022

Ahmed Ali Hasan Ahmed (Candidate)

The Thesis defense committee considers the thesis titled:

Examining the Impact of Cyber Risk Insurance on Reducing Cybersecurity Risks

Submitted by Ahmed Ali Hasan Ahmed to the College of Information Technology is satisfactory and acceptable for the Master of Science in CyberSecurity.

The Defense Committee:

Dr. Zakaria Issa

(Supervisor)

Department of Information system
University of Bahrain

Dr. Mazen Ali

(Member)

Department of Information System
University of Bahrain

ABSTRACT

The evolution of the Digital Age introduces business organizations to the security risks and threats that the Internet and other modern technological innovations have created. Technology is advancing rapidly, where the ability of a business to control and mitigate all security risks is almost impossible. Cyberattacks are becoming more sophisticated, and organized crimes, in many cases, are fully automated by using intelligent tools to launch an attack. The big question is how business organizations will respond to such a complex and changing set of cybersecurity risks. Cybersecurity has become an essential concern as enterprise management should develop a plan to reduce the risk even when a disaster happens. This research assumed that cyber insurance could be convenient for addressing such a problem. To confirm this assumption, a measurement instrument was carefully designed to research and examine the impact of cyber risk insurance on reducing cybersecurity risks to an acceptable level. The method used for data collection was qualitative and quantitative. The quantitative part was a questionnaire survey with a closed-ended question, and the qualitative part was semi-structured interviews with high-level business managers. Both techniques were used in the analysis, and as a result, the main work of this research was editing the risk model and adding cyber insurance to it to come up with a unique model that has cyber insurance in the plan of mitigating security risks. If the data analysis shows that using the proposed model can help an organization be financially stable, it should adopt the proposed model. As the number of vulnerabilities increases due to a large number of applications and devices used, the business organization needs to ensure they will not suffer from uncertain financial losses that may prevent the ability to continue functioning, so cyber insurance can be a powerful tool to ensure the continuity of the business.

DEDICATION

To my mom, dad, sisters and the friends whom I call brothers.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisor, Dr. Zakaria Issa and the program director of the Master Program, Dr. Wael Elmedany for their great support, help, and motivation. Their guidance helped me in the time of my research and during the writing of this thesis. I would like to thank my family for their love and support, nothing would be possible without them.

Table of Contents

APPROVAL	A
DECLARATION	B
ABSTRACT	C
DEDICATION	D
ACKNOWLEDGMENTS	E
TABLE OF CONTENTS	E
LIST OF TABLES	H
LIST OF FIGURES	J
LIST OF ABBREVIATIONS	K
1 Introduction	2
1.1 Background	3
1.2 Problem Definition	4
1.3 Research Objectives	4
1.4 Research Significance	4
1.5 Research Hypotheses	5
1.6 Conclusion	6
2 Literature Review	8
2.1 Introduction	8
2.2 Related Work	9
2.2.1 Cyber Risks	13
2.2.2 Cybersecurity risks during Covid-19	20

2.2.3	Cyber Risk Insurance	37
2.3	Conclusion	59
3	Methodology	61
3.1	Overview	61
3.2	Hypotheses Developemt	62
3.3	Research Model	68
3.4	Conclusion	70
4	Results and Discussion	83
4.1	Overview	83
4.2	Discussion	93
4.3	Conclusion	93
5	Conclusion and Recommendations	95
5.1	Summary	95
5.1.1	Recommendations when using cyber insurance . . .	97
5.1.2	Contribution	97
5.1.3	Limitation	97
	References	100
	APPENDIX	
	Abstract (in Arabic)	

List of Tables

2.1	Cyber-attacks during Covid-19	31
3.1	Scale items of the survey instrument	76
3.2	Reliability Analysis	78
3.3	Instrument's Constructs Cronbach Alpha Reliability coefficients at 95% coefficient Level	78
3.4	Internal Consistency Reliability for Constructs at 95% coefficient Level and $P \leq 0.0001$	80
3.5	Table 3.5: Factor Analysis of the Instrument	81
4.1	Study sample characteristics	84
4.2	one sample t test results for management of organizations have a positive attitude towards cyber insurance	86
4.3	one sample t test results for cybersecurity risks have a negative impact on business revenue	87
4.4	one sample t test results for cyber insurance has a positive impact on the cybersecurity risks	88
4.5	one sample t test results for cyber insurance coverage has a positive impact on business revenue	89
4.6	one sample t test results for security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance	90

4.7	one sample t test results for the perceived benefits of cy-bersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance	91
4.8	one sample t test results for security awareness has a positive impact on manager's attitudes towards utilizing security insurance	92
4.9	Hypothesis Results	92

List of Figures

2.1 Impacts of cyber breaches 19

2.2 Top ten most covered losses 44

3.1 Independent Variable and Dependent Variable 68

5.1 old model proposed

LIST OF ABBREVIATIONS

APT	Advanced Persistent Threat
WFH	Working From Home
NHS	National Health Service
CEOS	Chief Executive Officers
CRISM	Cyber Risk Scoring and Mitigation
CRAM	Cyber-Risk Assessment and Mitigation

Chapter One

Introduction

1.1 Background

1.2 Problem Definition

1.3 Research Objectives

1.4 Research Significance

1.5 Research Hypotheses

1.6 Conclusion

Chapter 1

Introduction

The Internet and telecommunication systems have transformed business transactions into the digital age. Using the Internet in business organizations not only enhances customer interaction and improves customer reach but also ensures easy availability of information, as well as introduces new business opportunities. However, as the digital age streams forward, it introduces new business threats and provides a wildly opened gateway for uninvited intruders to try and act adversely and in a harmful way. This makes it crucial for business organizations to protect their business from all kinds of potential security threats and risks of coming face to face with different forms of cyber-attacks, data breaches, or invasion of customers' personal and sensitive information. The compromise of information systems or data breach can have a negative impact on a business, including the loss of customers and, ultimately, loss of money. So, businesses are taking the necessary measures to defend against security threats and minimise the security risks to an acceptable level.

Insurance has always been treated as a response strategy in general, in the form of risk transfer to cover the financial loss when the risks are taking place. Nowadays, insurance companies offer to cover the losses through a new emerging insurance type known as cybersecurity insurance. This research claims that Cyber Risk Insurance can be used to reduce cybersecurity risks. It may not be strong in the technical site, but it can ensure that the organization is financially stable. As the number of vulnerabilities increases due to the large number of applications and devices used, the business organization needs to ensure not to cripple in the future, so cyber insurance can be a very powerful tool to ensure the business's continuity. This research will examine the impact of cyber risk insurance on reducing cybersecurity risks and then propose a model that will incorporate cyber risk insurance into the information security risks assessment process.

1.1 Background

Insurance is a form of risk management which covers financial loss where there is an insurance policy agreed on by both parties. For instance, insurance plays a significant role in covering losses in other fields like car protection, and most people can benefit from it. The car owner must have car insurance to cover the losses that may happen in future. However, cyber insurance failed to take place in IT risk management despite the positive expectation due to its high price. Although there are also many reasons that led to this happening, it is still considered one of the promising solutions in the near future.

1.2 Problem Definition

This research intends to investigate why most organizations do not have cyber insurance, although the attacks have been rising and data has become more valuable than ever. It would be beneficial for the organization to include cyber insurance in their management plan, as the technical teams of every organization focus on the technical side. However, because the hazard continually exists, there is a need to make arrangements in every management plan to avoid any fiasco due to cyber-attacks.

1.3 Research Objectives

- Investigate the factors that influence IT management decisions for utilizing cyber risk insurance in the security management plan.
- Review the measures taken to reduce cyber-attacks costs, and investigate how cyber risk insurance can further reduce that cost.
- Evaluate the impact of cyber risk insurance on an organization's security risk.
- Propose an enhanced risk mitigation model by incorporating cyber risk insurance in the risk mitigation model.

1.4 Research Significance

An assessment of the cybersecurity risks is based on standards and models that were designed and implemented before the rise of cybersecurity insurance. While cybersecurity risk assessment intended to select and implement the proper security controls in an attempt to mitigate the identified cybersecurity risks, this research will try and evaluate the impact of incorporating

the cyber risk insurance on reducing cybersecurity risks, and thus enhance the traditional cybersecurity risks assessment model.

The outcome of this research could indicate a positive or negative impact (depending on the organization that will be using it. In the positive impact scenario, it will be beneficial for any organization that is faced with the security threats, which in many cases, results in the loss of a huge amount of money, may integrate cyber insurance as a concept in their cybersecurity risk assessment, and based on the assessment outcome, could reduce the cost of their security controls and loss, if and when the controls fail to protect their cyber systems and assets. They could even use it as an effective risk management plan. If a negative impact is anticipated by an organization (i.e. the cost of the cybersecurity insurance exceeds the benefits), in such case, they would choose not to spend such money, and thus end up saving (reducing) their cost. Meaning that a positive or negative impact will help organizations save cost. And that should make this study even more significant.

1.5 Research Hypotheses

After reading the literature, I concluded some areas to explore further, which will be done in this research through seven hypotheses. The literature is further discussed in a later chapter, and here is a brief of the research hypotheses:

- “Management of organizations have a positive attitude towards cyber insurance.”
- “Cybersecurity risks have a negative impact on a business revenue.”
- “Cyber insurance has a positive impact on the cybersecurity risks.”

- “Cyber insurance coverage has a positive impact on a business revenue.”
- “Security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance.”
- “The perceived benefits of cybersecurity insurance have a positive impact on managers’ attitudes towards utilizing security insurance.”
- “Security awareness has a positive impact on managers’ attitudes towards utilizing security insurance.”

1.6 Conclusion

To conclude, organizations are continually suffering from cyber-attack, and the loss of reputation and financial status will not help them grow in the market. This research purpose is to adopt cyber insurance plans to help the organization to get on the right track in order to gain customer trust and also become financially stable.

Chapter Two

Literature Review

2.1 Introduction

2.2 Related Work

2.2.1 Cyber Risks

2.2.2 Cybersecurity risks during Covid-19

2.2.3 Cyber Risk Insurance

2.3 Conclusion

Chapter 2

Literature Review

2.1 Introduction

With the rise and development of technology, there have been several forms of sophistication, or perhaps what we can coin under the word advantages and disadvantages. Before the advent of technology, we could not imagine a cyber-world filled with cybercrimes, cyber-attacks, the need for cybersecurity, and many others. Nevertheless, it is apprehended that all these are necessary to adapt to the severe changes in the world, especially in terms of cyber technology and the Information Technology (IT) community.(Stine & Barrett, 2021) manifest that cybercrime has arisen significantly and that many attackers use it for economic frauds and other fraudulent purposes to seek what they want. According to the author, one instance of the rise of cybercrime is its increase in Canada by 160, which was described as ‘skyrocketing’ the previously recorded number and the former rates of cybercrimes. This shows us, as readers, that the concept of cybercrimes is a

simple understanding of what the world is currently facing from hackers, for example. It also leads readers to examine the application of Cyber Risk Insurance in reducing Cybersecurity risks.(Priyadarshini & Cotton, 2022)

However, there needs to be a complete examination and understanding of what the authors say about cybersecurity and cyber risks definitions. That is for the sake of knowing the two concepts and understanding their critical roles in the cyber world. In simpler terms, defining cybersecurity and cyber risks would pave the way to understanding the impact of cyber risk insurance on reducing the risks of cybersecurity.

2.2 Related Work

Before discussing the concept of cyber risk and the impacts of cyber risk insurance, it needs to be taken into account that the term cyber is applied to the notion of computers and digital ideas and themes. This makes it specific that there is a particular understanding of cybersecurity and cyber risks meanings. In elaboration, it can be put into effect that the term ‘cyber security’ demonstrates the practice of defending matters related to computers and other digital gadgets, such as servers, networks, electronic systems, and many more.

Without cyber security, it would be difficult for organizations and companies to protect their servers and electronic systems, primarily due to the presence of cybersecurity risks, which may unsettle and lead the information systems programs to failure. So, it is necessary nowadays for organizations and companies to not only work with laptops and other technological gadgets, but instead, people are required to have a backup plan for the event of a data breach or loss of information, especially while bearing in mind that there

are currently several and numerous ways hackers and cyber-attackers follow to harm organizations.

To better understand that, the author explored different papers from which two stood out regarding providing a solid understanding of the concepts of ‘cyber’ and ‘cybersecurity’, (Rajaram, Goh, & Zhou, 2022) (Rajaram et al., 2022) claim that the concepts ‘cyber’ and ‘cybersecurity’ are all associated with the same perspective related to computers and networks, and it is the method by which companies and nations can protect their most important information and products for the prevention of the cybersecurity risks. Therefore, it is indigenous to these points mentioned above that cybersecurity is substantial in the digital world and in the attempt to maintain the same roles and goals of the networks and servers. This also leads us to know that the cyber world has some general and major risks that need to be addressed efficiently to avoid stumbling into some insecurities regarding the cyber world. These authors did not only define the concepts, but also stated that cybersecurity has evolved significantly in the past years, and there have been various forms of change in the cyber field. So, organizations and institutions need to seek empowerment for their cybersecurity software and programs.

Nevertheless, there are some common categories related to the context of cyber and cybersecurity. These numerous categories are Network Security, Application Security, and several others. With that being said, it is lucid that the cyber world is filled with differential types that collaborate altogether to enhance the well-apprehension of the term ‘cyber’, and everything falls beneath it. (Rajaram et al., 2022)

Every dimension, even the cyber world, has some risks and dangers that may lead to other uncommon and rare risks. In the cyber world, these risks

are represented in cyberattacks, cybercrimes, cyber risks, and cybersecurity risks. Therefore, there needs to be some application to deficit these risks and manage them accordingly and without any complexities whatsoever. Perhaps there are some tools and frameworks – those that will be discussed later throughout this paper - along with other applications as well, that would be helpful to assure the well-apprehension of the cyber world to diminish and lessen its insecurities and dangers.

The work presented in the previous papers paves the way to comprehend better cybersecurity and how companies and institutions can secure their information and data from the dangers and risks of hackers and those who commit cybercrimes.

Interestingly, cybersecurity is defined in a pretty contrastive manner by another author, in which that author states that cybersecurity is the method of protecting servers, networks, devices, data, and all other matters related to the cyber world (cisa.gov). Cybersecurity is also the way that several information systems tend to apply and abide by to prevent unauthorized access within information systems.

This contributes to the awareness that cybersecurity is one of the most vigorous types of security in general, and that is due to the protection of data and servers through the prevention of hackers entering and breaching computer systems. Furthermore, what makes cybersecurity even more important is peoples' need for a digital world today, especially with the emergence of the latest pandemic, Covid-19. Schools, universities, and many other institutions, whether academic or not, have shifted to being digitalized rather than following the old traditional basis. People now study, shop, work, and do many other things online using only their computers. This

makes us perceive that today's world relies on computers, which are more likely to encounter one form of cybersecurity than they were exposed to earlier.(cisa.gov)

These are the significant reasons cybersecurity is essential today, especially for reducing cybersecurity risks in a currently considered digital world.

Moreover, there are even some risks and dangers to having a poor cybersecurity system, such as malware, as it can erase the whole information system, meaning that the organization or the user will lose the entire system only due to not having an exemplary cybersecurity system. A poor cybersecurity system can also result in the alteration of files within one system, or even that the attacker would use the files and the data in one computer to breach data and information on other computers. The attacker may also steal crucial personal information related to the computer, such as someone's credit card information, to make some unauthorized purchases without letting the person know about it.

Coherently, it is demanded – at least at some point during this digital era – that businesses look for fruitful and rewarding procedures and ways to stop cyberattacks. Unless this is done, cybercrimes will continue in our world today. As that, cyber-attackers would continue their attempts to take over information and data, especially with undeveloped information systems in companies. The situation may worsen by letting cybercrimes and cyberattacks reach many more in a world that is currently quite sophisticated to be partially digitalized.

So, at the end of this section, people, and organizations need to understand the complexities existing in our world today, bearing in mind the diverse

cybersecurity and cyber risks that may jeopardize almost every business today. Institutions and firms are further required to put into effect some of the suggested ways to help reduce cybercrimes significantly. For instance, (Lallie et al., 2021) suggest cyber risk insurance, which will be conveyed and discussed in a specific manner in this paper.

2.2.1 Cyber Risks

When we want to talk about cyber risk, we can figure out that it is the term that applies to information systems. The term ‘cyber risk’ is relevant to the risks of financial loss, damage to an organization, and the unauthorized usage of the information systems that the cyber risk deals with (Gralla, 2002). It is to be noted that cyber risk is related to any risk or damage within an information system, which means that cyber risk is a crucial matter under the irrelevant and unauthorized use of data and information regarding information systems.

Cyber risk can also be referred to as that sort of risk connected to the cyber world (Gralla, 2002). Signifying phrases with the word ‘cyber’ can only be valid if they are related to the digitalized world. Cyber cannot be connected to the traditional way of living, so the term ‘cyber risk’ in this precise context, is associated with the risks of the digitalized world rather than the traditional perspective of living.

Using the literature on cyber risks, we can comprehend and understand how the cyber world can be seen as fatal to companies of different ranks and statuses. Many factors related to cyber risks lead businesses and organizations to become exposed to cybercrimes and cyberattacks. This matter can shift those businesses – from being successful and innovative – to be led to their

failures and dilemmas.

Additionally, (securityscorecard.com) discusses and elaborates on the aspect of cybersecurity risks, presenting that they are essential to any organization working in the Information Technology (IT) field. What is stated in the paper is that the data and essential information loss, further as cyber-attacks on the information systems, are all some sorts of consequences of the term that is coined under cybersecurity risks.

