

**ATTITUDES OF EMPLOYEES TOWARDS
CYBERSECURITY**

**A THESIS SUBMITTED TO THE GRADUATE
SCHOOL OF APPLIED SCIENCES
OF
NEAR EAST UNIVERSITY**

**By
MOHAMED S. SALHEIN ELBELEKIA**

**In Partial Fulfillment of the Requirements for
the Degree of Master of Science
in
Computer Information Systems**

NICOSIA, 2020

**MOHAMED S. SALHEIN
ELBELEKIA**

ATTITUDES OF EMPLOYEES TOWARDS CYBERSECURITY

**NEU
2020**

**ATTITUDES OF EMPLOYEES TOWARDS
CYBERSECURITY**

**A THESIS SUBMITTED TO THE GRADUATE
SCHOOL OF APPLIED SCIENCES**

**OF
NEAR EAST UNIVERSITY**

**By
MOHAMED S. SALHEIN ELBELEKIA**

**In Partial Fulfillment of the Requirements for
the Degree of Master of Science
in
Computer Information Systems**

NICOSIA, 2020

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name: MOHAMED S. SALHEIN ELBELEKIA

Signature:

Date:

ACKNOWLEDGEMENTS

I would like in particular to thank the supervisor of my thesis, Prof. Dr Fezile Ozdamli, because she represents useful guidance and support me with valuable information and discussions that helped me overcome my problems. Finally, but definitely not the last extension of my warm appreciation goes to the head of department Prof. Dr. Nadire Cavus All words of thanks are not enough for her.

I would also like to thank my mother for her support, encouragement and thanks to my wife for her patience throughout my studies and to thank my brothers for all their efforts.

To my parents...

ABSTRACT

Due to innovations in technology and cyber advancements, the occurrence of cybercrime has prompted many researchers and cyber experts to place more focus on cyber security. Cyber security protects software, hardware and other components of a computer. Cyber attackers can gain access to communication controls and remote-control different weaponries which can lead to cybercrimes. Thus, cyber security should not be handled lightly, but rather, much effect should be inputted into its measures. The aim of this study is to undergo a quantitative study on the perception and attitude of employees towards cyber security in different Libyan organizations. Analysis of Variance, Independent t-test and Pearson correlation are the methodologies used to analysis collected data. Results showed that the Beta value forage implemented towards the Attitude towards Cybercrime and Cybersecurity in Business is attached to the alternate hypothesis which was accepted, depicting a positive significance and hence, implies that “employees’ age” had relevant impact on Attitude towards Cybercrime and Cybersecurity in Business. “Gender” which is attributed to the null hypothesis being accepted, showed no significance, implying that no positivity was maintained as regards gender towards the attitude of cybersecurity in business. “Position at work” and “Experience again shows that the significance was positive enough, giving rise to the fact that the employees with respect to their various positions in offices and experience had some positivity towards it generally. Hence, this study can aid Libyan organizations improve their cyber security and prevent any form of cyber-attacks during business transactions.

Keywords: Cybersecurity; Cybercrime; Business; Employee; Innovations

OZET

Teknolojideki yenilikler ve siber ilerlemeler nedeniyle ortaya çıkan siber suçlar, birçok araştırmacıyı ve siber uzmanı, siber güvenliğe daha fazla odaklanmaya yöneltmiştir. Siber güvenlik, bir bilgisayarın yazılım, donanım ve diğer bileşenlerini korumaktadır. Siber saldırganlar, iletişim kontrollerine erişebilmekte ve siber suçlara yol açabilecek farklı silahları uzaktan kontrol edebilmektedirler. Bu nedenle, siber güvenlik hafif bir şekilde ele alınmamalı, daha ziyade, önlenmesi için daha çok çaba harcanmalıdır. Bu çalışmanın abircisi, Libya'nın farklı kurumlarında çalışanların, siber güvenliğe karşı algı ve tutumları üzerine nicel araştırma yapmaktır. Varyans Analizi, Bağımsız t-testi ve Pearson Korelasyon analizleri kullanılmıştır. Sonuçlar, Siber Suç ve İşletmelerde Siber Güvenlik Tutumuna yönelik uygulanan Beta değerinin, kabul edilen alternatif hipotezle ilişkili olduğunu göstermiştir, bu da pozitif yönde anlamlılık olduğu anlamına gelmektedir. Bu nedenle "çalışanların yaşı" Siber Suç ve İşletmelerde Siber Güvenliğe Yönelik Tutum üzerinde etkili olduğunu göstermektedir. Cinsiyet değişkeninden kaynaklanan bir farklılık görülmemiştir. Bu, İşletmelerde Siber Güvenlik Tutumu ile cinsiyet arasında olumlu bir ilişki olmadığı anlamına gelmektedir. "İşteki Konum" ve "Deneyim" anlamlılık düzeyinin yeteri kadar olumlu olduğu görülmektedir. Bu da, çalışanların işteki farklı konumlarının ve deneyimlerinin genel olarak belli bir seviyede olumluluk gösterdiğini doğrulamaktadır. Dolayısıyla, bu çalışma Libya kurumlarının siber güvenliklerini geliştirmelerine ve ticari işlemler sırasında gerçekleştirilecek her türlü siber saldırıyı önlemelerine yardımcı olabilir.

Anahtar Kelimeler: Siber güvenlik; siber suç; işletme; çalışan; yenilikler

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	ii
ABSTRACT	iv
OZET	v
TABLE OF CONTENTS	vi
LIST OF TABLES	ix
LIST OF FIGURES	x
LIST OF ABBREVIATIONS	xi
CHAPTER 1: INTRODUCTION	
1.1 Overview on Cyber Security	1
1.2 Problem Statement.....	3
1.3 Aim of the Study	3
1.4 Importance of Study	3
1.5 Limitations of the Study	4
1.6 Thesis Structure	4
CHAPTER 2: RELATED RESEARCH AND THEORETICAL FRAMEWORK	
2.1 Related Research: Cybercrime	5
2.1.1 Cyber-crimes in organizations	7
2.1.2 Cybercrime and criminology.....	9
2.1.3 Nature and scope of cybercrime.....	9
2.1.4 Cyber attack.....	10