This means that companies lose their reputation and other crucial aspects of their institutions because of the cybersecurity risks, which resemble the formerly mentioned cyber-attacks and cybercrimes. Furtherly, one example of how cybersecurity risks are harmful to any particular organization is evident in how the company may be exposed to a network breach and data loss. All these matters and perspectives can be fatal to the fundamental put and organization in almost all companies working with technology.

Not only are we involved with reputation loss and monetary loss, but one problematic effect of cybersecurity risks is that organizations may witness some sort of vulnerability in terms of their systems. Cyber-attackers, or those who commit cybercrimes, may breach data and crucial pieces of information through some sort of error dysfunction within the system of that particular organization.

This is also a glimpse of how the cyber world is dangerous for businesses and organizations that own their functional assets. It is noticed through this that the need for systems development, tools, and frameworks adoption are all required to guarantee the sophistication and improvement of one institution.

This proves to readers and researchers that the advent and emergence of

cybercrimes and cyber risks in the stable process of companies require a particular platform or a tool to diminish and reduce the many risks of cybersecurity. With this in mind, and amidst all these changes and differentiation in this current digital world, we can examine whether the tool of cyber risk insurance is capable of lessening the cybersecurity risks discussed above or not.

That is why institutions and firms that aim to be prosperous in their professions are demanded to look for various ways to reduce cybersecurity risks. It can also be viewed that the remaining parts of the research talk about cyber risks and cyber risk insurance. This is due to wanting to know further about the cyber risk insurance policies and companies and how they may benefit companies through reducing such risks related to cybersecurity.

These are the simple reasons why cyber risks and the already discussed cyber security are problematic for companies who work with technology and information systems. According to what has been discussed previously, the variety of cyber risks emphasizes that organizations are demanded to navigate and look for ways, methods, and frameworks to diminish those risks. By doing so, institutions would be able to overcome a difficult phase in running an organization: to successfully stumble upon risks such as those related to cyber and come up at the end with the most negligible harms and damages possible.

All these points discussed until this part of the literature review demonstrate why managements and companies need tools and frameworks like cyber risk insurance. Such a framework is designated and created for the sake of helping businesses minimize the cyber risks, which are regarded as challenging in the information technology field.

This section mainly presents works of authors relevant to the topic of cyber risks in order to know and comprehend this particular term further to understand it completely.

According to (Gralla, 2002) there are two types of cyber risks: external and internal. Starting with the external risk, it is the risk that, like many others, takes its name from being external. The risk comes from outside the organization, meaning that it is not related to the inside of the firm or industry. This shows us the different outcomes, or perhaps the diverse forms of cyber risks.

Some instances of external cyber risk are phishing, cyberattacks, and any other attack that comes from the outside world, meaning any threat that does not come from the inside of the organization (Gralla, 2002). One illustration of an external cyber-attack is when an individual tends to become a threat to an organization by trying to commit fraudulent behaviors and acts for the sake of entering into the system. Therefore, we understand that there is a clear and valid difference between external and internal cyber risks, mainly because the external cyber risk results from a hacker or a cyber-attacker who intends to take over some data or control a system (Gralla, 2002).

As for the internal cyber risks, it was found in the priory mentioned website that, depending on what Forrester said, 46

Moreover, in the same paper, it was found in the conducted studies that at least half of the internal cyber risks resulted from abuse or the intent of conducting malicious behaviors. From this point, we can see that abuses, frauds and corruption are far more dominant in the internal cyber risks than in external cyber risks. According to (Gralla, 2002), cyber risks are defined as the loss of information and data of one specific organization. The paper

discusses that the concept of cyber-attacks is equivalent to data breaches, and this is due to the known aspect that the phase of cyberattacks involves wanting to harm the information system. This is through the stage of attacking one computer system to gain those pieces of information and data due to them being of high importance for the attacker. Today, cyber-attacks introduced a new form of the many insecurities we can find worldwide. In other words, people now cannot only harm other people through the traditional forms; instead, things can today be done through the internet, thus damaging and harming the intended information system. That is why cyber risks, as already mentioned by the website, are a vital matter needed to be looked upon to mitigate its risks and permit people to live without any cyber issues resulting from hackers or cyber attackers.

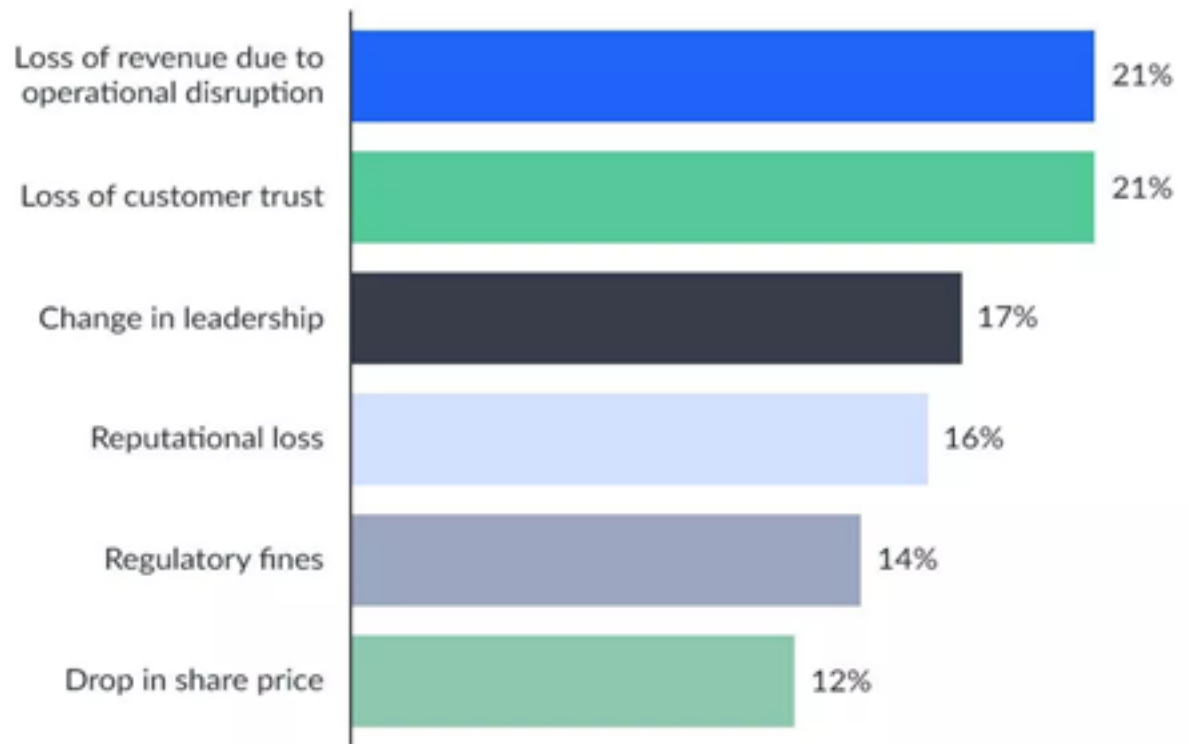
The paper also presents that the concept of cyber risk has some other potential issues, as noted within its term. These issues, or risks perhaps, are related to the harm to the organization's reputation, loss of productivity, and data damage. To further discuss, when we talk about cyber risks, we do not only consider the loss of information or the harm to information systems, but we shed light on the extent to which the organization's reputation would be harmed and affected. Following a cyber-attack, the author claims that organizations and companies would suffer from data breaches, money loss, resources, and information, as well as harm to the reputation of those organizations (Gralla, 2002).

Therefore, as per the author's words, the risks of cyber-attacks are plentiful and severe to the stability of general companies. These are why there needs to be a drastic change and some solutions in the cybersecurity and cyber risks field.

When discussing the impacts of cyber risk, it comes to our understanding through reading that they are many, from the impact of the loss of assets and finances to the loss of information and customers' trust. This indicates the severe effects of cyber risks, or what we can even term cybersecurity risks.

Extracted from the formerly cited website itself, figure 1 below shows the effects of cyber incidents or breaches on the stability of companies. It can be noticed that the loss of revenue has the most significant impact on organizations, resulting in a 21% impact, as well as that the loss of customer trust is also equivalent to the loss of revenue in percentage. Figure 1 posits that the factor of changing leadership also has an impact on companies, equaling a 17% impact. All these impacts demonstrate how negatively practical cyber risks or breaches are to companies and organizations. Cyber breaches on organizations lead to many adverse effects, as already stated, such as the loss of reputation that is regarded to be very effective in terms of one company's status and futuristic goals.

Biggest Impacts of Cyber Incidents or Breaches on Organizations



Data sourced from Deloitte's 2019 Future of Cyber Survey

Figure 2.1: Impacts of cyber breaches
(Deloitte, 2019)

This means that without cyber breaches, it is already understood that there would not be such risks, as noted in the figure. This presents and demonstrates the various negativities of cyber breaches on different and diverse organizations.

Figure 1 shows, with percentages, how effective cybersecurity and cyber risks are. We can note that organizations are significantly affected by cyber threats, cybercrimes and cybersecurity risks, as observed in the figure. This

is because organizations and institutions, through cybercrimes, lose the revenue they were expected to gain and their reputation because of the hacking usually occurring by those who want to conduct theft operations (Camillo, 2017).

As well as that, there is a notable drop in share price in the case of cybercrimes, further as the most important thing is the loss of customer trust. Shedding more light on this enables us to realize that, following one particular cybercrime, organizations lose their trust and the former loyal relationships with their customers. This may be the most negatively influential and role-changing factor in many and multiple organizations.

Hence, we understand that unless a new proper and designated framework is applied and adopted to save businesses and organizations, those institutions will eventually collapse and reach their very end (Camillo, 2017). This leads us to think of many ways to implement cyber risk insurance as precisely as possible.

2.2.2 Cybersecurity risks during Covid-19

During literature exploration, the author found multiple papers upscaling the discussion regarding cybersecurity and linking it to our present and current world events, including the Covid-19 pandemic. This only proves the complexity of cybersecurity and how integrated it is within our society and daily life. The pandemic has affected people in countless and various ways that we cannot mention in this paper; however, two papers stood out and are worth mentioning. “Cybersecurity Risks in a Pandemic” by (Williams, Chaturvedi, & Chakravarthy, 2020) and “cybersecurity in the age of Covid19” by (Lallie et al., 2021). These researches illustrate that, since

the Covid-19 pandemic, cyber-attacks and cybercrimes have increased significantly and that the pandemic, through its digitalization, changed many people's lives, especially in relation to cyber. However, this change was not said to be positive. According to the authors, the change was negative because of how multiple cybercrimes and cyber-attacks happened during the pandemic.

Not only this, but the authors also point out that the pandemic led cyber attackers even to target businesses and wanted, somehow indirectly, to affect society by focusing on the disruption of those businesses (Lallie et al., 2021).

Relevantly, many risks were acknowledged during the pandemic that affected the whole world, not only in terms of life or work but also in the sense that those cyber-attacks harmed many organizations. Nevertheless, During the pandemic, there have been numerous cyber-attacks, particularly attacks that targeted the stability of health care providers and health organizations. According to (Williams et al., 2020), there have been many cyber attackers, such as patients' data, their information, and credit card information, if applicable. This somewhat means that there are various vulnerabilities in the health sector nowadays, especially with the outbreak of Covid-19 and what it has to offer cyber attackers.

Also, as mentioned by the authors, 90% of health care providers encountered some sort of data breach. This leads us to understand and be aware of the fact that, since we have been living in a pandemic for almost two years now, there is an excellent chance of encountering problems related to server or internet breaches. It is because of the idea that cybercrimes and cyber-attacks have increased recently with the recent pandemic outbreak, especially with the shifting of the world from a conventional to a fully digi-

tal world.

Moreover, political, academic, financial, and many other sectors have been shaken due to the fatality of the pandemic that presented all over the globe. For example, financially, approximately six trillion US Dollars is estimated to be the overall monetary loss endured by the world due to the countless cyber-attacks during the pandemic by the year 2021 (Williams et al., 2020). It is even worth saying that the cyber field, which is considered even more critical than the priority stated sectors, has been most affected by the easiness with how servers and networks are currently being breached.

Proceeding, people may know how cybercriminals work during a typical day; however, it is yet unknown how cybercrimes occur and are being conducted during a pandemic. Being uncertain about this matter, according to the authors makes it even more difficult to combat and overcome the risks and the insecurities resulting from cyber attacks and cybercrimes (Williams et al., 2020) (Lallie et al., 2021).

Interestingly, according to (Jalali, Landman, & Gordon, 2020)), even regular people outside their occupation got affected by cyber attacks during the pandemic. To further elaborate, there are plenty of ways hackers and attackers can utilize the pandemic issue for their own and overall benefits. For instance, according to the authors, the pandemic has forced people to undergo a drastic change in shopping and many other matters. Since numerous groups of individuals are currently shopping online, it is easier and more accessible for hackers and other attackers to commit fraudulent acts and behaviors to benefit themselves.

One of these many ways is that hackers steal the data and information of

one individual attempting to do shopping online, and that is through introducing a new application or platform that gathers those individuals' data and personal information. This way, it would be easier for cybercrimes and cyber-attacks to be conducted than when the world is based in a traditional manner instead of fully digitalized.

Moreover, (Okereafor, 2021) discusses many threats resulting from the fragility of information systems during the pandemic. This may be because organizations and businesses emphasize ways to empower their businesses and return to their routine and ordinary lives rather than focusing on those information systems that would have helped them with significant issues like cybercrimes. That is, Covid-19 may have shifted the attention of some influential organizations from the cyber world to focus on returning the business to its regular rates of wins and losses. This is how Covid-19 impacted the cyber world, according to cyber-attackers, in a positive way by giving them millions of reasons and tools to attack information systems.

Nevertheless, a pandemic is still harmful to almost all communities and organizations. People in the cyber world endured so much from hacking and cybercrimes, so there needs to be a solution to what is currently happening. It can be stated that companies and organizations are facing some vulnerabilities and risks through the pandemic.

According to (Okereafor, 2021), a group of cyber criminals and others following the Advanced Persistent Threat (APT) attacked and targeted some fragile people, institutions, and organizations. Thus, people working in the cyber world have been negatively impacted by what we know regarding the multiple cybercrimes and cyber-attacks that pursued systems.

“The growth in anxiety and fear due to the pandemic is increasing the success rate of cyber-attacks,” the author stated. This is another reason cybersecurity risks during the Covid-19 pandemic are critical to employees and organizations. It further demonstrates how cybersecurity risks are increasing amidst the Covid-19 pandemic, according to what the author reveals (Okereafor, 2021).

Moreover, (Okereafor, 2021) states that as working from home (WFH) was introduced since the outbreak of Covid-19 as a way of preventing contact, information systems are more likely to be breached than when information systems of companies are being used. Using laptops or computers from home results in the easiness of hacking, as this fraudulent activity becomes more accessible when done on local computers than when done on computers or servers based in organizations.

This new act of working from home emphasizes increased cybercrimes and cyber-attacks. That is because hackers find a clear and valid path to put cyber risks like phishing and ransomware into information systems (Okereafor, 2021).

This is also regarding how hacking local computers and devices are more accessible than hacking and breaching into work servers. This also posits that, following the point mentioned earlier, cyber risks like ransomware and phishing are more accessible in local systems than in systems designated for work.

The same website emphasizes that the work from home (WFH) model, as practiced in a usual way today, is a model that substantially increases cyber-attacks and threats. Similarly, the rates of cyber-attacks and cybercrimes

increase due to the current normality of working from home.

One purpose for this is that employees use their organizations' devices rather than their personal devices and servers. Therefore, (Okereafor, 2021) recommends that employees and workers use their devices and computers when working from home during this fatal pandemic that has disrupted companies' effectiveness since the very beginning of the pandemic. That is the primary reason why working from home requires employees to use their devices to prevent the process of hacking computers related to work and not contribute to the breaching of data correlated to the company.

According to , (Okereafor, 2021)), on an average day, scams and phishing are considered to be two of the most common cyber-attacks in the cyber world. According to the author, there are even some sorts of phishing and scams that could lead organizations to distortion.

It is also presented by (Okereafor, 2021) that there are different types and examples of phishing attacks, which attackers utilize to produce as many maximum risks on information systems as possible. Some phishing instances are through email, text messaging, or even voice calls. These ought to substantially affect businesses, especially in the current Covid-19 situation that is generally affecting the world.

As per the paper, phishing acts, as mentioned, are one of the acts of hacking, which increased significantly in the past year: 2020. In relevance to (Okereafor, 2021), the first quarter of 2020 noted 600% more phishing acts than in 2019, for example. It is already commonly known that the Covid-19 pandemic started in the first quarter of 2020 in some countries, meaning that

the act of phishing through emails came in collaboration with the outbreak of the pandemic.

Based on (Okereafor, 2021), cybercrimes and cyber-attacks have significantly targeted health sectors and health organizations since the pandemic's beginning. Some health companies hacked earlier include research organizations, pharmaceutical institutions, and many others. That said, it is put into effect that the situation and the problem in healthcare organizations is more problematic than in the other sectors or fields.

Not considering the attacks on healthcare organizations during the pandemic, it is taken into account, generally, that hackers tend to target health-related firms. One reason for this is how healthcare organizations, according to (Okereafor, 2021), are regarded to be vulnerable to cyber-attacks and cybercrimes because they do not emphasize the development of their information systems. What the website demonstrates is that, financially, health services are typically not provided with enough amounts of money to improve their systems, specifically those associated with software and the methods that are considered to be efficient in the phase of combating the hackers and deficit their cybercrimes.