2.2 Theoretical Framework of The Study.....	12
2.2.1 A dual mode of cybercrime.....	13
2.2.2 Cybercrime value chain.....	14

CHAPTER 3: METHDOLOGY

3.1 Research Model.....	16
3.2 Hypothesis.....	17
3.3 Research Participants.....	17
3.3.1 Participants’ demographic data.....	18
3.3.2 Position at the organization.....	19
3.3.3 Years of experience at the organization.....	20
3.4 Data Collection Tools.....	20
3.4.1 Reliability test.....	21
3.5 Data Analysis.....	21
3.6 Research Schedule and Gantt Chart.....	22

CHAPTER 4:RESULTS AND DISCCUSIONS

4.1 Results.....	24
4.1.1 Attitude of employees.....	24
4.2 Analysis of the Result and Hypothesis Testing.....	35
4.2.1 Employees’ age on attitude towards cybercrime/cybersecurity.....	35
4.2.2 Employees’ gender on attitude towards cybercrime/cybersecurity.....	37
4.2.3 Employees’ position at work on attitude towards cybercrime/cybersecurity.....	38
4.2.4 Employees’ experience on attitude towards cybercrime/cybersecurity.....	40
4.3 Hypothesis Test Summary.....	41

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion 44

5.2 Recommendations 45

5.3 Future Study 46

REFERENCES 47

APPENDICES 51

Appendix 1: Questionnaire 52

Appendix 2: Ethical Approval Letter 55

Appendix 3: Plagiarism Report 56

LIST OF TABLES

Table 2.1: Daily estimate of cyber-crime activities (Kan et al., 2018).....	12
Table 3.1: Research participants.....	18
Table 3.2: Position at the organization	19
Table 3.3: Years of experience at the organization	20
Table 3.4: Reliability test result of the questionnaire	21
Table 3.6: Research schedule	22
Table 4.1: Scale items for the ATC-IB questionnaire	25
Table 4.2: Pearson’s correlation (employees’ age and attitude towards cybercrime/cybersecurity in business).....	36
Table 4.3: Statistical difference between employees’ gender and attitude towards cybercrime/cybersecurity (Independent t-test).....	37
Table 4.4: One-way ANOVA on the impact of the position at work towards the attitude of cybercrime and cybersecurity in business.	38
Table 4.5: One-way ANOVA on the impact of the experience towards the attitude of cybercrime and cybersecurity in business.	40
Table 4.6: Hypothesis Test Summary.....	41

LIST OF FIGURES

Figure 2.2: The Binary model of cybercrime	13
Figure 3.1: Research model	16
Figure 3.2: Research gantt chart.....	23
Figure 4.1: Block diagram of the summary of the hypothesis result.....	42

LIST OF ABBREVIATIONS

ANOVA:	Analysis of Variance
ATC-IB:	Attitudes towards Cyber security in business
BBC:	British Broadcasting Corporation
CC:	Correlation Coefficient
CIA	Confidentiality, Integrity, and Availability
HTML:	Hypertext Markup Language
ID:	Identity
ICT:	Information and Communication Technology
IP:	Internet Protocol
ISA:	Information Security Attitude
ISAP:	Information Security Attitude Program
SPSS:	Statistical Packages for Social Sciences

CHAPTER 1

INTRODUCTION

Chapter 1 briefly introduces the study in general. It entails the aim, problem statement as well as the basic structure of the thesis amongst others.

1.1 Overview on Cyber Security

Due to innovations in technology and cyber advancements, the occurrence of cybercrime has prompted many researchers and cyber experts to place more focus on cyber security. Cyber security is very important in the cyber space because it ensures the protection and safety of software, hardware and other information system components of a computer (Deibert and Rohozinski, 2010). Cyber security has been of great importance in recent years as a result of the invaluable role it plays in cyber-attacks such as malware attacks, fraud and other forms of cybercrimes. Several studies on cyber security that has been carried out by different researchers over the years has suggested the need to create more regulations that can help to strengthen cyber security measures (Zhou et al., 2015).

Reports obtained from (Cao and Yang, 2013) stated the level internet banking has aided internet frauds which has drastically increased to about 64% (\$174.4) in 2015, has been possible due to loopholes in the internet defense systems. Several malware attacks have been made over the years in internet banking and other aspects of the cyber space. Wazid et al. (2017) lately discussed on the evolution of mobile banking and the threats of malware attacks. Several software applications have been developed over the years by different software designers on the detection, protection and elimination of malware attack. This has been of great benefit, but there are several malware attacks that cannot be detected or resolved with these software (Shapsough et al., 2015).

Internet innovations has made cyber attackers to have an almost limited power. Cyber attackers can gain access to communication controls, power supply and remote-control different weaponries which can lead to terrorism and genocides. Thus, cyber security should not be handled lightly, but rather much effect should be imputed into cyber security measures (Ericsson, 2010). In the late Decembers of 2015, an outage on power supply in

Ukraine was experienced as a result of cyber-attack. This singular art brought about a great deal of economic loss, and threat to security. Malwares were used to delict information's from different systems. Governmental bodies should take cyber security seriously and strictly. Most cyber attackers can use a nation's domain address to lunch a zombie attack which can cause conflict between two countries and eventually lead to war. Despite the threat to cyber-attacks have not had a permanent solution yet, the vulnerability of cyber-attacks can be reduced by packets such as firewalls, which has the ability of detecting any unknown file that could be infectious to a system. Port and Internet protocol (IP) address can actually also be useful in maintaining internet security by identifying file sources (Chapman, 2001). Firewall security has several limitations which cyber attackers can take advantage of and infect a system. Firewalls lacks the ability to detect "spoofed messages" which is not available the set of filter roles in firewalls (Li et al., 2018; Mishra et al., 2014; Reddy et al., 2016; Srinivas et al., 2018). Most software's and application programs are highly vulnerable because most of them are installed in devices without strong antivirus protection. The highest aspect of malicious attack in recent years is in the area of scams. Many individuals and organizations are on a daily bases defrauded through several fake templates. The area of scams is one of the most difficult aspect to carryout cyber security because unlike other malware attack, it cannot easily be treated. Moreover, some users disable security reasons for some reasons which can cause the computer to be more vulnerable art that period (Bishop, 2002; Subhashini and Kavitha, 2011).

However, cyberattacks are more prevalent in developed nations as opposed to developing nations. Developing countries also face cyber-attacks because the world has become a global village and everything is interconnected through the internet. Organizations should be informed on the importance of cyber security especially in Libya, because competitors and internet fraudsters can take advantage of any weak defense in an organization cyber space. Identifications on the perception of Libyan organizations on cyber security and creating attitude can help to reduce the level of cybercrime in Libya as well as creating awareness to different organizations on internet safety protocols.

1.2 Problem Statement

While cybercrime's evolution in countries that are developed was usually phased with information technology's growth in Libya and also many other developing countries with comparable circumstances, it seemed unexpected. Cybercrime in other words is the use of computer applications and packages in committing illegal practices over the internet, which include scams, malware attack and other forms of illegal cyber space activities (Ericsson, 2010).

Internet penetration rate in Libya is on the increase, Nevertheless, users of the internet were not prepared for crimes brought in by network globally. Even amongst Organizations, Information Security Attitude (ISA) rate has never been deliberate (Deibert and Rohozinski, 2010). Hence, this research study is to regulate the level of attitude of hazards in the cyber space amongst Organizations in Libya.

1.3 Aim of the Study

The aim of this study is to undergo a quantitative study on the perception and attitude of employees towards cybercrime and cyber security in different Libyan organizations.

1.4 Importance of Study

The recognition of the threat cyber criminals poses to organizations and a control of the world's resource and power, provides an urgency for more studies to be carried out on how to improve cyber security. However, the perception and attitude of many countries such as Libya on cyber security is low. Hence through a quantitative study on cyber security in Libyan organizations and literatures from previous studies, Libyan organizations can improve their cyber security and prevent any form of cyber-attacks and infestations because the **basic objectives of the study** tend to

- Analyze the cyber security's strength in Libya organizations
- Investigate the percentage of cyber-attacks on Libyan organizations.
- Determine the attitude and perception of Libyan employees to cyber security.
- Promote attitude on cyber security in Libyan organizations.

1.5 Limitations of the Study

This study covers a wide area on the identification of cyber security level, cyber threat and perception of Libyan organizations on cyber security. However, the study fails to examine measures that can be taken to improve the level of cyber security in Libyan organizations. Also, the study did not attempt to investigate the level of research on cybercrime in Libyan Universities.

1.6 Thesis Structure

This thesis is sectioned into five chapters. With the end goal for readers of this study to achieve a superior comprehension of the study, presentation of an outline of what every chapter entails in the thesis are listed beneath:

Chapter 1 entails the basic introduction under this study that would literally guide the reader and would further explain the problem of this study, its limitations as well as its aim.

Chapter 2 which is the Literature review & Theoretical framework of the thesis is all about related literature as regards the thesis as well as sections that aims to see that the perception & attitude of employees towards cyber security in workplaces can be ascertained.

Chapter 3 basically entails detailed methodology that was implemented in the cause of this research. Statistical tools/applications that was used to ensure maximum and reliable results are also discussed herein.

Chapter 4 would then detail the results and further discussions on how those results were attained.

Chapter 5 finally would encompass the concluding aspect of the thesis in general.

CHAPTER 2

RELATED RESEARCH AND THEORETICAL FRAME WORK

Chapter two of this study explains in details the related research that has been carried out before now by researchers as well as the theoretical framework of the study.

2.1 Related Research: Cybercrime

Cybercrime is a term used to denote the novel characteristics of crime introduced by cyberspace. With this crime on ever expansion, practical measures on tackling it are really less efficient. Hence, there is the need for more technical strategies to manage this growing concern. As necessary as it is to comprehend the motives of criminals so as to understand their motives for the crime and to generate end execute management techniques, so is it also necessary to understand their victims; to understand the users of computer systems and point out wherein they fall victims to these criminals. A number of definitions have been ascribed to this term with different degrees of specificity. To properly define cybercrime, there is the need to comprehend the impact of information and communication technology to our world (Jahankhani et al., 2011). As a result of the distinct characteristics of cyberspace, novel opportunities have been made possible for cyber criminals. These characteristics have been referred to as transformative keys (Jahankhani et al., 2011). These include:

1. Globalization: makes provision for cyber criminals with novel chances to go beyond traditional limitations
2. Distributed networks: these invent novel chances for mistreatment
3. Synopticism and Panopticism: these capacitate remote monitoring skills on victims
4. Data trails: make possible for cyber criminals to perpetrate impersonation

According to Wall (2005), there exists three main levels of the internet's influence on offender opportunity. First and foremost, the advent of cyberspace has provided increased opportunities for traditional thefts such as fraud, stalking, chipping. These already existed in real daily life but have increased in prevalence as a result of cyberspace. Traditional

criminals not only use the internet to communicate with each other, they also use it to perpetrate masterly offences like fraud, money laundering with greater accuracy and at lesser dangers. Also, cyberspace has made it easy for novel chances for conventional offences like hacking, spread of viruses, extensive fraud, online porn, and offensive speech. According to the Confidentiality, Integrity, and Availability CIA, hacking stands to be the most documented form of cybercrime against it. Nonetheless, latest innovations have included parasitic computing, in which offenders utilize a number of distant computers to carry out operations like preservation of illicit information like porn images and plagiarized software.

The extensiveness of cyberspace is so enormous it has made available new forms of crime such as spamming, rejection of service, property piracy, and fake e-marketing. On criminal attitude, there exists about four major kinds of crime. These can be placed in either of four categories as follows:

1. Those related to integrity like detrimental infringement
2. Those related to computer use like deceit, possession by theft
3. Those related to information like pornography
4. Content related like violence

According to Jahankhani et al. (2011) these crimes exist in different grades ranging from mild, medium to most detrimental. For instance, in the class of those related to integrity, chipping is considered mildly detrimental, while refusal of service as well as information combat is considered most harmful.