An instance of the risks and threats healthcare providers tend to endure in the phase of the conflict with cyber attackers is seen in the WannaCry ransomware. According to (Okereafor, 2021), this particular attack happened in 2017 and was located in the National Health Service (NHS). Following that precise cybercrime, the systems in the National Health Service were all incapacitated and thus could not function accordingly. This shows us that there is an issue with the health service organizations, specifically that they cannot endure the risks of cybersecurity unless they improve their systems

and find another tool or framework to minimize such threats.

The paragraph mentioned above also lets us reckon on the importance of having a well-developed and sophisticated information system that could help combat and endure the risks of the cybercrimes, such as those that consist of the dysfunction of systems.

Relatively, those systems are regarded to be very important to the health-care providers, as they may include important information related to the organizations themselves and the patients.

This indicates that cybersecurity risks have increased during the pandemic outbreak and that systems have been more exposed to cybercrimes and cyber-attacks than on a typical day without the pandemic.

Summarizing (Okereafor, 2021) work, it ought to say that organizations must have a look and an overview at these crucial matters to not have their businesses minimized. One solution to this dilemma is that businesses install some protective software and firewalls to prevent individuals and hackers from breaching the data related to one specific organization.

This is in accordance with what is mentioned in the research paper by (Ahmad, 2020) . As per what was stated in (Okereafor, 2021), the Covid-19 pandemic negatively affects companies and institutions looking forward to moving with their businesses to further sophisticated and improved levels. That is because, as previously elaborated, the employees of various businesses tend to get affected by working from home simply due to exposure to different cybersecurity risks when following the perspective of working from home.

When at home, (Ahmad, 2020) exemplifies that employees are exposed to more cybersecurity risks like phishing and ransomware than when those exact employees work directly at the institution or firm. This means that the idea of working from home increases the chances of employees being threatened with cybersecurity risks, such as those already discussed and explicitly explained on the former page (Ahmad, 2020).

Consequently, one of the solutions proposed by (Ahmad, 2020) is that employers or those responsible need to alert those who work from home about the potential cybersecurity risks and not to be drawn into such malicious and fraudulent acts that might lead the organization to its downfall. Organizations are supposed to ensure that the system or the software one employee will use and apply in his work from home (WFH) process is fully protected.

It makes no sense that companies direct their employees to work from home and have it processed efficiently without telling them about those cybersecurity risks (Ahmad, 2020). Doing this will not make the employee entitled to working from home, and that is because that employee would not be aware of the diverse forms of the cybersecurity risks nor how to handle and manage them efficiently.

What (Ahmad, 2020) states are the aspects of rehabilitating the employees who would work from home, thus making them fully and entirely qualified to overcome the many multiple threats that resemble the phishing and ransomware risks.

This is seen in the current Covid-19 situation that enhances for many cyber attackers to commit cybercrimes and the intention of leading organizations

to eternal distortion. That is why the perception of (Ahmad, 2020) is based on wanting the work from home employees and workers to apprehend the cybersecurity risks.

The paper also demonstrated that the global cybercrimes during the Covid-19 pandemic cost much more money than the amounts that would result during a typical day. This is proof that the Covid-19 situation complicates the issues of cybersecurity risks, as those risks tend to increase significantly to cause dysfunctions in the organizations and companies in the current Covid-19 world (Ahmad, 2020).

Therefore, it is needless to say that, without these precautions in the current work-from-home aspect that is resulted from the widespread of the latest pandemic, organizations would be exposed to severe loss, which would then make those organizations fragile and incompetent in the world of cyber risks and other insecurities.

These are the purposes why organizations, at least from the opinion of (Ahmad, 2020), are required to educate their workers and employees about the different strategies for managing cybersecurity risks.

Without the application of these essential matters like the education of employees about cybersecurity risks that are viewed as fatal to organizations, companies would eventually end due to the negligence of those cybersecurity risks.

What is more, (Wister, 2021) states that the Covid-19 pandemic has been negatively impacting people and organizations, which is very much consistent with what was mentioned earlier in the section by (Lallie et al.,

2021). Such organizations are inclusive of educational institutions and other businesses as well. Consequently, the issue of working from home, as discussed formerly, has introduced a lot of chains and restrictions to those who work from home.

The issue of Covid-19, as stated in the paper, introduced a new and unprecedented global health crisis to various people globally, especially in the cyber world we live in today. The author also presented that the pandemic impacted the lives of people everywhere. This demonstrates that the pandemic changed people's lives, which is why people are currently forced to work from home rather than the traditional works people had been accustomed to before the outbreak of the pandemic.

Figure 2 manifests some cyber-attacks that occurred during the Covid-19 pandemic (Wister, 2021). This figure illustrates how cyberattacks and cybercrimes affect healthcare providers, in general, and other firms and institutions.

For instance, April 8th, 2020 (Wister, 2021) conveys that many cybercrimes occurred on the same day. All those issues reveal a sort of dysfunction within the systems of companies and organizations amid the crisis of Covid-19.

Having said all that, one form of cyber-attacks held during April 8th is some sophisticated-based Covid-19 phishing attacks intended to bypass the defenses of information systems and servers. It is also said that cybercrimes and cyber-attacks have been increasing since the outbreak of the Covid-19 pandemic.

The figure further proves that there are plenty, perhaps countless, cyber-attacks that occur daily, especially in healthcare providers like hospitals and other institutions. Some more different types of cyber-attacks include malware, social engineering, and zoom bombing, as noted in figure four that is placed in (Wister, 2021). The hackers and those who typically commit fraudulent acts that are critical to the safety of the environment, in general, are reckoned to be utilizing the current case of Covid-19 where a lot of organizations, even those who were not accustomed to the idea of financial crises, do not have plenty resources at the current moment (Wister, 2021).

Table 2.1: cyber-attacks during Covid-19

Date	Description of cyberattack	Type of Attacks
April 8, 2020	The exposure to compromised e-commerce websites is greater than ever 26% increase in web skiing in March.	Malware
April 8, 2020	"Latest vaccine release for coronavirus (COVID-19)" mall spam spreads NanocoreRAT malware	Malware
April 8, 2020	NCSC advisory: COVID-19 exploited by malicious cyber actors	Social Engineering
April 8, 2020	Fake COVID19 websites spreading FirebirdRAT via fake DHL emails	Malware
April 8, 2020	Rush to adopt online learning under COVID-19 exposes schools to cyber-attacks	Zoom Bombing
April 8, 2020	Sophisticated COVID-19-based phishing attacks leverage PDF attachments and SaaS to bypass defences	Phishing, Malware
April 8, 2020	CDC warns of COVID-19- related phone scams, phishing attacks	Phishing

Some organizations are today heading toward bankruptcy because of Covid-19, as the pandemic forced those organizations to a new digital way of life that affected many people's lives. Moreover, the situation with the diverse organizations was substantially worsened, and as a result, many general people were financially affected by the pandemic.

This negative impact of Covid-19 on people has also had its effect on organizations. Due to that, people were financially struck by the pandemic, and organizations had no customers or people to sell their merchandise on. This information explains the effects of Covid-19 on a more expansive and

general scale regarding the organizations' inability to improve their information systems (Wister, 2021).

The same website also manifests the current new concerns of the Chief Executive Officers during the outbreak of the pandemic, Covid-19. Based on the words of (Wister, 2021), chief executive officers (CEOs) are currently thinking about some more concerns amid the pandemic outbreak. These concerns are because of what we can note today as the increase in cyber-crimes and cyber risks that can disrupt companies.

Some examples of these concerns are the CEOs attempt to mitigate and minimize the malware threats that most hackers tend to produce within the current pandemic that made the world based on a random and irrelevant status.

Chief Executive Officers in all companies and organizations are aware that, without this act of lessening cyber risks and cyber-attacks, companies would be affected in a significant manner, further as that people may be incapable of doing business in a relevant way that would comply with what is required.

Not only this, but another instance of what concerns CEOs during the pandemic is securing safe remote access. Considering the work-from-home perspective, it can be understood that unless a secure link is produced to workers, cyber attackers will keep attacking businesses by targeting their information systems for disruption and dysfunction (Wister, 2021).

Chief Executive Officers today think about how they could adopt to protect their evident information amidst the current Covid-19 pandemic (Wister, 2021). This is reasonably necessary for all chief officers of businesses to

think about and plan carefully, especially with the increase in cybercrimes and cyber-attacks.

Putting this altogether lets us realize and recognize the need for the protection of information systems and security systems. If not emphasized today, during these cyber threats that we have been discussing throughout the paper, companies would not be able to survive the cyber-attacks.

This presents the fatality of cyber and cybersecurity risks that are totally damaging to any company. Unless there is proper protection of information systems, organizations would be incapable of minimizing the threats, which are regarded as the primary objective of any company and organization (Paat & Markham, 2021).

In addition to the former point, (Wister, 2021) discusses that companies are required to restructure their facilities and re-examine their priorities due to the pandemic outbreak. That is because of the emergence of the Covid-19 pandemic that disrupted plans and objectives. Because organizations are currently facing increased cyber threats and cyber-attacks, (Wister, 2021) states that companies are demanded to have new priorities like improving their security programs. That is, based on the paper, companies need to rescale their budgeting criteria, and this is in order to provide the factor of improving security programs with the highest budget possible.

The indication of all these matters is a revelation of the risks that organizations and firms in cybercrimes are facing nowadays. That is why institutions are demanded to look for various ways to diminish the cyber risks and minimize them to the lowest rates possible. What is worth mentioning is that (Andrade, Ortiz-Garces, & Cazares, 2020), as well as (Wister, 2021),

discussed how Covid-19 had led houses to adopt the most modern networks and servers for their systems without putting in mind a structural and organized way to stop the cybercrimes and cyber-attacks.

This means that the attack on such homes that (Andrade et al., 2020) referred to as intelligent, are now more exposed and subjected to cyber-attacks led by hackers. This indicates the crisis communities and environments currently face amid the Covid-19 situation.

(Andrade et al., 2020) also points out that the process of purchasing modern devices and computers with the idea of turning their houses to being smart affects the locations of those houses. As mentioned earlier, with the sophistication of devices emerges an increase in the cybersecurity risks and the cyber threats that generally exist in all places people live in.

Thus, the hypothesis here, as expressed by (Andrade et al., 2020), is that modern laptops and other technological devices need to be developed for the security of those gadgets as well. If not protected and appropriately secured, using either the latest developmental procedures or by applying and adopting the cyber risk insurance, then it would be most likely that those devices become breached and contravened.

These are justifications that have been argued in a paper by (Andrade et al., 2020) and another by (Kaiser, Wiens, & Schultmann, 2021) regarding how the current Covid-19 situation has affected the lives of people, especially those following the process of working from home. Those employees and workers deal with their latest smart computers daily, exposing themselves to a significant percentage of the cybersecurity risks and the cyber threats that can alter the lives of those individuals and companies. That is why (Andrade et al., 2020) justify that the current Covid-19 situation has changed the lives

of many people and employees working from home (Kaiser et al., 2021).

In the same sense, another group of authors manifested a similar identification – as seen within the other prior texts – regarding the cyber risk crisis during the Covid-19 pandemic. (Sardi, Rizzi, Sorano, & Guerrieri, 2020) Indicate that there has not been an acceptable form of emphasis by researchers on cybersecurity risks and their ability to cause a dysfunction in the information systems within organizations. There are multiple types and examples of cyber-attacks during the current Covid-19 crisis.

(Sardi et al., 2020) also identified cyber risks as the risks or the threats that result from some malicious activities that are electronically-based rather than being subjected to the traditional definition of breaches. Cyber risk is also related to the different ways and types of malicious activities that distort the safety and security of one particular organization.

Not only this, but according to (Sardi et al., 2020), the cyber risks that occur in one organization or institution can deficit and lessen the financial resources of that particular firm, for instance. That is mainly because of the previously mentioned and demonstrated point regarding how cyber and cybersecurity risks can lead companies to lose large sums of money.

When we know that there has been an increase in the cyber-attacks, as per the words and the statements of the World Health Organization (WHO), it comes to our understanding that the health sector is greatly affected by the current Covid-19 crisis (Sardi et al., 2020), which agrees with what was mentioned earlier by (Williams et al., 2020). One reason for this is that health organizations are not concerned with the dramatic increase of cyber-attacks in the world, meaning that the statement of the World Health Organization had to be associated with the cyber-attacks affecting health sectors.

One instance given by (Sardi et al., 2020) regarding how cybersecurity risks and threats increased is reckoned in Italy from January to April 2020. According to the authors, during those mentioned months, the cyber-attacks in Italy doubled and increased significantly, resulting in many breaches. This shows us the remarkable effectiveness of the latest Covid-19 pandemic and how it shaped and altered the world of cybersecurity in a different contrastive manner.

Based on the findings of (Sardi et al., 2020), it is further put into effect that most countries lack awareness of this subject and how to mitigate and minimize cybersecurity risks. In the authors' words, only the United States is giving this topic some emphasis and attention. Consequently, the lack of attention and awareness on this topic in most countries, if not all, signifies that there needs to be a proper and comprehensive solution to the emerging cyber threats and cyber-attacks.

By putting some awareness and knowledge about the cyber world into people, individuals and communities would eventually brainstorm ideas to at least deficit cybersecurity issues and how they could manage them efficiently.

In other words, the concept of cybersecurity risks consists of some dangerous outcomes for companies and organizations. Without a proper and accurate plan on how to mitigate those cyber-attacks that include different types like phishing and malware, industries may be put to a definite end that would severely affect them (Sardi et al., 2020).

This is the primary reason why the perception of (Sardi et al., 2020) is based

on advocating a proper understanding and apprehension of the cybersecurity risks, especially today in such a fatal pandemic. With the awareness of how to handle and manage the cybersecurity risks, the health sector would be exposed to lesser cyber and cybersecurity risks than they note today with no form of awareness.

2.2.3 Cyber Risk Insurance

When discussing and discussing the perspective and importance of cyber risk insurance, we can know that, because today there are many forms of cybercrimes and cyber-attacks, companies and organizations must have some insurance not to be drawn into fraudulent acts and behaviors (Palmer, 2021).

It is of no use that companies and organizations perform their duties and roles through servers and devices when they are aware of the risks that they may face. That is, companies and organizations need to insure their information systems with cyber risk insurance institutions to prevent distortion or complexities when exposed to cybercrimes or cyberattacks (Palmer, 2021). That is because of the increasing number of cyber-attacks and risks during this period..

According to the article, cyber risk insurance helps protect companies and organizations from what we already know as cybercrimes and cyber-attacks (Palmer, 2021). This indicates that without cyber risk insurance for companies and policies, it would be difficult for companies to maintain their operational strategies and perform their duties acutely and accurately.

What is discussed by the author is that businesses can keep working and not risk being extensively exposed to cybercrimes and cyber risks using cyber risk insurance. That is because adopting and using cyber risk insurances

can help organizations minimize the cyber-attacks and the threats of hackers that are dominant and prevalent in today's world.

In addition, applying the concept of cyber risk insurance can help groups and organizations deficit their monetary losses in financial terms by having their costs and expenses covered in the event of data, information, or money loss (Palmer, 2021). This means that there is insurance on their money and data once they deal with cyber risk insurance companies, which shall minimize, as stated, their losses of data, finances, assets, networks, and many other substantial matters as well.

Thus, as already seen and acknowledged, cyber risk insurance includes countless benefits for organizations and companies. People can agree to partner with insurance companies to ensure that their data and information, even if lost, would eventually be recovered. This would maximize the productivity and the profitability of every company working with the insurers, for they would be sure, after all, that their information and data are in safe hands with the insurance companies (Palmer, 2021).

Moving on to talking about the perception of cyber risk insurance, (Armstrong, 2021) claims that companies and institutions must protect their reputation and all the other things they would lose in the event of cybersecurity risks. The author states that, with the help and assistance of cyber risk insurance, users, especially institutions, shall protect their evident pieces of information and the other necessary matters. This is because cyber risk insurance is designated to protect and support businesses, not to be withdrawn into setbacks.

By this means, the aspect of cyber risk insurance, at least in its simple defini-

tion, shall deficit the cybercrimes that, as mentioned priorly, are skyrocketing in locations like Canada (Armstrong, 2021). This will mitigate the risks resulting from those cybercrimes, such as ransomware, loss of information, monetary loss, and many other matters therein.

Therefore, according to the author, in this current digital age, it is far better to apply cyber risk insurance to lessen the committed cybercrimes worldwide than when this risk insurance is not used. Applying this would resolve the cybercrimes and lead the communities to have a professional background.

The author further points out that the concept of cyber risk insurance is substantial to every party using a digital device (Armstrong, 2021). This is because all digital information and data can be exposed to cybercrimes or cyber-attacks. Hackers or cyber-attackers may head to the point of using their hacking systems to breach other computer systems. However, with the help of cyber risk insurance, companies would be more likely to withstand errors and difficulties than when this risk insurance is not used.

This allows us to understand the importance and the significance of cyber risk insurance, further as how this risk insurance takes its name in ensuring that electronic and digital devices would not be exposed to any forms of risks. Through this, we can also note that cyber risk insurance will allow systems and data to be more secure for the safe usage of computer systems.

With the help of cyber risk insurance, companies and organizations could also handle and manage their information and data electronically. That is because any electronic business is exposed to cybercrimes and cyber risks, except for those businesses and organizations that adopt cyber risk insur-

ance (Armstrong, 2021).

Consequently, as far as we are concerned, using cyber risk insurance is a beneficial procedure to secure businesses by ensuring the safety of essential data and information. According to the author, these are some reasons why cyber risk insurance is vital for the deficit of cybercrimes and cybersecurity risks.

Another paper proposes that cyber risk insurance helps a lot toward ensuring the success of the company and that organizations would not face any threats related to cyber risks or cybersecurity (travelers.com).