Lately, much has been on the Table about the characteristic of cybercrime and measures to manage it. Much debate still hovers over the scope, extent and management of cybercrime (Dodel and Mesch, 2019). Much has been documented on the subject of warring against cyber criminology with its constant changed especially with the advent of increased computer technology. Absence of a well-defined boundary on its definition is quite a challenge since it affects the ease of possibly defining solutions and measures to tackle the situation especially as the cybercrime is on rapid rise in terms of criminal proportion and their businesses. In 2012-2013, according to Sir Bernard Howe, the Commissioner of

Metropolitan Police in the Evening Standard of November 2013 commented that this time frame experienced a 60% increase in cyber criminology. And more to that in same financial year, cyber criminology cost the British economy a whopping 81 billion pounds. This rise is spurred by the fact that huge financial rewards lie in cyber criminology with very little possibility of legal consequences compared to the traditional arm robber (Hogan, 2013).

Contrary to traditional crime committed in a particular locality, cybercrime is done online with no reference to geography. Hence the need for global action to tackle this situation. This response is necessary to address the glaring challenges which hinder effective management of cybercrime. Some of these challenges are concerned with technology, constitution and nature of the cybercrime. Traditionally, crime has always been from the social, material and cultural point of view within a particular geographical location. With this well-cut definition, it has made it possible for characterizing crime, setting up measures on how to handle it. But this is not readily applicable with cybercrime because the environment is not specific to a distinct geographical location, nor is it restricted to a specific culture or social strata. Abuse of minors and rape for instance which are all typical of conventional crime can be characterized on the basis of the criminal, deciding on the social status of the criminal, geographical location based on residence whether rural or urban, city, state etc.

Nonetheless, with respect to cybercrime, such characterizing cannot be done because cyberspace is anti-spatial. Hence identifying crime by geography could be quite challenging. Cyber criminology makes possible comprehending the motives of cyber criminals by the analyses of social traits and their spatial locations. As an example, poverty can be considered a motivation for cyber criminals if the greater proportion of cyber criminals' stem from poverty-stricken backgrounds or if cybercrime seems high in poverty endemic zones.

2.1.1 Cyber-crimes in organizations

The threat associated with cybercrime has made many organizations to employ different forms of security measures to prevent victimization. Organizations such as banks and other

type of organizations are really faced with a lot of challenges with financial security. Cyber-criminals exploit different avenues from hacking to malware attacks that can take control of an entire system. If confidential information's are obtained by cybercriminals organizations can go bankrupt are be blackmailed on releasing these information's to their competitors (Zheng et al., 2017).

Organizations can be attacked, through any internet application from cyber criminals. Different kind of malware and worms can be used to attack a system. However, chats and messages can be used to gain access to information's and ID of users. Emails has been an easy way that cyber criminals use to gain access to systems and infect systems with different forms of viruses that can destroy the network system of a particular domain. Simple and attractive messages can be used by cyber criminals to attack a system. Some of these viruses do not need to be launched before they spread to destroy and infect the entire data base of a system (Hamid et al., 2014).Several attacks can be carried out on systems security systems, which is usually regarded as active attacks, hence compromising the "hypertext markup language" also known as "HTML". Other kinds of malicious codes can be downloaded into a system to gain control over a system. It is highly risky and dangerous for a computer user to go into the internet space without a firewall defense or an antivirus system. Cybercriminals utilize what is known as zombie attacks. This is carried out by using another system as a host in sending information's and messages to other users. Usually, such acts are carried out based on criminative purposes, thus an innocent individual can be accused and labeled as a cyber-criminal if the domain and IP of the message is been traced. This is usually carried out by installing a virus or worm in a victims (botnet) computer system and using the system without the person's attitude and knowledge (Ning et al., 2013). Several researches were analyzed on "Botnet" in 2009 by BBC and it was observed from the reports of journalists that about 21 thousand computer systems has been infected with malware, and are been used to send information as spam mails and blackmailing of e-commerce sites. It was however discovered that majority of the infected computers were from developing countries that did not have access to proper internet security in their systems (Hamid et al., 2014).

However, most organizations are always equipped with a strong firewall and antivirus system that can be used to defend any incoming infectious attack that can crash the entire system of the organization. Moreover, professional cyber computer engineers are employed in these organizations to monitor and ensure that there is maximum security in the cyberspace.

2.1.2 Cybercrime and criminology

The study of criminology helps in understanding the motives of offenses done by individuals with particular traits like the frequency of criminals from a specific group of persons that are discriminated against socially, politically, educationally and economically. More so, the link between geography and social traits are linked to crime and social marginalization in conventional crime cases but this is not so with cybercrime. A significant aspect worth considering is the fact that internet accessibility is quite low among the marginalized neighborhoods of society who are at the same time socially exclude, hence greater possibility of involving in crime. More so, cybercrime requires some degree of skill and knowledge in information technology. And from this point of view, it can be seen that cyber criminals appear to be the more privileged with internet access above the average in society. Hence, conclusions based on the relationship between crime and social marginalization that are applicable with conventional crime do not readily find their place with cybercrimes are atypical with respect to the expectations of conventional crime. Therefore, the available viewpoints that associate the motive of crime social extrusion and discrimination do not find applications with cybercrime as they do with conventional crime. This absence in understanding clear cut motives has been a major drawback for state legislature to manage cybercrime (Dodel and Mesch, 2019).

2.1.3 Nature and scope of cybercrime

Crime is common phenomenon in a society. As impossible as it is to live free of conventional crime in the real world, so it is to not experience cybercrime in cyberspace. Nonetheless, with the passage of time, the nature and extent of criminal act changes in a given society. Hence the nature of the society involved can to a large extent determine the trait as to what to describe as a cybercrime. This is so because the complicatedness of the

society can determine the complicatedness of the crime in it. To well comprehend the nature of a criminal act in a society, it is necessary to take into consideration the various factors which influence and affect the crime. Social, economic and political factors all play a role in understanding a cybercrime so as to properly implement measures to tackle the situation. Measures involved prevention and fixing taken up by the machinery to manage cybercrime and criminal activities in the given society are also vital aspects to be considered when trying to decide on the nature and scope of a cybercrime (Donald and Osei-Bryson, 2019).