This means that the webpage's author suggests applying for cyber risk insurance as a supplementary tool to lessen the financial losses and the other severe losses that are adjoined with the concept of cybercrimes, as already illustrated.

This idea of bestowing the concept of cyber risk insurance contains a lot of practical matters to be seen as things that would benefit companies and organizations in general (travelers.com). People with the risk insurance application would not need to stumble on the cybersecurity and cyber risks.

Instead, organizations would head toward a good corporate strategy to eliminate cybercrimes and cyber attackers, for institutions would then have plentiful amounts of money, monetary values, and assets in their organizations.

The points mentioned above are why cyber risk insurance is substantial in cyber technology. According to (travelers.com), there cannot be any form of stability without using the supplementary tool; cyber risk insurance. By

using and having it applied in any company, organizations can ensure that their businesses would be based on continuous forms of success, as they would not be accustomed to any cyber risks anymore.

As previously stated, that is why cyber risk insurance is regarded to be the mitigator of cyber risks and cybersecurity risks. Companies can use it to ensure that no other hacker or attacker views one company's confidential information and data. As a result, for now, at least, it can be reckoned that the usage of cyber risk insurance makes the performance of an organization very useful and helpful to businesses. It can also be understood that there is no way for any business to overcome the threats of cybercrimes, which are considered many nowadays, without heading for the application of cyber risk insurance (travelers.com).

In addition, (Romanosky, Ablon, Kuehn, & Jones, 2017) manifests that the need for cyber risk insurance has become more than ever due to the frequent breaches happening nowadays. That is because of the commonness of cybercrimes and cyber risks, as already perceived, and the way these crimes are nowadays regarded as things occurring daily as if they were expected. These crimes have arisen recently and require people to think deeply about methods, such as risk insurance, to deficit such crimes and immoral behaviors.

The paper further elaborates on cyber risk insurance and defines it as a broad concept that tends to compensate the parties suffering from cybercrimes, such as the first and third parties. According to the research, if one organization suffers from cyber risks, such as the already listed malware, ransomware, and other things, the insurance parties would need to compensate the affected parties (first and third parties). This is how the authors

defined cyber risk insurance (Romanosky et al., 2017).

To further illustrate, if a hacker electronically attacked one organization to attain that company's confidential information, then the cyber risk insurance parties would be required to address those losses and resolve them accordingly, whenever and wherever applicable (Romanosky et al., 2017).

It is further discussed in (Romanosky et al., 2017) that the aspect of cyber risk insurance has been a very helpful criterion for companies and organizations since it was first applied. The authors cited Marotta et al. in what they demonstrated that cyber risk insurance companies compensated and covered the loss of 14 carriers and cited the words of Majuca et al. concerning how cyber risk insurance organizations covered the losses concluded from cyber-crimes.

Having a deep look at these statements regarding cyber risk insurance provides us, readers, some insights regarding the sustainability and effectiveness of such insurance companies in a world that, as discussed earlier, is noticing a rapid increase in cybercrimes and cyber risks. We can note that without these insurances, it would be difficult and troublesome for organizations and companies to overcome the issues of cybercrimes (Romanosky et al., 2017).

It is also asked about the role of cyber risk insurance policies and what costs they cover and exclude. The same paper talks about this matter in a specific way, explaining that the first thing insurance companies do is segregate between the first and the third parties (Mendes-Da-Silva, Lucas, & de França Carvalho, 2021).

This means that one of the core fundamentals carried out by the insurance organizations is the differentiation between the first and third parties that suffered from the cybercrimes or any other issue resulting from the cyber world (Romanosky et al., 2017).

The article discusses that the first party in the cyber risk insurance matters is the party that insured its assets, information, devices, data, servers, and many other matters. Therefore, we can differentiate between the first and the third parties by understanding which party insured its assets (Mendes-Da-Silva et al., 2021).

The hypothesis of (Romanosky et al., 2017) is that if one party deals with an insurance company directly, and resolves to a contract between the insurance company and the party, then that side would be referred to as the first party. As for the third party, we understand that the side is external to the contract done and agreed upon by the first party and the insurance company.

We can also realize that the third party is the party that suffered – one way or another – from the behavior of the first party, leading to a breach of data, information or any other example of cyber risks.

Figure 3 is a diagram illustrated by (Romanosky et al., 2017) to posit ten of the most covered losses by the cyber risk insurance policies in cybercrimes and cyber-attacks.

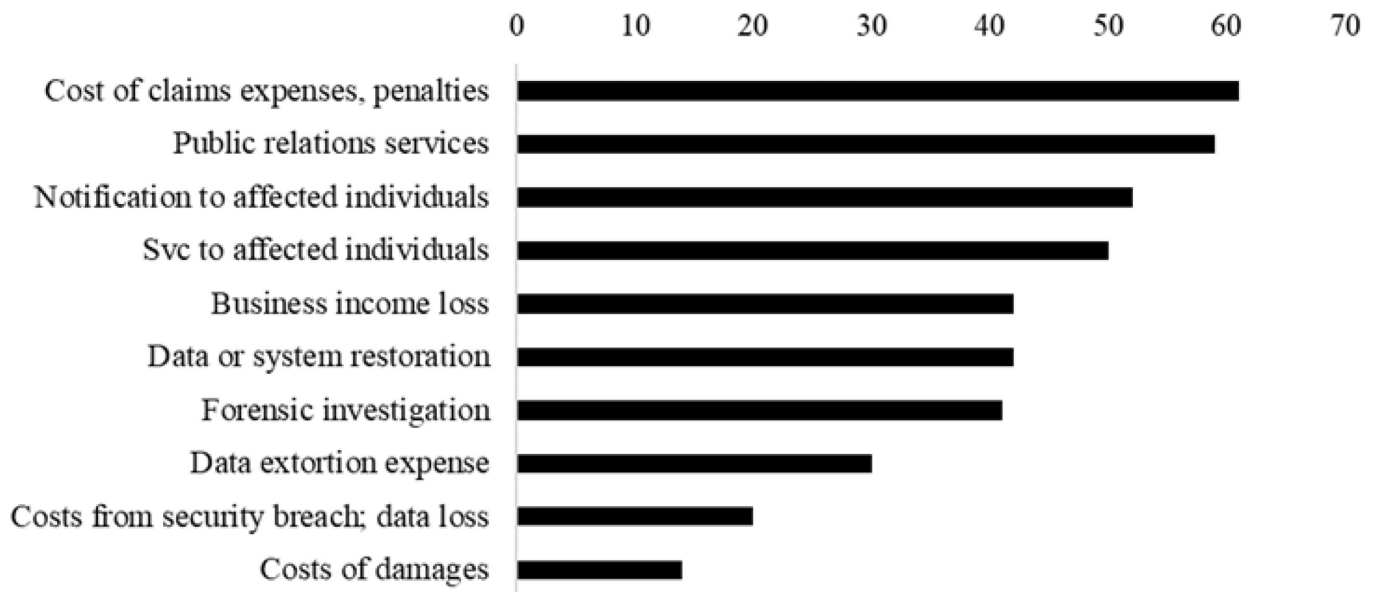


Figure 2.2: Top ten most covered losses
(Romanosky et al., 2017)

As seen in figure 3 above, some of the losses covered by insurance companies, according to the website, include the cost of expenses and penalties. This means that whatever is paid by the insured parties (first parties) is compensated for them. As well as that, first parties are also compensated or have their amounts covered on their loss of income, or perhaps what can also be stated as loss of revenue of that particular business.

That is, if one business were low in income due to whatsoever, then that business would be compensated by the insurance companies. Organizations are also compensated for a security breach or data loss, meaning that their monetary losses of money, data, and information would be covered by insurance companies (Romanosky et al., 2017).

This promotes the idea that cyber risk insurance is a matter of several benefits and that people, especially organizations and companies, can utilize it by applying it not to pay any further expenses, whatever they were.

Insured organizations can also not pay for the damages in their information systems, meaning that those companies would not pay for the damages in their systems.

By stating all this, we come to know that the risk insurance companies, as stated, are very fruitful and profitable in terms of their advancement and productivity to organizations in general.

Additionally, (Tonn, Kesan, Zhang, & Czajkowski, 2019) clarifies that cyber incidents breaching databases and information systems are considered one form of violation of the privacy of individuals. Within this cyber circle, it is assumed that organizations and users working on a computer cannot work proficiently without being exposed to breachers and attackers from diverse locations, especially in this current world that is full of cybercrimes; the world that is currently revolving around computers and cyber technology.

Therefore, the paper signifies that there should be a cyber risk assessment to evaluate the sort of risks companies and organizations generally face in their pursuit to combat hackers and attackers. According to the paper, if a proper and convenient structure of cyber risk management and cybersecurity are applied within the field of the cyber world, along with cyber risk insurance as well, then it would be more likely to state that companies would not face severe issues related to cybercrimes as they do now (Tonn et al., 2019).

Moving on to discussing another perspective related to cyber risk insurance, (Camillo, 2017) examines that the instances of cyber risks are inevitable, especially with the advanced and sophisticated forms of technology we can find today. The author states that the whole world is currently affected by the concept and the ideology of cyber because of their thought and belief. With that said, it is to be herein exemplified that there is no way out from

the different classes and the different risks of cyber. People can mitigate and lessen those risks, yet in the author's perspective, the world will always be based on the effects and the aspects of cybercrimes and cybersecurity risks.

What is being said by the author is that the sophistication of cybercrimes and the cyber world will keep on touching and affecting even the things and the matters that we consider today as protective to the cyber environment of organizations.

To further demonstrate, Camillo says that cybercrimes will be inevitable in the future, especially considering that hackers and cyber risks develop over time. This means that even the aspect of cyber risk insurance would not be able to impact and reduce the cybersecurity risks positively.

Despite this, there is a positive tone in the academic article written by Camillo (Camillo, 2017), it is thought in that research that insurers and researchers will eventually find some leading solutions and prevalent ways for the mitigation of cyber risks, overall. This further means that small and big organizations are looking for ways to implement processes and procedures to reduce the effects of cyber risks on systems, particularly information systems used by those who work in organizations.

Another matter discussed by Camillo is the features existent within cyber insurance policies, which, as mentioned earlier, are equivalent to the recovery of data, breaches of data, monetary loss and many others as well. Once again, this enforces the presumption that cyber risk insurance is currently a prevailing aspect in the field of reducing the risks of cybersecurity that were pointed out earlier at the beginning of the research (Camillo, 2017).

Another matter discussed by Camillo is the features of cyber insurance policies, which, as mentioned earlier, are equivalent to the recovery of data, breaches of data, monetary loss, and many others. Once again, this enforces the presumption that cyber risk insurance is currently a prevailing aspect in reducing cybersecurity risks that were pointed out earlier at the beginning of the research (Camillo, 2017).

In the article by Camillo, he states that there is a deep and delicate relationship between the insurers and the insureds (customers), in which the insurers tend to provide the insureds with services for properly functioning the business. These services include crisis management, legal consultation, advice, and other services (Camillo, 2017).

In other words, people can benefit from cyber risk insurance policies and companies, and this is because organizations can always consult experts in the field of cyber risks and navigate ways to overcome the issues they may go through.

Another feature offered by insurers is the mentioned security management, which advocates for the concept of analyzing crises properly. With the help of this feature, organizations can overcome the difficulties they will face after one crisis and thus move on with things accurately, without any further complexities regarding the topic of cyber risks.

The ideology of cyber risk insurance can be referred to as a model or perhaps, a guide for companies and organizations to pave their way from the debris of failure and breach breaches to being successful once again. That is why the idea of proper cyber risk management and having proper cyber risk insurance are both fundamentals every company needs to have.

With this understanding and these ideas, organizations would be able to utilize all the negative matters resulting from cyber risks and cybersecurity risks to change their statuses and positions from unhelpful to becoming leaders and pioneers in that same field they have been accustomed to (Camillo, 2017).

All these matters illustrate and convey why cyber risk insurance is essential to maintain the sustainability and the improvement of the world and the concept of insuring cyber risks, even though the world is advancing and improving to further levels in the sense of cyber (Camillo, 2017).

Furthermore, another group of researchers propose using another tool for cyber risk insurance and claim that there are some deficits within cyber risk insurance in the first place (Shetty et al., 2018). What the authors say about this is that enterprises and organizations are required to apply cyber self-protection rather than only implementing the cyber risk insurance parties to insure the losses of organizations.

As already discussed, there are two parties in this operation: the insured and the insurers. According to the authors, enterprises would be unable to overcome the point of monitoring hackers, cyber-attacks, cybercrimes, and many other things if the cyber self-protection tool is not applied effectively in those enterprises.

The authors state that companies and organizations need to know of the potential cybercrimes and the hackers that intend to disrupt the safety of the information systems of those organizations. If insurers cannot monitor the cybersecurity risks within one information system, then it is most likely that

that insurance company would not be doing a fine job in satisfying organizations.

Therefore, it is proposed in the paper that the Cyber Risk Scoring and Mitigation (CRISM) be applied to have an estimated view of the potential cyberattacks and look at the dangers that might be inescapable while not using this CRISM tool.

According to the authors, the tool would lead enterprises and insurance companies to perfect their work, not only in terms of compensating the affected first parties but also to prevent those attacks and breaches from happening (Shetty et al., 2018).

With that being said, it is relatively known that the authors' opinion favors the application of the Cyber Risk Scoring and Mitigation tool. This does not mean that companies would not use the cyber risk insurance or that the cyber risk insurance would eventually be of no use. Instead, it means that with the help and assistance of cyber risk insurance and Cyber Risk Scoring and Mitigation (CRISM) tools, enterprises would be able to defect the shortcomings resulting from cyberattacks, cybersecurity risks, and cybercrimes (Shetty et al., 2018).

Consequently, implementing CRISM would benefit insurers and the insureds for organizations and businesses in a world filled with cyber-attacks and cybercrimes, which would lessen those risks resulting from the world we live in today. This is mainly due to the estimation of cyber-attacks and other things that would make the process easier.

Another paper also discusses implementing another framework other than CRISM (Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2017). The

purpose behind implementing a tool for cyber risk insurance is not only to perceive things from an insured perspective. This means that the authors believe that applying a framework besides cyber risk insurance would help companies and institutions to be more sophisticated than when such tools and frameworks are not designated for cyber risk insurance.

That security breaches are common nowadays, and because we live in a world that is, as mentioned, full of cybercrimes and cyber-attacks, the authors suggest the implementation of cyber-risk assessment and mitigation (CRAM) in order to efficiently deficit and lessen the many breaches we have been noticing since the outbreak and the beginning of cybercrimes (Mukhopadhyay et al., 2017).

Depending on what the authors say, the cyber-risk assessment and mitigation framework take its name to lessen and evaluate the risks of cybercrimes. The authors further claim that the application of the cyber-risk assessment and mitigation framework would significantly decrease cyber-attacks, and that is because of the framework's capability of estimating the probability of one attack.

By doing so, it is indigenously clear and lucid that organizations would at least not face cyber and cybersecurity risks as they are now without the CRAM or the CRISM frameworks.

Further, the authors refer to one other merit related to the CRAM framework, which is associated with the calculation of losses resulting from cybercrimes and cyber-attacks using the method of approximation to see the average loss of data in every cyber-attack (Mukhopadhyay et al., 2017).

Doing this matter mentioned above would lead the organization to enhance and develop their information systems according to the losses endured in every cyber-attack.

Despite all these tools and methods, the paper's authors propose the application of cyber risk insurance, along with CRAM (Mukhopadhyay et al., 2017). This is because, with the help and assistance of cyber risk insurance organizations and policies, companies could diminish and minimize their losses, whether in terms of data or money, to the least possible.

This reveals the fact that the tool of cyber risk insurance is a fine one and can be used to diminish and minimize the risks of cybersecurity risks and the other known risks and uncertainties in the cyber world.

Despite this, it ought to say that, as already discussed, the application of other frameworks like cyber risk assessment and mitigation (CRAM) helps companies and organizations be as productive as possible (Mukhopadhyay et al., 2017).

Thus, the perspective of (Mukhopadhyay et al., 2017) is that cyber risk insurance is a helpful tool for companies to benefit from. However, according to the paper, the CRAM framework can work with cyber risk insurance companies to assure the maximum profitability and total productivity of businesses and organizations.

In simpler words, as already put and discussed in this section of cyber risk insurance, there are several, perhaps plenty of ways and ideas that would help and assist businesses with the perspective of wanting to create as many chances without the intervention of other cyber-attackers or those who sim-

ply want to commit unnecessary cybercrimes.

One of these ways is the application of cyber risk insurance and the adoption of some of the frameworks discussed earlier in the paper, such as CRAM and CRISM. Using all these matters, it would be definite that companies and organizations would at least minimize – if not eradicate – the issues of cyber and cybersecurity risks to the minimum possible rate.

This leads us to comprehend that, without these frameworks and tools, companies would not be able to endure the difficulties that we can find in the cyber world and cyber field; basically, the common cybercrimes that are currently occurring daily result in shutting companies down.

‘Zurichna’ illustrates how cyber risk insurance protects the data of people and the indivisible groups in a community. With this, hackers would not be capable of breaching data and stealing other people’s information (zurichna.com, 2020).

When this is related to organizations and industries, they can work on making their data, servers, and information confidential to avoid intruding by any hacker.

According to (zurichna.com, 2020), a Zurich Company, Cyber insurance consists of several benefits and advantages, such as the costs of a privacy data breach, costs related to reputational damage, and many others. All these concepts and advantages shall lead organizations and companies to overcome the failures we can view throughout this article based on cyberattacks, cyber risks, and cybercrimes.

Therefore, as far as it is understood, the application of the cyber risk insur-

ance framework is quite beneficial to companies, as it advocates for security and minimizes the tension created by hackers and the other groups of people who intend to ruin the safety of those organizations.

That is why, at least in accordance with the opinion of (zurichna.com, 2020), the application and the implementation of the cyber risk insurance tool are essential for maintaining businesses for as long as possible.

It is also a further demonstration of the need for a framework that would be able to maximize the productivity of organizations and diminish the risks endured by them.

As already said, Zurich explains our need today for executing the cyber risk insurance to insure devices and servers. Without this relationship between the insurer and the insured, it is very likely that companies would not be able to survive in one single cyber-attack (zurichna.com, 2020).

Even today, it is commonly known and understood that vehicles could not be driven on the roads without being first insured by the insurance company. This means that insuring devices and servers – despite seeming unworthy to some – is considered a crucial matter in the cyber world. That is the primary reason cyber risk insurance is necessary for groups and organizations.

As reckoned in figure four, adopting such tools and frameworks as cyber risk insurance, for example, helps organizations to be more flexible and more accurate in terms of leading the business to the shore (zurichna.com, 2020). This is a matter of many dilemmas, especially when considering the many risks in the cyber world today.

Therefore, businesses need to think of ways to adapt themselves to using different frameworks to have as many chances to conduct professional work.

It can be figured out and observed using the perception in (zurichna.com, 2020), that the matter of cybersecurity risks is role-changing to industries and organizations, especially those that base their works on a digital manner rather than a traditional way.

Due to this difficulty of running a business during the digital time, organizations are supposed to look for ways to lessen such risks and risks and cybercrimes through the adoption of tools and frameworks that are against cybercrimes. If not adopted and applied, it is almost certain that companies would not be able to proceed with their businesses efficiently.

Using the same mentality and idea, it is presumed that the digital world comprised of servers, networks, computers, and other devices becomes much better and safer for companies and firms with the adoption of cyber risk insurance or cyber risk assessment and mitigation frameworks.

In summary, we can take into account – through the many advantages we can view by just deeming on the figure – that the concept and the phenomenon of cyber risk insurance is a matter that needs to be adopted within every information system by people and organizations. Companies would not be able to perform their operations and tasks as proficiently as they would in the case of not having cyber risk insurance (zurichna.com, 2020).

Additionally, another paper (Khalili, Naghizadeh, & Liu, 2018) manifests that the market of cyber risks is increasing substantially, leading different forms of individuals and organizations to look for ways to diminish the

cybersecurity risks. With that in mind, it is noted that people and organizations, according to the paper, are currently looking forward to improving their systems by applying cyber risk insurance to reduce cyber risks. (Khalili et al., 2018) also states that products like cyber risk insurance can promote businesses by managing and handling the cybersecurity risks and the cyber threats that are the most significant concerns of companies during the Covid-19 pandemic. This means that cyber risk insurance is beneficial for businesses to apply to avoid stumbling upon the different cybersecurity risks.

Furthermore, it is also demonstrated by (Khalili et al., 2018) that adopting cyber risk insurance increases the safety and security of organizations and their systems. Therefore, the contract between the insurer and the insured increases and promotes further protection within the systems in general. This enforces the availability and the profitability of applying for cyber risk insurance within different information systems.

This way, organizations could increase the security of their websites and information systems not to let intruders like cyber-attackers disrupt those systems. This demonstrates that the key strategy for organizations to adopt to reduce and minimize cybercrimes is seen in the application of cyber risk insurance (Khalili et al., 2018).

This gives us an overview of the importance and significance of the application of cyber risk insurance in systems to reduce cyber risks by increasing security in those systems. It also allows us, researchers and readers, to comprehend the various positive points behind applying and adopting the cyber risk insurance tool.

We can apprehend and therefore state that the concept of cyber risk insurance is beneficial for companies and organizations, and this is because of the primary role it plays within those companies and such systems (Khalili et al., 2018).

Similarly, it is crucial for those who want to diminish the cybersecurity risks to apply for cyber risk insurance. That is to lessen the rates of phishing, malware, and all the other forms of cyber-attacks occurring within systems (Khalili et al., 2018).

Regarding what was stated on (travelers.com), the website views the application of cyber risk insurance to be essential to businesses and companies. The perception above presumes that the mindset of spreading the usage of cyber risk insurance needs to proliferate substantially, especially within the servers and the information systems that have stumbled upon diverse forms of cybersecurity risks like malware, for instance.

This concept of finding the cyber risk insurance a beneficial tool to deficit and minimize the risks of cybersecurity and cyber threats ensures all that has been stated until now regarding this matter. That is, until now, it has been generally stated and indicated that the aspect of cyber risk insurance complies with what companies and organizations need to stop or perhaps reduce the severance of cyber risks.

As seen in (travelers.com), organizations and industries may not have a promising future in their businesses without the application and implementation of cyber risk insurance, which is designated to secure the data in those businesses and not to let breachers take over that evident information. That is the reason why cyber risk insurance is essential.

One more benefit of the acceptance of cyber risk insurance in businesses

is that companies would be able to recover their data in the event of a data breach. This means that in the case of a cyber-attack, businesses would be able to recover their lost data.

This is one instance of how cyber risk insurance can be helpful to businesses, allowing them to not care for the lost data because it will eventually be recovered.

Further, it is revealed that cyber risk insurance can help companies with the costs of business disruption, loss of revenue, damage to equipment and tools, and many other matters. This illustrates that businesses and organizations can benefit from the application of cyber risk insurance and thus reduce and minimize the cyber threats that are regarded to be plenty in number nowadays.

Another benefit of using cyber risk insurance is that it shall protect businesses safely and profoundly from all those cybersecurity threats ravaging the cyber world. Without the application of such a tool, the website presumes that breaches and infringements would easily happen to companies and institutions.

Not only can cyber risk insurance help companies and organizations with recovering the breaching of data or servers, yet it even can be helpful with the idea of devices' protection to prevent any unauthorized access to those devices.

In the same manner and with a clear perspective, cyber risk insurance can help companies protect their confidential and private pieces of information to prevent any breaches of those data.

Even in the case of stealing devices, it exemplifies that organizations, with the assistance of the cyber risk insurance tool, can protect the evident data and information within those devices, even if they were in the hands of hackers who intend to commit cybercrimes.

Similarly, this provides us with an elaborative understanding of how cyber risk insurance works, which is created and conveyed for the proper solution for the many multiple cybercrimes and cyber-attacks currently occurring. Such a form of cyber risk insurance, along with other tools and frameworks like the CRAM and CRISM, are necessary and helpful to every organization to do its job and accomplish its objectives in the best way possible.

This confirms the point and idea that a great benefit and impact revolve around the cyber risk insurance tool. This is especially considering the outstanding role cyber risk insurance plays in reducing and lessening the cyber-security risks and threats that have been the greatest fear of organizations. The paper, (travelers.com), explains in an intensive way how people and organizations could live their everyday lives with the application of cyber risk insurance as if there had never been such risks and threats.

Implementing cyber risk insurance is also supposed to help companies with the additional expenses to be paid in the event of a breach in data or an information system. Companies would be able to not pay for the legal costs, investigation, recovery of information if applicable, and many other matters in case they adopt the cyber risk insurance program.

So, overall, it can be said that putting all the cited references together has some things in common. One of these ordinary things from the words stated throughout the paper is the importance and cruciality of the cyber risk in-

surance, especially regarding being applied in health sectors.

As previously mentioned, the Covid-19 pandemic has increased the rates of cyber-attacks and cybercrimes, which means that institutions and health-care providers are supposed to navigate some ways and solutions to mitigate the cybersecurity risks amid Covid-19.

One of these ways and solutions, as manifested in the ‘Cyber Risk Insurance’ subject, is the application of cyber risk insurance to ensure that companies would minimize the diverse forms and types of cybersecurity risks emerging from Covid-19.

With this in mind, companies and organizations can deficit the outcomes of the Covid-19 cybersecurity risks through the accurate application of tools like the cyber risk insurance, even with the two mentioned frameworks: CRISM and CRAM.

2.3 Conclusion

All in all, this provides us with an answer to the question of whether cyber risk insurance could play a significant role in reducing cybersecurity risks. In simpler terms, with cyber risk insurance and its compliance with its rules and policies, companies can continue their progression and advancement in their businesses. One reason for this is that cyber risk insurance covers the costs of loss of data, information, monetary amounts, and all other matters and concepts endured while exposed to one form of the many cybersecurity risks.

Chapter Three

Methodology

3.1 Overview

3.2 Hypotheses Development

3.3 Research Model

3.4 Conclusion

Chapter 3

Methodology

3.1 Overview

In order to achieve the research aims, it is adequate to obtain valuable and essential data that will only help the reader gain knowledge in this subject. Many researchers use several ways to gather the required information to come across a piece of reliable information which will enhance the validity of the results. The research will use a mixed design technique to understand the research topic better. The mixed-method used is a composition of qualitative and quantitative parts. The quantitative part will be a questionnaire survey with a closed-ended question, and the qualitative part will be semi-structured interviews, and at the end, content analysis will be done to achieve a better understanding of the topic. Both techniques will be used in the analysis, but the main work will be on editing a risk model and adding cyber insurance to it to develop a unique model that has cyber insurance in the plan of mitigating security risks.

3.2 Hypotheses Development

H1: Management of organizations have a positive attitude towards cyber insurance

According to (Panda, Farao, Panaousis, & Xenakis, 2021), there are a lot of organizations that recently started to pay attention to cybersecurity risks and considering it as a business risk, as a result, those organizations' management are now thriving to seek ways to ensure their business continuity. Earlier but in support with that, (Franke, 2017) argued in a paper that during circumvention, current technological controls sometimes lag the hackers' skills, resulting in residual IT security risks which cannot be totally eliminated through available technological advancements alone. Hence, it is suggested by organizations' management to involve another 'willing' party so that residual IT security risks are transferred to through cyber insurance. However, despite this positive attitude towards cyber insurance, (Panda et al., 2021) claim that it is still failing to take a central part within the organizations in the management of IT security risk. This raised the hypothesis, according to the author of this research, of whether management of organizations are leaning toward adhering to positive attitudes regarding cyber insurance.

H02: cybersecurity risks have a negative impact on a business revenue.

According to the literature, (Havakhor, Rahman, & Zhang, 2020) discussed that cybersecurity risk events can be disruptive to the organization and can possibly affect it at a competitive disadvantage. It is also evident in that paper that cybersecurity attacks and breaches have been rising recently disrupting businesses and not only on operational glitches. Such failures sink the organization in fines and litigation costs, harm the trust, trigger the rep-

utation of the organization and eventually might force the organization to apply major shifts in a desperate try to remediate the damages. Nevertheless, according to the author, the severity of a particular cybersecurity risk has the potential to impact and disturb the core value of the organization. However, there is limited evidence regarding the vulnerability of an organization in relation to its fundamental value. On the other hand, there is evidence that organizations that invest in cybersecurity ultimately deal with significantly less cyber incidents which consequently means that even during the occurrence of cybersecurity risks there is little to no money loss and hence, slightly affected business revenue and organizational capital cost (Blobe, 2018). Interestingly, (Weber, 2018) argues that sometimes organizations are dealing with risks, in which some are considered outstanding such as the risk of harmed reputation, those organizations consequently be unnoticed and neglected by the consumer market. However, they become very interesting and catchy to the investors. So, according to the author of this research, this raised the hypothesis whether cybersecurity risks have a negative impact on a business revenue.

H03: Cyber insurance has a positive impact on the cybersecurity risks.

It was found in the literature, according to (Panda et al., 2021), that organizations that integrate cyber insurance eventually become more alert and aware of the appropriate behaviours to protect themselves from cybersecurity risks. Those behaviours, whether positive or negative, are oriented according to the nature of the attack. So, a decision taken by an organization integrating cyber insurance is said to have a positive impact on cybersecurity risks. In further elaboration, those organizations will have an increased endpoint security which will consequently decrease any possible losses caused by a network attack. However, on the other hand, for example if the or-

ganization lacks anti-malware system which will the cyber insurance would take care of within the insured organization, it may also unintentionally negatively impact neighboring PCs that are under malware attack. This is why, a hypothesis of whether cyber insurance has a positive impact on cybersecurity risks is raised.

H04: Cyber insurance coverage has a positive impact on a business revenue.

According to (), the typical image of help provided by insurances is not about dealing with the everyday small risks, it is rather about managing large ones, although might be uncommon but are considered very expensive when they occur. In this case, the coverage provided by cyber insurance will certainly has a positive impact as the organization will fully recover, at least financially, from cyber-attacks. On the contrary, (Panda et al., 2021) claim that because of the novelty of the cyber security field and scarcity of calculated related losses accompanying cyber-attacks, insurers are facing uncertainty in pricing their services. This, although indirectly, but ultimately affects the business revenue as the management of organizations are unaware of how much to invest in cyber insurance, especially with the difficulty in accurately predicting risks. They are unclear of the needed coverage or the correct amount of investment in cyber insurance without sinking their budget and negatively impacting the business revenue. Interestingly, (Franke, 2017) also discuss another important aspect regarding cyber insurance coverage is related to the waiting period applied for the insurer to compensate the lost revenue of a business. Depending on the waiting periods offered by the insurers, it can positively or negatively affect the business revenue as obviously, the shorter the period, the better it is for the insured. According to ,(Franke, 2017) interviews were made with insurance companies and

the shorted waiting periods provided were 6 or 8 hours. The waiting periods are a mechanism that is similar to a deductible, only that it is based on time instead of money. With that being said, the author of this research hypothesized that cyber insurance coverage has a positive impact on business revenue.

H05: Security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance

(Xie, Lee, & Eling, 2020) argued that there is a lack of clarity on what is and is not covered by cyber insurance, and identified this as a main reason to why cyber insurance has been limitedly adopted. Similarly, (Franke, 2017) discussed that one of the important discrepancies is about whether mistakes and omissions are covered or in other words, any non-malicious events. Moreover, it is worth mentioning that insurers have policies with varying levels of rules. Some companies are considered very strict as they are not covering non-malicious events and even if so, not all events are covered such as power outages (Franke, 2017). Basically, it is unknown what kind of risk is accepted and covered by cyber insurance insurers. However, there are some types of cyber insurances that provide coverages for human errors or technical failures and non-malicious events for an extra fee. Similarly, other cyber insurers do not include first party errors in their standard prices but provide separate extensions to buy that covers for omissions committed by insured organizations (Franke, 2017). Nonetheless, there are cyber insurers that provide coverage in three different versions as firstly, the regular business interruption costs that happened because of security attacks. Secondly, full costs coverage for system failures not caused by security attacks but due to any unintended and unplanned interruption. Thirdly, protection against any adverse effects due to reputational harm because of data loss,

for instance. Finally, it is evident to the author of this research that there is ongoing development towards what is being covered by cyber insurance companies. This is in support with (Franke, 2017), who reported that insurance intermediaries remarked that there will be an increased coverage of non-malicious events. Finally, it can be said that cyber insurers are willing to insure any risk regardless of its origin as long as it is paid if cyber insurance is considered as a financial risk transfer method. This raised the hypothesis that security risk unrelated to cyber-attack and infrastructure failures are positively impacted by cybersecurity insurance.

H06: The perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance

There are important benefits of cybersecurity insurance discussed by (Panda et al., 2021) as it is mentioned that management of organizations are provoked by cyber insurance companies to invest more in protection. It is also, believed that cyber insurance enhances the social optimum through increasing the organizations' level of cyber protection as well as serving as an indication to the level of protection the organization is at. Lastly, cyber insurance introduces the world to new and upgraded standards in cybersecurity. All perceived benefits of cyber insurance are said to have a positive effect on those in decision-making positions to adopt cybersecurity insurance. On the contrary, as previously mentioned, the author also argued the complexity of risk estimation and weighing whether the investment in cyber insurance is worth it or not. Similarly, this is in support with (Panda et al., 2021) mentioned regarding IT managers and cyber insurance. The authors argue that IT managers anticipate very little expectations from cyber insurance services which makes the decision of contracting with cybersecurity insurers appear to be overpriced. Not only that, but (Franke, 2017) proceed to claim

that IT managers self-insure the unfrightening small losses and attempt to assure their stakeholders that catastrophic and disastrous breaches have low probability of occurring. Moreover, according to (Weber, 2018), despite the desire and attempt to consider adopting cyber insurance because of high cyber incidents number, there is still a gap between the cyber insurance currently in process and the security actions established by IT managers. With that being said, the author questioned whether the perceived benefits of cybersecurity insurance have a positive impact on managers' attitudes towards utilizing security insurance or not.

H07: Security awareness has a positive impact on managers attitudes towards utilizing security insurance

In the literature, it is found that decision-makers are struggling because of the lack of standardization as well as experience across the services provided by cyber insurance companies (Panda et al., 2021). In elaboration, if IT managers are deciding to adopt cyber insurance they need to have a sophisticated understanding of their organizations' cybersecurity risks in order to choose the appropriate cyber insurance coverage type that will most benefit their organizational security risks. Although there is a very wide application and knowledge of security measures, it is still considered a struggle for cybersecurity managers to assign and classify limited resources across a variety of security countermeasures to mitigate or even prevent the negative impacts of a security breach. Not only that, but decision-makers are required to consider alternative options to handle residual risks because there is not any amount, no matter how big, of investment in cybersecurity can guarantee full protection (Panda et al., 2021). This allowed the author of this research to hypothesize that security awareness has a positive impact on decision-makers' attitudes toward utilizing cybersecurity insurance.