The growth of cybercrime has generated novel social, economic and political challenges. More so, the absence of well-defined legislature to handle the crime due to poor understanding of its nature and scope has led to even complex problems. In most cases, government equipment and machinery are not well developed to detect and handle the surge of cybercrime. The spread of information technology has brought the world closer and made it a global village economically, socially and somewhat culturally. From a single geographical location, one can have access to the entire world. The rise in this modern technology has broken barriers to time and space. Adequately managing cybercrime on the global level is challenging as cyberspace is borderless vis-à-vis the physical world. Available machinery still cannot handle cybercrime conveniently as cybercrime is transnational. The improvement of internet science with its enormous opportunities have also brought attached to it the challenge of criminals committing cybercrimes and go undetected. Increased dependence on computer technology has paved the way for increase cybercrime activities (Hadlington, 2017).

2.1.4 Cyber attack

The outbreak of cyber-attack has been a major area of concern in the last few decades. Several cyber-attacks such as virus, phishing attack, Trojan horse, worms, ransomwares, spywares, unauthorized access, as well as system control has been major way cyber criminals has used to attack cyber users (Erika et al., 2013). Virus is usually infectious to system when attached to a program. A virus can corrupt an entire system when executed. Attacks related to social platforms are phishing attacks, which usually operates with a fake web-link. Execution of such links can expose personal information's of a user, hence

giving the intruder the avenue to have access to an unauthorized data base such as passwords, credit card information's and user identifications. Trojan horse usually contains hidden codes that can get information of a system as well as taking over an entire system when it is executed. An unauthorized control of an account or system is a very serious treat especially the gaining of a user's financial information (Adomi and Akpojotor, 2018). A worm attack is a self-replication infection that can spread from one system to another, by attacking host networks, hence causing webpage overloading. Worms unlike viruses do not depend on executions to spread through a system, worms automatically spread through a system without user execution.

Worms unlike viruses do not depend on executions to spread through a system, worms automatically spread through a system without user execution.

Reports from the European authorities mentioned that about ten thousand organizations and two hundred thousand people in about one hundred and fifty countries were attacked with a ransomware known as "*WannaCry*". Ransomware usually attack a system by limiting user's from having complete access to their system. These cyber criminals lock specific user applications and files, to be unlocked in exchange for a monetary ransom. Spywares is another type of program used to monitor vital information's of a user. Tracks of webpages, emails and contact list can be monitored, which can later be misused.

Gaining an unauthorized access to a system by guessing or stealing personal information's of a person can also be categorized as cybercrime. Also, the system of a user can he hacked into to gain control over the activities of that particular system (Ash and Burn, 2003).

The Table below shows an estimated daily financial income by cybercriminal globally (Kan et al., 2018).

Table 2.1: Daily estimate of cyber-crime activities (Kan et al., 2018)

Cybercrime category	Estimate of daily activities
Phishing	33 thousand
Malicious attacks	80 billion
Ransomware	4 thousand
New malware	300 thousand
Hacking	780 thousand

2.2 Theoretical Framework of The Study

This section of the study provides a detailed elaboration of the study model and various correlation between cyber security and employee's perception and attitude of its existence. Study by Talib, et al. (2010), illustrated that threat attitude is likely to have an influence on the rationale motivation towards cybercrime protection. They further illustrated that there is a significant positive relationship between information security attitude program (ISAP) and response efficacy, perceived severity and self-efficacy.

Study by Hasan, et al. (2015). proposed that there are discrepancies between females and male's perception to cybercrime and females are more aware of the cyber regulations and stick to cyber ethical values compared to the male counterpart. Previous literary studies have illustrated that sex group is an often-mentioned demographic background that is related with discrepancies in Life styles.

Study by Neiss, et al. (2009) also proposed the difference in attitude and perception to cybercrime among different age groups. They further stated that the difference is as a result of dissimilarities in perspective between young people and old age group. Younger people are driven by their emotional perception which is different from the older adults.

ICT knowledge is vital in the prevention of cybercrime (Asokhia, 2010). Hence, it is vital to educate people on cybercrime so as to avoid the risks associated with it. One of the ways to improve the attitude of cybercrime is to integrate it into the university academic curriculum (Biugaadt and Kyobe, 2011). This will improve future behavior of individuals towards cybercrime in terms of safety and security.

2.2.1 A dual mode of cybercrime

The concept of the word “cybercrime” is composed of different kinds of online crimes as proposed by Ibrahim, (2019), offences committed using computer, computer associated networks, or other forms of ICT. On the other hand, cyber enabled crimes “can still be committed without the use of ICT00 such as cyber fraud. These dual categories are illustrated in Figure 2.2. Unlike traditional crimes however, one criminal scheme in the realm of cyberspace may involve multiple nations and actors and even impact on multiple nations simultaneously.

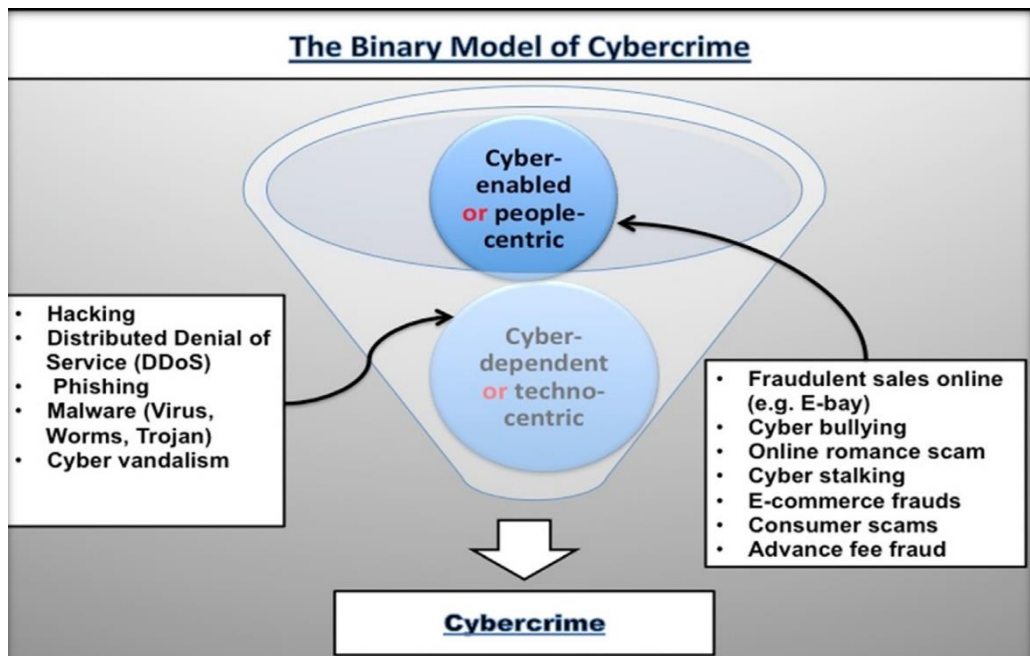


Figure2.2: The Binary model of cybercrime(Ibrahim, 2016)