3.3 Research Model

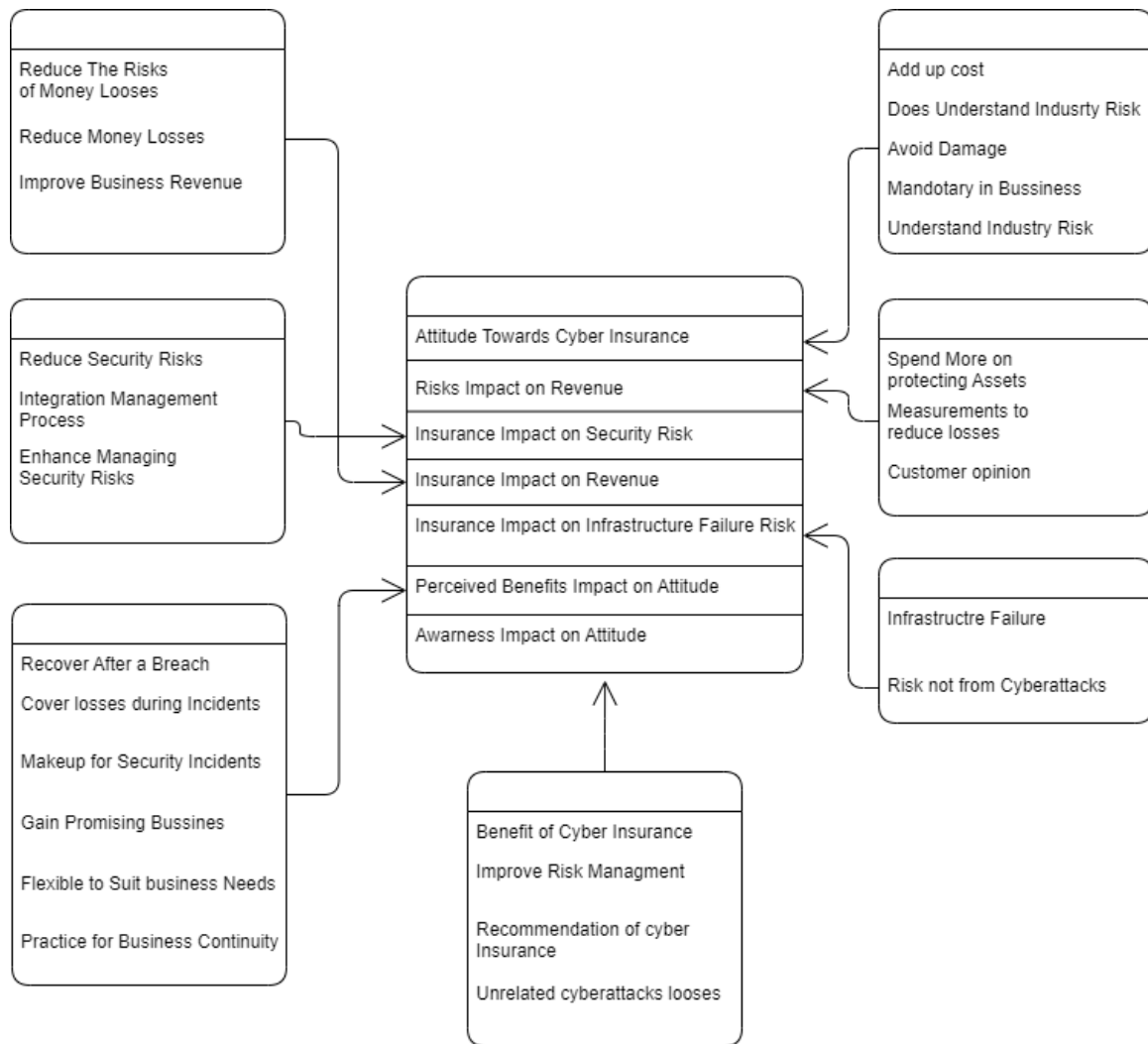


Figure 3.1: Independent Variable and Dependent Variable

In researches, representing the theoretical image of all the objects being studied is referred to as a research model. It is considered as one of the most useful methods to comprehensively describe the interrelationships of the researchers' ideas and provide a further explanation of them. There are multiple types of research models that are utilized by the researchers in the field of information security. However, the choice of using a single or

multiple research models is not random, but highly depends on many factors. The area explored by the researcher as well as the research question, research methodology and targeted audience are some examples of those factors. For instance, the research questions are considered major factors in defining the research model, especially that they are derived from the hypotheses. In elaboration, the questionnaire prepared by the author intends to show the impact of the cyber risk insurance on business continuity and business revenue, which allow multiple variables to emerge. So, the author mapped each statement in the questionnaire with its interrelated variable, which can be seen in Table 3.1. This way of research data presenting considers the research model to be prescriptive.

Generally speaking, there are two broad classifications for research models, as they can either be descriptive or prescriptive. Firstly, the descriptive research models are the simplest models in which the research question is described and the variables, whether dependent or independent, are listed with no clear specification of any interrelationships among these two types of variables. Secondly, the prescriptive research models are known to be more complex than the former. These models can contain visual representation to list and identify the dependent and independent variables. It also, on the other hand, shows an understanding of the interrelationships among the variables.

As previously mentioned, the model of this research paper is prescriptive, as clearly shown in Figure 3.1 the author presented the variables and their classification as dependent or independent and how each of them is integrating with one another. The author also mapped the variables in accordance to the hypotheses and questions in the questionnaire. This presentation of variables falls under the Simple Influence Diagram – 2 tier model category.

This diagram clearly shows the classifications of the variables. This diagram has two levels, dependent and independent, and each level has multiple variables, it is considered as a prescriptive in nature.

3.4 Conclusion

In order to investigate how cyber insurance would impact the cybersecurity risks, seven hypotheses were developed, as shown next:

H01: Management of organizations have a positive attitude towards cyber insurance.

General liability insurance policies, in many cases, will not protect organizations from losses related to cyber-attacks or data breaches. When in fact, data is one of the most valuable assets and worth much more than physical assets; thus, it is important for a business to have the needed safeguards in place to guarantee that such assets are well protected. Improving the liability insurance with cybersecurity coverage can provide the organization with freedom from worry in the event of an attack due to the fact that the organization's financial overall condition (or state) is well protected. This is measured by asking participants to answer the following questions:

Q1. I believe that cyber insurance policy can add cost to the company's operations' spending.

Q2.I believe that insurance provider does understand our industry and its risks?

Q3.I believe that insurance provider will always look for ways to avoid paying the full damage caused by an attack.

Q4.I believe that cyber insurance should be mandatory for most business.

Q5.insurance provider understands our industry and its risks?

H02: cybersecurity risks have a negative impact on a business revenue.

Loss caused by security incidents and breaches is frequent and widespread. Unauthorised access, theft, and data compromise can impact a business in many different ways, including the loss of profits and customers (which also means loss of money). So, depending on how tense a security incident or breach is, it can impact much more than short-term earnings. The long-term reputation of the organization can be at stake as well. This is measured by asking participants to answer the following questions”

Q6.I believe that the security risks are causing business to spend more than they should to protect their information assets

Q7.My company is taking the measures needed to deal with cyber risks to reduce the loss of profits

Q8.I believe that the customers will not do business with a company that has high cybersecurity risks

H03: Cyber insurance has a positive impact on the cybersecurity risks.

Cybersecurity insurance protects businesses from internet-based risks. So, considering the broader picture and taking everything into account, risks relating to information technology activities resulting in financial losses are also covered. This means that organizations will be protected from threats arising from unintended cyber incidents, errors, or accidental privacy violations. This is measured by asking participants to answer the following questions”

Q9.I believe that cyber insurance can reduce my company's security risks.

Q10.I believe that cyber insurance should to be integrated into security risks management process

Q11.I believe that having a framework can further enhance managing security risks?

H04: Cyber insurance coverage has a positive impact on a business revenue

Nowadays, businesses no longer rely on information technology to run the business. In fact, there is a rise in "digital empowerment", which introduces higher risks and threats that, in some cases, can result in the loss of a large amount of money. Having cyber insurance can be an essential factor in recovering these losses because cybersecurity insurance provides a financial safeguard against a wide range of security incidents and attacks. This is measured by asking participants to answer the following questions:

Q12. I believe that cyber insurance can reduce the risks of money loss not covered by liability coverage

Q13. I believe that cyber insurance can reduce the risks of money loss a

Q14. I believe that cyber insurance can improve business revenue by covering for losses due to attacks

H05: Security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance

Cyber-attacks are a significant threat to the system and functionality of an

organization, but when critical infrastructure fails due to other causes of a cyber-attack, the effects can be wide-reaching and devastating. As infrastructure becomes increasingly reliant on connectivity, a system failure that disrupts business operations will cost the organization time and money. This is measured by asking participants to answer the following questions:

Q15. I believe that Infrastructure failures is an important security risk to be mitigated

Q16. I believe that cyber insurance can help reduce the risks not associated with cyber-attack

H06: The perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance

An organization needs to protect all the digital information that the organization creates and stores because a security incident or an attack would cause an organization financial loss in terms of theft of money or profit loss due to disruption of operations, where such incidents or attacks could result in damage to the reputation of the business, or even worse, where it could cause damage to other companies like business partners or suppliers that the business is relying on to do business. Cyber insurance may cover these losses, not only the ones encountered immediately but also the ones after the interruptions, where some cybersecurity insurance policies can cover the increased costs to business operations caused by a security incident or a security attack. This is measured by asking participants to answer the following questions:

Q17. I believe that cyber insurance can help my company to recover after a security breach

Q18. I believe that cyber insurance will cover losses due to all types of security incidents and attacks

Q19. I believe that cyber insurance can make up for cyber incident losses

Q20. I believe that cyber insurance policy can help you gain promising business

Q21. I believe that cyber insurance should be flexible enough to suit the needs of any business.

Q22. I believe that cyber insurance can help gaining more business opportunity

Q23. I believe that cyber insurance can be considered as best practice for business continuity

H07: Security awareness has a positive impact on managers attitudes towards utilizing security insurance

Being aware of the current security threats can result in a good practice on what an organization may need to do to reduce the security risk identified or the anticipated security threat and security incidents. Security threat awareness helps management understand proper security deployment as well as enhanced methods that can result in managing and reducing these identified risks. The reality of this is that these types of attacks are increased in frequency and severity, and thus the risks are becoming higher. So, being aware of what threats the organization faces, managers can benefit from using cybersecurity insurance to recoup losses related to cybersecurity incidents and attacks. This is measured by asking participants to answer the following questions:

Q25. I believe that cyber insurance can help improve risk management

Q26. Based on the current security threats, I would recommend a cyber in-

insurance for any organization

Q27. Cyber insurance can make up for losses caused by unrelated cyber-attacks

The key intention of this paper is to investigate the degree to which various cybersecurity insurance factors impact cybersecurity risk would influence organizations to engage in using cybersecurity insurance and integrate that with their cybersecurity risk assessment, and thus, incorporate that into the overall risk management program. A survey instrument in the form of a questionnaire was developed. The questions were constructed in the questionnaire based on the research objectives. A convenience sampling method was used. According to Qualtrics (2022), it is a sampling type that involves the sample of accessible subjects that are available to participate in the research study, know about the topic being studied, and are willing to participate. There are two reasons for using this sampling type. First, it provides means for easily obtaining the raw data for further analysis. Second, only contacting participants with knowledge about the topic under study would ensure that the collected data is based on practical knowledge and not based on the participants' opinions. However, the respondents were randomly selected from the different Bahraini business organizations. The Scale items of the instrument are shown in Table 3.1.

Table 3.1: Scale items of the survey instrument

Variable	Scale item Statements
Attitude Towards Cyber Insurance	I believe that cyber insurance policy can add cost to the company's operations' spending
	I believe that insurance provider does understand our industry and its risks?
	I believe that insurance provider will always look for ways to avoid paying the full damage caused by an attack
	I believe that cyber insurance should be mandatory for most business
	insurance provider understands our industry and its risks?
Risks Impact on Revenue	I believe that the security risks are causing business to spend more than they should to protect their information assets
	My company is taking the measures needed to deal with cyber risks to reduce the loss of profits
	I believe that the customers will not do business with a company that has high cybersecurity risks
Insurance Impact on Security Risks	I believe that cyber insurance can reduce my company's security risks.
	I believe that cyber insurance should to be integrated into security risks management process
	I believe that having a framework can further enhance managing security risks?
Insurance Impact on Revenue	I believe that cyber insurance can reduce the risks of money loss not covered by liability coverage
	I believe that cyber insurance can reduce the risks of money loss
	I believe that cyber insurance can improve business revenue by covering for losses due to attacks
Insurance Impact on Infrastructure Failure Risk	I believe that Infrastructure failures is an important security risk to be mitigated
	I believe that cyber insurance can help reduce the risks not associated with cyber-attack
Perceived Benefits Impact on Attitudes	I believe that cyber insurance can help my company to recover after a security breach
	I believe that cyber insurance will cover losses due to all types of security incidents and attacks
	I believe that cyber insurance can make up for cyber incident losses
	I believe that cyber insurance policy can help you gain promising business
	I believe that cyber insurance should be flexible enough to suit the needs of any business.
	I believe that cyber insurance can help gaining more business opportunity
	I believe that cyber insurance can be considered as best practice for business continuity
Awareness Impact on Attitudes	I am aware of the benefits that cyber insurance policy can present to our company.
	I believe that cyber insurance can help improve risk management
	Based on the current security threats I would recommend a cyber insurance for any organization
	Cyber insurance can make up for losses caused by unrelated cyber-attacks

Pilot Test

Pilot testing took place in two stages. The first stage consisted of developing and testing the terms used in the instrument as well as the instructions on how to use the instrument and asking participants to complete the survey. The third and final stage was to test the reliability of the instrument.

Stage 1:

A group of 3 professionals were asked to review the wording to ensure clarity. This review resulted in minor wording changes. After the changes were

made, the instrument was presented to a group of bank employees. Informal interviews were held with three participants; one of them was a manager. Participants identified problems with the format of the instrument items and their associated scales. For example, using a scale from one to five and only identifying “1” as “Extremely Disagree” and “5” as “Extremely Agree” was not clear enough to some participants. One of the participants, in each answer, selected a number and circled “extremely disagree” or “extremely agree”. In several answers, that participant selected number 5 and circled “extremely disagree”, which was a complete contradiction. When asked about that, the participant explained that the numbers were selected to indicate the level of disagreement. Based on these comments, the instrument format was changed so that numbers 2 through 4 were also paired with text as indicated in Appendix. No content changes were made to any items.

Stage 2:

In order to test the internal consistency and reliability, the pilot test included a stage to calculate the internal consistency reliability coefficient. The 27 items of the instrument have been thoroughly tested, as shown in Table 3.2

Table 3.2: Reliability Analysis

Variable	Corresponding Values
Total Number of Items	27
Number of Cases	40
Confidence Interval	95%
Correlation between forms	0.754
Guttman Split-half	0.8327
Spearman-Brown Equal-length	0.8598
Spearman-Brown Unqual-length	0.8599

The instruments' constructs Cronbach's alpha reliability coefficients were also calculated. The calculations were done in several steps. The first step was calculating the Cronbach's alpha for the instrument. The results are illustrated in Table 3.3. The fourth and final step was calculating the Cronbach's alpha reliability coefficients for each independent variable of the instrument. The Cronbach's alpha reliability coefficient calculation shows that all constructs maintain internal consistency reliability. It was found that all scales were above 0.80 as shown in Table 3.3

Table 3.3: Instrument's Constructs Cronbach Alpha Reliability coefficients at 95% coefficient Level

Variables	Number of items	Number of cases	P value	Cronbach's alpha
Attitude Towards Cyber Insurance	5	40	<0.001	0.849
Risks Impact on Revenue	3	40	<0.001	0.9742
Insurance Impact on Security Risks	3	40	<0.001	0.8716
Insurance Impact on Revenue	3	40	<0.001	0.9525
Insurance Impact Infrastructure Failure Risk	2	40	<0.001	0.9499
Perceived Benefits Impact on Attitudes	7	40	<0.001	0.8618
Awareness Impact on Attitudes	4	40	<0.001	0.9281

In multiple regression results, a value R of 1 indicates that the dependent variable can be perfectly predicted from the independent variables. A value close to 0 indicates that the independent variables are not linearly related to the dependent variable. The R^2 value explains the observed variability of adoption. Thus, R and R^2 were calculated. The calculations supported the notion that the dependent variable can be perfectly predicted from the independent variables (see Table 3.4).

To further ensure the reliability of the instrument, factor analysis was done using the principal components method of analysis with a varimax rotation applied to the data (see Table 3.5).