2.2.2 Cybercrime value chain

The literature on value chain analysis defines it as the full range of activities required to bring a product or service from conception, through the different phases of production to the end users or consumers (Tang and Rush, 2013). The concept of value chains likewise, identifies with the contributions from numerous on-screen characters in different enterprises, despite the fact that the connections portrayed by the value chain will, in general, be increasingly vertical inside one kind of product that is industrial than the idea of business biological system, which cuts on a level plane crosswise over numerous divisions, items and administrations. By and by, the idea of significant value chains provides significant commitments to understanding the environment since: first, it finds specific on-screen characters inside the value chain and displays how they alter position after some time. Second, it tags the basic progression of exercises required for the generation of products and ventures. Third, it distinguishes the linkages between the different exercises in the chain. Fourth, it encourages us to see who gains along the production network and recognizes the solid and frail connections. At the end of the day, it distinguishes who assumes a significant job in its prosperity, or how it is administered. At long last, it features the significance of updating or improvement of abilities and framework, administrations and items. A value chain structure in this way gives bits of knowledge into the elements of a business biological system. As in the real business world, cybercriminals contend and organize their activities so as to increase an upper hand over a particular fragment of the market. The succession of exercises, depicted over, that is required to make an item or administration, includes the blend of contributions from different on-screen characters, which, in many businesses are progressively dispersed comprehensively. A focal worry of significant value chain examination is to improve the comprehension of and unload the connections between the entertainers associated with the scope of exercises that lead to creating a decent administration.

Every one of the exercises from different entertainers is proposed to help the undetected age of budgetary benefit. Accordingly, every movement can be related with various techniques for accomplishing a monetary profit inside their own specialty markets, wellsprings of upper hand and gains or worth included advantages, consolidating with one

another to shape a worth chain. Cybercrime would thus be able to be viewed as an overall value chain encouraging misrepresentation, with various activities, net revenues, innovative capacities and redesigning of items and administrations and, subsequently, openings joined to each stage.

Inside cybercrime esteem chains bringing about wholesale fraud and charge card misrepresentation, we can distinguish three fundamental exercises: (1) recognition of vulnerabilities in the computerized system, including the web, (2) dissemination and infection of the system, and (3) abuse of the system weaknesses.

CHAPTER 3 METHODOLOGY

This chapter provides an overview of the research’s methodology, in which the research model, participants, process and data collection tools that were implemented in the research were all but clearly discussed, Furthermore, the data analysis techniques used and data collection procedures were also debated.

3.1 Research Model

This study, which is aimed at attitudes of employees towards cybersecurity can be briefly but concisely illustrated with the Figure (Figure 3.1) under the subtopic “*research model*”.

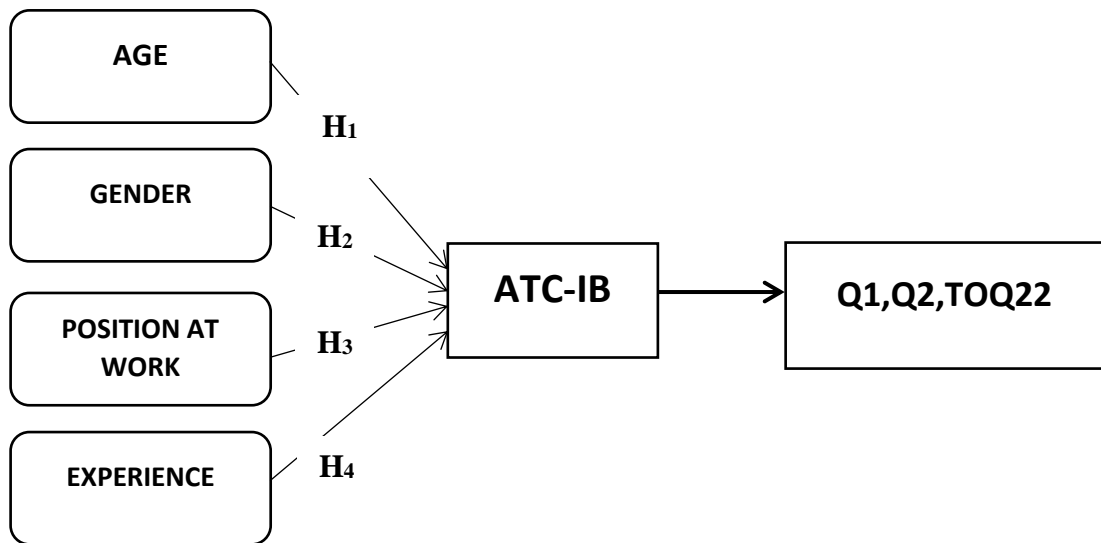


Figure 3.1: Research model (Lee, 2017)

3.2 Hypothesis

In the course of this study, some hypothesis would be considered so as to analyse issues related cyber security in Libyan organization. They are listed beneath;

- H₀: There is no relevant impact that exists between Employees' age and attitude towards cybercrime/cybersecurity.
H₁: There is relevant impact that exists between Employees' age and attitude towards cybercrime/cybersecurity.
- H₀: There is no relevant impact that exists between Employees' gender and attitude towards cybercrime/cybersecurity
H₁: There is relevant impact that exists between Employees' gender and attitude towards cybercrime/cybersecurity.
- H₀: There is no relevant impact that exists between Employees' position at work and attitude towards cybercrime/cybersecurity.
H₁: There is relevant impact that exists between Employees' position at work and attitude towards cybercrime/cybersecurity.
- H₀: There is no relevant impact that exists between Experience and attitude towards cybercrime/cybersecurity.
H₁: There is relevant impact that exists between Experience at work and attitude towards cybercrime/cybersecurity.