Table 3.4: Internal Consistency Reliability for Constructs at 95% coefficient Level and P
 ≤ 0.0001

Construct Name	Item	Inter-item correlation					R	R2
Attitude Towards Cyber Insurance	Q1	1					0.6478	0.4196
	Q2	0.8485	1					
	Q3	0.8508	0.9188	1				
	Q4	0.8956	0.91	0.8794	1			
	Q5	0.9111	0.8661	0.8661	0.9213	1		
Risks Impact on Revenue	Q6	1					0.6201	0.3845
	Q7	0.5975	1					
	Q8	0.6465	0.8318	1				
Insurance Impact on Security Risks	Q9	1					0.8093	0.655
	Q10	0.8270	1					
	Q11	0.8549	0.8698	1				
	Q12	1					0.8457	0.7152
Insurance Impact on Revenue	Q13	0.8905	1					
	Q14	0.8931	0.8628	1				
Insurance Impact Infrastructure Failure Risk	Q15	1					0.7581	0.5747
	Q16	0.7581	1					
Perceived Benefits Impact on Attitudes	Q17	1					0.8682	0.7538
	Q18	0.8682	1					
	Q19	0.5894	0.5492	1				
	Q20	0.87142	0.88543	0.85566	1			
	Q21	0.8865	0.84272	0.84272	0.89642	1		
	Q22	0.86256	0.81996	0.81996	0.87222	0.67079	1	
	Q23	0.84789	0.86152	0.83255	0.84789	0.86152	0.83255	1
Awareness Impact on Attitudes	Q24	0.7181	1				0.8226	0.6766
	Q25	0.5894	0.5492	1				
	Q26	0.86963	0.88361	0.8539	1			
	Q27	0.88468	0.84098	0.84098	0.89458	1		

Table 3.5: Table 3.5: Factor Analysis of the Instrument

Factor	F1	F2	F3	F4	F5	F6	F7
Q1	0.9294	-0.0898	0.0019	0.0067	0.0864	-0.042	0.1397
Q2	0.9083	0.1824	-0.1354	-0.1176	0.0357	-0.0725	0.0005
Q3	0.8047	0.3023	0.214	0.1577	0.0846	0.1973	0.0591
Q4	0.8791	0.2872	0.1348	0.0749	0.0822	0.1138	0.1067
Q5	0.9099	0.1835	0.1041	0.016	0.131	0.1334	0.0254
Q6	0.2346	0.2973	-0.0311	0.8525	0.0885	0.098	0.1827
Q7	0.3518	0.1989	0.0775	0.802	0.0312	0.2646	0.076
Q8	-0.0932	0.0332	0.1183	0.8456	-0.1324	0.1455	-0.0665
Q9	0.0678	0.0711	0.7443	-0.0219	0.0839	-0.1438	-0.0125
Q10	0.2168	0.099	0.7612	0.9113	0.0976	0.0291	0.0643
Q11	0.5305	0.3717	0.7165	0.1276	-0.0508	0.1033	0.2092
Q12	0.2666	0.8508	-0.0386	0.0434	0.0071	0.1556	0.2246
Q13	0.492	0.8945	0.185454	-0.0709	-0.0136	0.1491	0.0302
Q14	0.4283	0.7482	0.278989	0.1079	-0.0013	0.0058	0.1573
Q15	0.3709	0.3838	0.1838	0.0436	0.7126	-0.04	0.1109
Q16	0.4036	0.2131	0.2765	0.0219	0.7568	0.0245	0.1833
Q17	0.5084	0.2762	0.2363	0.162	-0.0201	0.0974	0.8393
Q18	0.3045	0.238427	0.1607	0.1307	0.1699	0.097	0.8005
Q19	0.1971	0.1887	0.0815	-0.0367	0.0526	-0.2527	0.8687
Q20	0.0913	0.0059	0.1708	0.0099	-0.0563	0.0672	0.9297
Q21	0.267	0.1834	0.1957	-0.0113	-0.0022	0.0277	0.8816
Q22	0.2511	0.1472	0.254	-0.0939	0.0445	0.1266	0.8664
Q23	0.0414	-0.0337	0.0083	0.016	0.3061	0.091952	0.7024
Q24	0.1087	0.1356	0.0556	-0.0258	-0.0156	0.8834	-0.0397
Q25	0.2315	0.2664	-0.3771	0.1772	0.3193	0.7198	-0.1647
Q26	0.2577	0.1777	0.1145	0.16215	0.2229	0.8518	-0.0287
Q27	0.2459	-0.0583	0.0772	0.0189	0.1547	0.905	-0.1113

Extraction Method:Principal Component Analysis — Rotation Method:Varimax with Kaiser Normalization.

Chapter Four

Results and Discussion

4.1 Overview

4.2 Discussion

4.3 Conclusion

Chapter 4

Results and Discussion

4.1 Overview

The vast majority of the study sample constitutes 126(74.6%), representing students with an educational level of four years of college. Around half of the study's sample has an average level regarding their security awareness skill and understanding of cybersecurity insurance, 81(47.9%) and 79(46.7), respectively. Additionally, 72(42.6%) of participants have an average level of understanding of cybersecurity risk, and 66(39.1%) are involved in cybersecurity risk assessment. Finally, the descriptive statistics show that 59(34.9%) of participants have an average level of involvement in cybersecurity planning. Table (4.1) summarizes sample characteristics.

Table 4.1: Study sample characteristics

Variables	Frequency	Percentage%	Mean $\pm$ SD
What is the highest level of formal education you have completed?			
- 2 Years college	11	6.5	
- 4 Years college	126	74.6	
- Master's degree	32	18.9	
Please rate your skill level Security Awareness.			
- Low	4	2.4	
- Less than average	20	11.8	
- Average	81	47.9	3.38 $\pm$ 0.98
- Better than average	36	21.3	
- High	28	16.3	
Please rate your skill level of understanding cybersecurity Risk.			
- Low	7	4.1	
- Less than average	31	18.3	
- Average	72	42.6	3.25 $\pm$ 1.07
- Better than average	30	17.8	
- High	29	17.2	
Please rate your skill level of understanding cybersecurity Insurance.			
- Low			
- Less than average	21	12.4	
- Average	37	21.9	2.79 $\pm$ 1.03
- Better than average	79	46.7	
- High	21	12.4	
	11	6.5	
Please rate your level of involvement in cybersecurity Risk Assessment.			
- Low	26	15.4	
- Less than average	34	20.1	
- Average	66	39.1	2.88 $\pm$ 1.21
- Better than average	20	11.8	
- High	23	13.6	
Please rate your level of involvement in cybersecurity Planning.			
- Low	33	19.5	
- Less than average	37	21.9	
- Average	59	34.9	2.76 $\pm$ 1.26
- Better than average	17	10.1	
- High	23	13.6	

Hypothesis testing:

This part provides test results for the study's research hypotheses that were tested by utilizing a one-sample t-test to investigate how cyber insurance would have an impact on cybersecurity risk. The upcoming tables show Mean $\pm$ SD, the proportional weight of participants' response, item rank, t-value and significant value for testing item mean opposed to hypothetical mean, which is assumed by (3).

Ha1: Management of organizations have a positive attitude towards cyber insurance.

This part is composed of five questions to study if the management of organizations has a positive attitude towards cyber insurance and the result presented in table (4.2.1) showed that item number (4), which states, "I believe that cyber insurance should be mandatory for most business" has the highest mean (3.42 $\pm$ 0.88). In contrast, item number (3), which states, "I believe that an insurance provider will always look for ways to avoid paying the full damage caused by an attack", has the lowest mean (2.56 $\pm$ 0.89). In order to test the first research hypothesis, the results show that the mean score of the entire section was (3.01 $\pm$ 0.38), which is not statistically significantly different from the hypothetical mean-t(168)=0.447, p=0.328 with 60.2% of participants have agreed that the management of organizations has a positive attitude towards cyber insurance.

Table 4.2: one sample t test results for management of organizations have a positive attitude towards cyber insurance

No	Question	Mean	SD	T value	Proportional weight %	Rank	p-value
1	I believe that cyber insurance policy add cost to the company's operations' spending	2.67	0.81	5.289	53.4	4	<0.001
2	I believe that insurance provider does understand our industry and its risks?	3.21	0.73	3.683	64.2	2	<0.001
3	I believe that insurance provider will always look for ways to avoid paying the full damage caused by an attack	2.56	0.89	6.467	51.2	5	<0.001
4	I believe that cyber insurance should be mandatory for most business	3.42	0.88	6.229	68.4	1	<0.001
5	Insurance provider understands our industry and its risks?	3.21	0.8	3.484	64.2	3	<0.001
	Total mean score	3.01	0.38	0.447	60.2	–	0.328

Ha2: cybersecurity risks have a negative impact on business revenue

This part is composed of three questions to study if cybersecurity risks have a negative impact on business revenue, and the results in Table (4.3) showed that item number (8), which states, "I believe that the customers will not do business with a company that has high cybersecurity risks " has the highest mean (3.66 ± 0.93) while item number (6) which states "I believe that the security risks are causing the business to spend more than they should to protect their information assets " has the lowest mean (2.73 ± 0.86). In order to test the second research hypothesis, the results show that the mean score of the total section was (3.30 ± 0.52), which is statistically significantly higher than the hypothetical mean- $t(168)=7.473, p<0.001$ with 66.0% of participants have agreed that the cybersecurity risks have a negative impact on business revenue; thus the alternative research hypothesis is accepted.

Table 4.3: one sample t test results for cybersecurity risks have a negative impact on business revenue

No	Question	Mean	SD	T value	Proportional weight %	Rank	p-value
6	I believe that the security risks are causing business to spend more than they should to protect their information assets	2.73	0.86	4.094	54.6	3	<0.001
7	My company is taking the measures needed to deal with cyber risks to reduce the loss of profits	3.51	0.90	7.346	70.2	2	<0.001
8	I believe that the customers will not do business with a company that has high cybersecurity risks	3.66	0.93	9.313	73.2	1	<0.001
	Total mean score	3.30	0.52	7.473	66.0	–	<0.001

Ha3: Cyber insurance has a positive impact on the cybersecurity risks.

This part is composed of three questions to study if cyber insurance has a positive impact on the cybersecurity risks, and the results in Table (4.4) showed that item number (11), which states, "I believe that having a framework can further enhance managing security risks" has the highest mean (3.70 ± 0.75) while item number (9) which states, "I believe that cyber insurance can reduce my company's security risks" has the lowest mean (3.43 ± 0.82). In order to test the third research hypothesis, the results show that the mean score of the total section was (3.58 ± 0.58), which is statistically significantly higher than the hypothetical mean- $t(168)=13.023, p<0.001$ with 71.6% of participants have agreed that the cyber insurance has a positive impact on the cybersecurity risks. Thus, the alternative research hypothesis is accepted

Table 4.4: one sample t test results for cyber insurance has a positive impact on the cyber-security risks

No	Question	Mean	SD	T value	Proportional weight %	Rank	p-value
9	I believe that cyber insurance can reduce my company's security risks.	3.43	0.82	6.833	68.6	3	<0.001
10	I believe that cyber insurance should to be integrated into security risks management process	3.62	0.70	11.451	72.4	2	<0.001
11	I believe that having a framework can further enhance managing security risks?	3.70	0.75	12.160	74.0	1	<0.001
	Total mean score	3.58	0.58	13.023	71.6	–	<0.001

Ha4: Cyber insurance coverage has a positive impact on business revenue

This part is composed of three questions to study if cyber insurance coverage has a positive impact on business revenue, and the results in Table (4.5) showed that item number (12), which states, "I believe that cyber insurance can reduce the risks of money loss not covered by liability coverage" has the highest mean (3.53 ± 0.66), while item number (14) which states, "I believe that cyber insurance can improve business revenue by covering for losses due to attacks" has the lowest mean (3.47 ± 0.76). In order to test the fourth research hypothesis, the results show that the mean score of the total section was (3.51 ± 0.56), which is statistically significantly higher than the hypothetical mean- $t(168)=11.767, p<0.001$ with 70.2% of participants have agreed that the cyber insurance coverage has a positive impact on business revenue. Thus, the alternative research hypothesis is accepted.

Table 4.5: one sample t test results for cyber insurance coverage has a positive impact on business revenue

No	Question	Mean	SD	T value	Proportional weight %	Rank	p-value
12	I believe that cyber insurance can reduce the risks of money loss not covered by liability coverage	3.53	0.66	10.306	70.6	1	<0.001
13	I believe that cyber insurance can reduce the risks of money loss	3.52	0.71	9.563	70.4	2	<0.001
14	I believe that cyber insurance can improve business revenue by covering for losses due to attacks	3.47	0.76	8.052	69.4	3	<0.001
	Total mean score	3.51	0.56	11.767	70.2	–	<0.001

Ha5: Security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance.

This part is composed of two items to study whether cybersecurity insurance positively impacts security risks unrelated to cyber-attack and infrastructure failures. The results in Table(4.6) showed that item number (15), which states, "I believe that Infrastructure failures are an important security risk to be mitigated", have the highest mean (3.64 ± 0.76). In contrast, item number (16), which states, "I believe that cyber insurance can help reduce the risks not associated with cyber-attack", have the lowest mean (3.24 ± 0.78). In order to test the fifth research hypothesis, the results show that the mean score of the entire section was (3.44 ± 0.58) which is statistically significantly higher than hypothetical mean- $t(168)=9.886, p<0.001$ with 68.8% of participants have agreed that the security risk unrelated to cyber-attack and infrastructure failures are positively impacted by cybersecurity insurance. Thus, the alternative research hypothesis is accepted.

Table 4.6: one sample t test results for security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance

No	Items	Mean	SD	T value	Proportional weight %	Rank	p-value
15	I believe that Infrastructure failures is an important security risk to be mitigated	3.64	0.76	11.052	72.8	1	<0.001
16	I believe that cyber insurance can help reduce the risks not associated with cyber-attack	3.24	0.78	4.027	64.8	2	<0.001
	Total mean score	3.44	0.58	9.886	68.8	–	<0.001

Ha6: The perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance.

This part is composed of seven items to study if the perceived benefits of cybersecurity insurance have a positive impact on managers' attitudes towards utilizing security insurance. The results in Table (4.7) showed that item number (21), which states, "I believe that cyber insurance should be flexible enough to suit the needs of any business", have the highest mean (3.56 ± 0.82). In contrast, item number (18), which states, "I believe that cyber insurance will cover losses due to all types of security incidents and attacks", have the lowest mean (2.85 ± 0.89). In order to test the sixth research hypothesis, the results show that the mean score of the total section was (3.33 ± 0.43), which is statistically significantly higher than the hypothetical mean- $t(168)=10.015, p<0.001$ with 66.6% of participants have agreed that the perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance. Thus, the alternative research hypothesis is accepted.

Table 4.7: one sample t test results for the perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance

No	Items	Mean	SD	T value	Proportional weight %	Rank	p-value
17	I believe that cyber insurance can help my company to recover after a security breach	3.41	0.79	6.719	68.2	2	<0.001
18	I believe that cyber insurance will cover loses due to all types of security incidents and attacks	2.85	0.89	2.159	57.0	7	0.016
19	I believe that cyber insurance can make up for cyber incident loses	3.30	0.78	5.044	66.0	6	<0.001
20	I believe that cyber insurance policy can help you gain promising business	3.37	0.79	6.025	67.4	5	<0.001
21	I believe that cyber insurance should be flexible enough to suit the needs of any business.	3.56	0.82	8.887	71.2	1	<0.001
22	I believe that cyber insurance can help gaining more business opportunity	3.40	0.73	7.103	68.0	4	<0.001
23	I believe that cyber insurance can be considered as best practice for business continuity	3.41	0.83	6.508	68.2	3	<0.001
	Total mean score	3.33	0.43	10.015	66.6	–	<0.001

Ha7: Security awareness has a positive impact on manager’s attitudes towards utilizing security insurance.

This part is composed of four items to study if security awareness has a positive impact on managers’ attitudes towards utilising security insurance, and the results in Table (4.8) showed that item number (25), which states, ”I believe that cyber insurance can help improve risk management ” has the highest mean (3.54 ± 0.76) while item number (4) which states ”cyber insurance can make up for loses caused by unrelated cyber-attacks” has the lowest mean (2.88 ± 0.82). In order to test the seventh research hypothesis, the results show that the mean score of the total section was (3.36 ± 0.48), which is statistically significantly higher than the hypothetical mean- $t(168)=11.767, p<0.001$ with 67.2% of participants have agreed that the security awareness has a positive impact on manager’s attitudes towards

utilizing security insurance. Thus, the alternative research hypothesis is accepted.

Table 4.8: one sample t test results for security awareness has a positive impact on manager's attitudes towards utilizing security insurance

No	Items	Mean	SD	T value	Proportional weight %	Rank	p-value
24	I am aware of the benefits that cyber insurance policy can present to our company.	3.50	0.76	8.638	70.0	2	<0.001
25	I believe that cyber insurance can help improve risk management	3.54	0.76	9.270	70.8	1	<0.001
26	Based on the current security threats I would recommend a cyber-insurance for any organization	3.50	0.82	7.999	70.0	3	<0.001
27	Cyber insurance can make up for loses caused by unrelated cyber-attacks	2.88	0.82	1.871	57.6	4	0.032
	Total mean score	3.36	0.48	9.742	67.2	–	<0.001

Table 4.9 shows the results of the hypothesis developed in this study. Two hypotheses were retained, and five hypotheses were accepted. The majority of the study indicated that cyber insurance could be a great add-on to any organization to secure its financial stability.

Table 4.9: Hypothesis Results

Hypothesis	Mean±SD	P-value	Decisions
Ha1: Management of organizations have a positive attitude towards cyber insurance.	3.01±0.38	0.328	Alternative hypothesis retained
Ha2: cybersecurity risks have a negative impact on business revenue	3.30±0.52	<0.001	Alternative hypothesis accepted
Ha3: Cyber insurance has a positive impact on the cybersecurity risks.	3.58±0.58	<0.001	Alternative hypothesis accepted
Ha4: Cyber insurance coverage has a positive impact on business revenue	3.51±0.56	<0.001	Alternative hypothesis accepted
Ha5: Security risk unrelated to cyber-attack and Infrastructure failures are positively impacted by cybersecurity insurance.	3.44±0.58	<0.001	Alternative hypothesis accepted
Ha6: The perceived benefits of cybersecurity insurance have a positive impact on managers attitudes towards utilizing security insurance.	3.33±0.43	<0.001	Alternative hypothesis accepted
Ha7: Security awareness has a positive impact on manager's attitudes towards utilizing security insurance.	3.36±0.48	<0.001	Alternative hypothesis accepted

4.2 Discussion

The collected and analysed data clearly shows that while management of organizations has a positive attitude towards cyber insurance, it is all driven by security awareness and how cybersecurity risks can have a negative impact on business revenue. Businesses are to make money, so reducing the security risks that impact the business revenue negatively is a goal for management. Understanding the benefits of cyber insurance on security risk is found to have a positive impact on managers' attitudes towards utilizing security insurance. Management of organizations has to also realize the benefits of cybersecurity insurance in order to take the step of deciding to utilize cyber insurance and enhance the cybersecurity risks.