3.3 Research Participants

The study was conducted during the Fall 2018-2019 period. Employers were selected from three Libyan companies situated in Libya. Participants from Arabian Gulf oil Company, Libyan Telecom & Technology Company and Al-Jumhouria bank consisted of volunteers (employees) in this study.

The participants involved in the research consists of 312 employees. All participants that executed their job as employees were based in the Libya.

3.3.1 Participants' demographic data

Discernment as well as the attitude of someone may be influenced by gender in a rather considerable manner (Gefen and Straub, 1997). In other words, many researchers regarded gender as a key factor and its impact in determining the intention of just some customers (Zhang, 2012; Riquelme and Rios, 2013).

Age is also seen as a significant variable in the research of consumers' perceptions of any fresh literature technology although, this has to do with cybercrimes and not just technology (Gefen and Straub, 1997).

A demographic data that would appear in form of a frequency Table can be seen in Table 3.2. It shows the data of the participants that actively played their parts in this research.

Table 3.1: Research participants

Demographic Variables	Frequency	Percentage (%)	
Gender	Male	184	59.0
	Female	128	41.0
	Total	312	100.0
Age	23 – 60 years		
Level of Education	High school	37	11.9
	Bachelor	245	78.5
	Master	30	9.6
	Total	312	100.0

Males involved numbered about 184 and the corresponding value for that digit is 59.0% while the female counterpart had a total frequency of 128 with the percentage value being 41.0%. Since respondents are employees working in organizations, they had an age range between 23-60 years. The highest level of education attained by those employees was the Master's degree. 245 (a percentage of 78.5) of them had Bachelor degrees, 30 (9.6%) of them had Master's degree certificate to their name while 37 (11.9%) of those employees were all graduates of high school.

3.3.2 Position at the organization

Table 3.2 clearly depicts the positions held by the employees (respondents) in the organization.

Table 3.2: Position at the organization

Position held	Frequency	Percentage (%)
Manager	20	6.4
Supervisor	56	18.0
Senior Laborer	148	47.4
Junior Laborer	88	28.2

From the result in Table 3.2, it was observed that about 6.4 % of them with a frequency of 20 were managers, 18.0% with a frequency of 56 held supervisor's position in the organization, 47.4% of them again were Senior laborer while the last of them but definitely not the least being the Junior laborer had a frequency of 88 with a percentage (%) value of 28.2.

3.3.3 Years of experience at the organization

How long in terms of “years of experience” at the organization for the employees was also analyzed and results attained in Table 3.3.

Table 3.3: Years of experience at the organization

Number of years	Frequency	Percentage (%)
Less than 5	81	26.0
Between 5 - 10	86	27.5
Between 10 - 15	30	9.6
15 – above	115	36.9

From the result reported, it was observed as shown in Table 3.3 below, that 26.6% have worked in the organization for less than 5 years, 27.6% have been working between 5-10 years, 9.6 % have been working in same organization between 10 to 15 years while 36.9% have been working there for as long as 15 years and above. This part of this questionnaire was attained during work hours of the organization and again, 312 employees actively participated in the survey.

3.4 Data Collection Tools

Questionnaire being paper-based was the focal tool used by the study’s researcher in other to get data from 350 Employees in 3 different Libyan organizations. The questionnaires were given to employees in different locations, Arabian Gulf Oil Company, Libya Telecom and Technology and Bank Al-Jumhouria. A total of 38 questionnaires were omitted from the final analysis due to incomplete information or some missing vital information that wasn’t properly filled by the participants. The remaining dataset (completed hence valid questionnaires) contained responses from 312 participants (employees). The first part (Section A) of the questionnaire dealt with the general demographic data of each employee (respondent/participant). The second part (Section B) had to do with other one-dimensional Attitudes towards cyber security in business (ATC-IB)(Lee, 2017). Questionnaire that was implemented is comprised of approximately 22 questions which was meticulously selected and arranged. Now this action was to really discover the genuine effect of the perception of

these employees towards cybersecurity in general, particularly in Libya. The participants answered to items on 4-point Likert Scale from “*Strongly Disagree*” (4point), “*Disagree*” (3point), “*Agree*” (2point), “*Strongly Agree*” (1point) and the evaluation of the study required a basic instrument of measurement which is reliability and validity. In other to test, reliability analysis would be achieved using Statistical Packages for Social Sciences (SPSS) Cronbach Alpha and hence, was calculated as **0.749** by using **Cronbach’s Alpha** for the 22 questions in Section B and its shown in Table 3.4.

Table 3.4: Reliability test result of the questionnaire

Dimension	Cronbach’s Alpha Reliability
ATC – IB	0.749

3.4.1 Reliability test

A reliability test has been implemented so as to check if the questions are organized in a way that avoids slight information to assess the credibility part of the study in question. Hence, Cronbach alpha in more details states that if the result attained after analysis. Again, the outcomes accomplished were very satisfying which signified that this study could progress as a proof by a total reliabilty of about "**0.749**" which was for a comprehensive questionnaire being issued to respondents/participants (employees).

3.5 Data Analysis

As earlier discussed, the questionnaires that were used to collect data from the employees in the three Libyan organizations/companies was 350 in number. Afterwards, they were inserted into Statistical Packages for Social Sciences (SPSS) version 21 and that was when the researcher found some questionnaires were short of information or wasn’t even filled at all and hence, they were discarded. The valid information attained from the participants were then analyzed and interpreted. Frequency and percentage were used for analyzing the demographic data while the Cronbach alpha technique was used to find the total reliability of the questionnaires used.

3.6 Research Schedule and Gantt Chart

The study in general acquired a total period of 32 weeks in order to be successfully completed. The schedule as planned can be seen in Table 3.6 beneath.