4.3 Conclusion

Cyber insurance can be costly; however, the significant benefits it provides are what every organization is looking for. This year, most of the Gulf countries' insurance companies have recently launched their cyber insurance programs. Most of these insurance policies cover a majority of the checklist.

Chapter Five

Conclusion and Recommendations

5.1 Summary

5.1.1 Recommendations when using cyber insurance

5.1.2 Contribution

5.1.3 Limitation

Chapter 5

Conclusion and Recommendations

5.1 Summary

This research intended to provide an answer to whether cyber risk insurance could play a significant role in reducing cybersecurity risks. This research indicated that institutions and firms that aim to be prosperous and successful in their professions are demanded to look for various ways to reduce cybersecurity risks. The collected and analysed data shows that cybersecurity insurance is one of these options that can be taken to reduce the cybersecurity risks and bring them down to an acceptable level. With cyber risk insurance and the compliance of its rules and policies, companies can continue with their progression and advancement in their businesses with less risk to worry about. One reason for this is that cyber risk insurance covers the costs of loss of data, information, monetary amounts, and every other matter and concept endured in the process of being exposed to one form of the many cybersecurity risks.

The research findings clearly show that managers have a positive attitude towards cyber insurance, but the steps to be taken are mainly driven by security awareness and the impact of cybersecurity risks on business revenue. The main goal is to reduce the security risks and reduce their effects on the business revenue. This research has shown the benefits that cyber insurance can achieve in terms of reducing security risks.

It has been shown that the attacks on the organizations are becoming more and more sophisticated. Despite having a secure infrastructure, the risks still exist; thus, having a policy can protect you from a threat that may occur in the future, which can be considered an advantage. This research idea of applying cyber insurance can result in a solid and extended continuity plan. The key intention of cyber insurance is to have a safeguard in place in case of any disaster that may occur. Furtherly, in order for organizations to run a successful business, managers shall look through the broader picture and take all the threats and risks into account, especially in the new era of business that depends on digital transformation. As with digitalization, more risks and threats were introduced that did not exist and were not foreseen in the known cybersecurity picture. However, having an extra safeguard layer of cyber insurance policy can decrease financial loss. While privacy is becoming an issue, especially after introducing laws that protect customers' data and violating rules of these laws can result in many lawsuits, cyber insurance can play a factor in protecting the customers' data and cover any lawsuits that the organization is going to face in case of a privacy breach. Finally, ransomware attacks can be unpredictable, mainly because any organization depending on technology can get hit by ransomware attacks, and that is not because security was not in place or because they did not apply security measures. Most ransomware attacks target large software compa-

nies' glitches, which can be found in any updates to their software, but with the right insurance policy, the organization can be saved from any related ransomware attacks.

5.1.1 Recommendations when using cyber insurance

When assessing cyber risks, an organization should keep in mind that cyber threats are continuously changing, increasing uncertainties. Cyber insurance, in general, covers specific cyber-attacks. So, an organization must demonstrate a complete understanding of the cyber events the cyber insurance policy intends to protect against. For optimum cyber security risk mitigation, an organization should include a cyber insurance strategy within its risk management program. For optimum outcome, the option to get a cyber insurance policy should be based on the worst-case scenario.

5.1.2 Contribution

The study tests the willingness to adopt cyber insurance as an added advantage for the organization itself. There is a wide need of this study findings, specially the survey from professional in the fields about accepting to implement cyber insurance policy and what the benefits that can add up specially during sophisticated cyberattacks. The study also addressed something not known by public, specially in Bahrain, regarding Cyber Insurance policy.

5.1.3 Limitation

This Thesis suffered from several limitations, which will be discussed further. However, from the authors' point of view, they are considered to be few and not prominent. Firstly, as the Thesis contained mixed research methods, the author conducted interviews as part of the qualitative method used.

The author had only interviewed eight respondents, which, to some extent, makes it hard to generalize the findings. However, according to (Boddy, 2016), deciding the required sample size is partially dependent upon which scientific paradigm the research is taking place and is considered contextual. Since this Thesis is focused on the impacts of a specific project (cybersecurity insurance) on a specific matter (cybersecurity risks), and the interviewed personnel were seniors with respectable experience in their field, it is fair to say that a representative picture can be gained (Boddy, 2016). According to the mentioned paper, even a sample of 12 in a homogeneous population can also be useful.

Nonetheless, the author would like to mention another limitation. Secondly, the Thesis neglected to mention an important pillar of risk management. Since this Thesis is focused on managing cyber risks in organizations, the author did not discuss cyber risk appetite, as it is a fundamental pillar in risk management and the way organizations react and respond to risks. Cyber risk appetite is considered as one of the most powerful tools to help organizations prioritize investments in cybersecurity, which is cybersecurity insurance in this Thesis. However, the author had discussed the impacts of risks on the organizations' revenue but did not explicitly mention statements of risk appetite, such as if a certain organization states that it does not want to accept risks that might have a slight chance of negatively impacting its revenue.

Finally, the author of this Thesis believes that the aforementioned points could have empowered the research more if more respondents were included, for example, in terms of data generalization and publicity. It would also grasp a more comprehensive understanding of risk management if risk appetite was further discussed because it helps in creating awareness of cy-

ber risks and risk management decisions.

References

- Ahmad, T. (2020). Corona virus (covid-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3568830
- Andrade, R. O., Ortiz-Garces, I., & Cazares, M. (2020). Cybersecurity attacks on smart home during covid-19 pandemic. *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*. doi: 10.1109/worlds450073.2020.9210363
- Armstrong, D. (2021). Cyber extortion. *Cyber Risks and Insurance: The Legal Principles*. doi: 10.5040/9781526514165.chapter-005
- Blobel, B. (2018). Data protection and data security in shared care information systems. *Recent Health Policy Innovations in Social Security*, 301–334. doi: 10.4324/9781351307444-20
- Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal*, 19(4), 426–432. doi: 10.1108/qmr-06-2016-0053
- Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, 2(1), 53–63. doi: 10.1080/23738871.2017.1296878
- Franke, U. (2017). The cyber insurance market in sweden. *Computers and Security*, 68, 130–144. doi: 10.1016/j.cose.2017.04.010
- Gralla, P. (2002). Electronic safety net: Cyberinsurance policies can offer protection when technology fails. *EDPACS*, 29(9), 15–16. doi: 10.1201/1079/43281.29.9.20020304/35217.6

- Havakhor, T., Rahman, M. S., & Zhang, T. (2020). Cybersecurity investments and the cost of capital. *SSRN Electron. J.*
- Jalali, M., Landman, A., & Gordon, W. (2020). Telemedicine, privacy, and information security in the age of covid-19. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3646320
- Kaiser, F. K., Wiens, M., & Schultmann, F. (2021). Use of digital health-care solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the covid-19 pandemic. *Health and Technology*, 11(5), 1125–1137.
- Khalili, M. M., Naghizadeh, P., & Liu, M. (2018). Designing cyber insurance policies: The role of pre-screening and security interdependence. *IEEE Transactions on Information Forensics and Security*, 13(9), 2226–2239. doi: 10.1109/tifs.2018.2812205
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers amp; Security*, 105, 102248. doi: 10.1016/j.cose.2021.102248
- Mendes-Da-Silva, W., Lucas, E. C., & de França Carvalho, J. V. (2021). Flood insurance: The propensity and attitudes of informed people with disabilities towards risk. *Journal of environmental management*, 294, 113032.
- Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2017). Cyber risk assessment and mitigation (cram) framework using logit and probit models for cyber insurance. *Information Systems Frontiers*, 21(5), 997–1018. doi: 10.1007/s10796-017-9808-5
- Okereafor, K. (2021). Challenges of managing cybersecurity at covid-19. *Cybersecurity in the COVID-19 Pandemic*, 103–118. doi:

10.1201/9781003104124-5

- Paat, Y.-F., & Markham, C. (2021). Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, 19(1), 18–40.
- Palmer, D. (2021, Mar). *What is cyber insurance? everything you need to know about what it covers and how it works*. ZDNet.
- Panda, S., Farao, A., Panaousis, E., & Xenakis, C. (2021). Cyber-insurance: Past, present and future. *Encyclopedia of Cryptography, Security and Privacy*, 1–4. doi: 10.1007/978-3-642-27739-9_1624 – 1
- Priyadarshini, I., & Cotton, C. (2022). Cyber risks and cyber insurance. *Cybersecurity*, 307–328. doi: 10.1201/9781003187127-9
- Rajaram, P., Goh, M., & Zhou, J. (2022). Guidelines for cyber risk management in shipboard operational technology systems. *arXiv preprint arXiv:2203.04072*.
- Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). Content analysis of cyber insurance policies: How do carriers write policies and price cyber risk? doi: 10.7249/wr1208
- Sardi, A., Rizzi, A., Sorano, E., & Guerrieri, A. (2020). Cyber risk in health facilities: A systematic literature review. *Sustainability*, 12(17), 7002. doi: 10.3390/su12177002
- Shetty, S., McShane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management†. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 43(2), 224–238. doi: 10.1057/s41288-018-0078-3
- Stine, K., & Barrett, M. (2021). Portuguese translation of the framework for improving critical infrastructure cybersecurity version 1.1 (cybersecurity framework).

doi: 10.6028/nist.cswp.04162018pt

- Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*, 79, 103–114. doi: 10.1016/j.tranpol.2019.04.019
- Weber, J. L. (2018). Corporate social responsibility disclosure level, external assurance and cost of equity capital. *Journal of Financial Reporting and Accounting*, 16(4), 694–724. doi: 10.1108/jfra-12-2017-0112
- Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*, 22(9). doi: 10.2196/23692
- Wister, A. V. (2021). Precarious aging: Covid-19 risk, resilience and response. *COVID-19: Systemic Risk and Resilience*, 141–162. doi: 10.1007/978-3-030-71587-8_9
- Xie, X., Lee, C., & Eling, M. (2020). Cyber insurance offering and performance: An analysis of the u.s. cyber insurance market. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 45(4), 690–736. doi: 10.1057/s41288-020-00176-5

Invitation to Participation in a Research Study

Dear Sir/Mam

This is a request for your participation in a Master Thesis research study at University of Bahrain. The purpose of the research is to evaluate the impact of cyber risk insurance on organization's security risk and investigate the factors that influence IT management decision for utilizing cyber risk insurance in the security management plan. Generally, participation takes about 4 to 6 minutes.

To gather your input and allow statistical analysis of it, you are asked to complete the multiple-choice survey that is posted in the above website. Your participation is entirely voluntary and anonymous. You are under no obligation to participate, although your input would be extremely valuable and appreciated.

Thank you for your consideration. If you have any questions or would like to have a copy of the research when completed, please contact me via email at 20171166@stu.uob.edu.bh.

Sincerely,

Ahmed Ali Hasan Ahmed

This project has been reviewed and approved by The University of Bahrain Committee for postgraduate studies.

Survey Questions

What is the highest level of formal education you have completed?

☐ 2 Years College ☐ 4 Years College ☐ Masters degree ☐ Ph.D. degree

Please rate your skill level Security Awareness.

☐ Low ☐ Less than average ☐ Average ☐ Better than average ☐ High

Please rate your skill level of understanding Cybersecurity Risk.

☐ Low ☐ Less than average ☐ Average ☐ Better than average ☐ High

Please rate your skill level of understanding Cybersecurity Insurance.

☐ Low ☐ Less than average ☐ Average ☐ Better than average ☐ High

Please rate your level of involvement in cybersecurity Risk Assessment.

☐ Low ☐ Less than average ☐ Average ☐ Better than average ☐ High

Please rate your level of involvement in cybersecurity Planning

☐ Low ☐ Less than average ☐ Average ☐ Better than average ☐ High

1. I believe that cyber insurance policy can add cost to the company's operations' spending

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

2. I believe that insurance provider does understand our industry and its risks?

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Ex-

tremally Agree

3. I believe that insurance provider will always look for ways to avoid paying the full damage caused by an attack

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

4. I believe that cyber insurance should be mandatory for most business

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

5. insurance provider understands our industry and its risks?

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

6. I believe that the security risks are causing business to spend more than they should to protect their information assets

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

7. My company is taking the measures needed to deal with cyber risks to reduce the loss of profits

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

8. I believe that the customers will not do business with a company that has high cybersecurity risks

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Ex-

tremally Agree

9. I believe that cyber insurance can reduce my company's security risks.

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

10. I believe that cyber insurance should to be integrated into security risks management process

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

11. I believe that having a framework can further enhance managing security risks?

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

12. I believe that cyber insurance can reduce the risks of money loss not covered by liability coverage

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

13. I believe that cyber insurance can reduce the risks of money loss.

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

14. I believe that cyber insurance can improve business revenue by covering for losses due to attacks

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Ex-

tremally Agree

15. I believe that Infrastructure failures is an important security risk to be mitigated

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

16. I believe that cyber insurance can help reduce the risks not associated with cyber-attack

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

17. I believe that cyber insurance can help my company to recover after a security breach

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

18. I believe that cyber insurance will cover loses due to all types of security incidents and attacks

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

19. I believe that cyber insurance can make up for cyber incident loses

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

20. I believe that cyber insurance policy can help you gain promising business

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

21. I believe that cyber insurance should be flexible enough to suit the needs of any business.

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

22. I believe that cyber insurance can help gaining more business opportunity

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

23. I believe that cyber insurance can be considered as best practice for business continuity

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

24. I am aware of the benefits that cyber insurance policy can present to our company.

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

25. I believe that cyber insurance can help improve risk management

(1) Extremally Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremally Agree

26. Based on the current security threats I would recommend a cyber insur-

ance for any organization

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

27. Cyber insurance can make up for losses caused by unrelated cyber-attacks

(1) Extremely Disagree (2) Disagree (3) Fairly Agree (4) Agree (5) Extremely Agree

Cyber Insurance Process



Figure 5.1: old model proposed

ملخص

في عصر التطور الرقمي، تواجه منظمات الأعمال العديد من المخاطر و التهديدات الأمنية التي تخلفها شبكة الإنترنت وغيرها من الابتكارات التكنولوجية الحديثة. تشهد التكنولوجيا في عالمنا اليوم تطوّر وتقدّم سريع ومستمر، الأمر الذي يحدّ من قدرة الشركات على التحكم في جميع الثغرات الأمنية أو حتّى التخفيف منها. إنّ الهجمات والجرائم الإلكترونية اليوم هي أكثر تعقيداً من السابق، حيث أنّه وفي كثيرٍ من الحالات، تكون هذه الجرائم مُجهّزة بالكامل باستخدام أدوات ذكية مُعدّة خصيصاً لشنّ الهجمات الإلكترونية.

مع جميع هذه المتغيرات والعوامل المعقدة في العالم الرقمي، كيف يمكن لمؤسسات الأعمال أن تستجيب لمخاطر الأمن السيبراني؟

عند الأخذ بالمُعطيات، أصبح الأمن السيبراني أحد مصادر القلق الأساسية لإدارة المؤسسة، حيث من جانبها، أصبح من الضروري وضع خطة لمواجهة وتقليل المخاطر عند حدوث أي كارثة أمنية.

يفترض هذا البحث أن الحلّ المناسب لمساعدة المؤسسات أمام هذا التّحدي هو التأمين الإلكتروني. لتأكيد هذه الفرضية تمّ بكل عناية، تصميم أداة قياس لفحص تأثير التأمين الإلكتروني ضد المخاطر وأثره على الوصول بمخاطر الأمن السيبراني إلى مستوى مقبول.

تمّ جمع البيانات بطرق نوعيّة و كميّة يتكوّن الجزء الكميّ من استبيان مع سؤال مغلق، بينما النوعي كان عبارة عن مقابلات شبه منظمة مع مدراء أعمال رفيعي المستوى. تم استخدام كلتا الطريقتين في التحليل، ونتيجة لذلك، يصبّ العمل الرئيسي لهذا البحث في تحرير نموذج للمخاطر وإضافة التأمين الإلكتروني إليه لتكون النتيجة وجود نموذج فريد يتضمّن على تأمين إلكتروني في خطة المؤسسات لتخفيف المخاطر الأمنية.

بناءً على تحليل البيانات، إذا أظهرت النتائج أن استخدام النموذج المقترح يمكن أن يساعد المؤسسات على الوصول إلى الاستقرار المالي، فإنّ النموذج المقترح يُحبّذ و يجب اعتماده.

من المهم لفت النّظر أيضاً أنّه بسبب وجود العدد الكبير من التطبيقات والأجهزة المستخدمة حالياً، فإن نقاط الضعف والثغرات الأمنية في ازدياد بطريقة تناسبيّة، وبالتالي يجب على مؤسسة الأعمال أن تتأكد من أنها لن تعاني من خسائر مالية غير مؤكدة قد تمنعها من القدرة على مواصلة العمل، وفي هذه الحالة طبعاً، يمكن أن يكون التأمين الإلكتروني أداة قوية لضمان استمرارية العمل.

جامعة البحرين
كلية تقنية المعلومات



دراسة أثر التأمين الإلكتروني
في التقليل من مخاطر الأمن السيبراني
أطروحة مقدمة كجزء من متطلبات الحصول على
درجة الماجستير في الأمن السيبراني

إعداد

أحمد علي حسن أحمد

٢٠١٢١١٦٦

إشراف

د. زكريا عيسى

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين

يونيو ٢٠٢٢