Table 3.6: Research schedule

Schedule	Duration (weeks)
Thesis proposal	5
Proposal submission	1
Design of Questionnaire	2
Related Literature	4
Collection of Data	6
Data entry into SPSS	2
Data Analysis	3
Final thesis drafting	2
Thesis review by Supervisor	3
Corrections and defense preparations	4
TOTAL	32

Additionally, Figure 3.5 depicts the Gantt diagram meant for this particular research

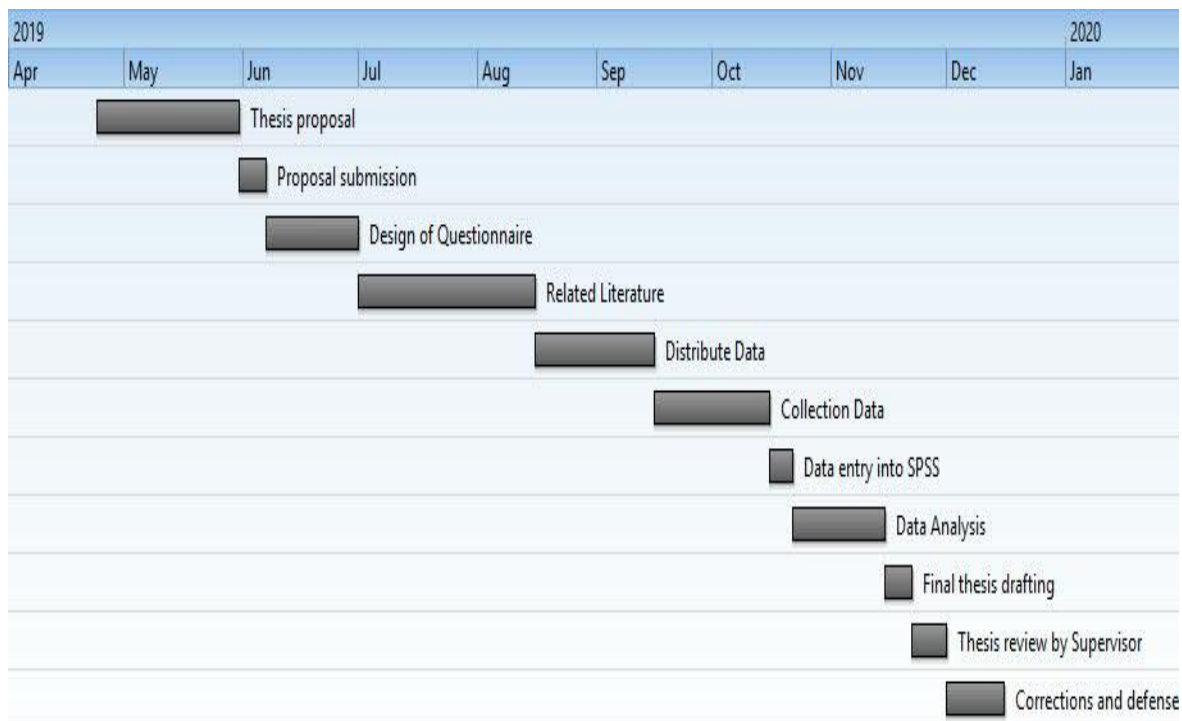


Figure 3.2: Research gantt chart

CHAPTER 4

RESULTS AND DISCCUSIONS

Chapter four simply discussions in details, the result that has been attained by the researcher after analysis of the collected data has been performed.

4.1 Results

Results after the analysis were explained under this section. Various discussions as regards the result that has been obtained from the analysis carried out via the use of statistical tools were also done.

4.1.1 Attitude of employees

The various responses for the bio-data of the respondents of the questionnaires used as a tool in the methodology of this thesis, would be further analyzed and deduced in this section via the descriptive statistics of frequencies using the Statistical Packages for the Social Sciences (SPSS) version 21 as an analysis tool. The analysis under this section would cover the respective verdicts with reference to the afore-mentioned hypothesis. The responses of the respondents (employees) in those companies as well as their respective answers as regards the questionnaires that has to do with their “attitude towards Cyber Security in business” issued to them will also be analyzed and placed in the chapter.

Table 4.1: Scale items for the ATC-IB questionnaire

Items	SA %	A %	D %	SD %	M	SD
Responsibility of the management is to ensure a company is protected from cybersecurity.	48.7 (152)	50.0 (156)		1.3 (4)	1.54	.571
Keeping the company protected from potential cybercriminals I think is my role.	3.5 (11)	4.2 (13)	69.6 (217)	22.8 (71)	3.12	.631
Everyone in the organization plays a role in protecting the organization against threats from cybercriminals.	28.2 (88)	66.3 (207)	3.5 (11)	1.9 (6)	1.79	.593
It is tough to tell how I can help protect the organization from cybersecurity.	12.8 (40)	69.9 (218)	13.5 (42)	3.8 (12)	2.07	.664
No possession of the right skills to be able to protect the organization from cybercrime.	13.1 (41)	68.3 (213)	14.1 (44)	4.5 (14)	2.10	.666
Securing IT is not important within my organization.	7.7 (24)	23.4 (73)	39.1 (122)	29.8 (93)	2.91	.913
Delivery of all the protection a company needs can be achieved by Computer systems.	15.1 (47)	56.7 (177)	22.1 (69)	6.1 (19)	2.19	.762
Reporting cybercrime is a waste of time	4.8 (15)	33.0 (103)	43.3 (135)	18.9 (59)	2.76	.811
I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.	26.9 (84)	65.1 (203)	6.1 (19)	1.9 (6)	1.83	.616

Table 4.1: Scale items for the ATC-IB questionnaire continued.

Items	SA %	A %	D %	SD %	M	SD
Reporting a cyber-attack to the Police it might impair the reputation of the company	11.5 (36)	77.2 (241)	10.6 (33)	0.6 (2)	2.00	.498
More can be achieved to communicate the dangers from cybercrime to people in the organization.	6.4 (20)	3.8 (12)	75.6 (236)	14.1 (44)	2.97	.661
There is an awareness company's IT use strategy and attempt to follow it.	0.3 (1)	9.3 (29)	78.5 (245)	11.9 (37)	3.02	.474
If a cyber-attack occurred, I would not know how to report it.	12.2 (38)	73.7 (230)	10.6 (33)	3.5 (11)	2.05	.606
I don't think that reporting a cyber-attack on the company is my responsibility.	7.4 (23)	54.8 (171)	27.2 (85)	10.6 (33)	2.41	.776
It is not my concern if material for an organization material is affected by threats from cybercrime.	8.7 (27)	47.4 (148)	31.7 (99)	12.2 (38)	2.47	.817
I am confident that I would be able to spot the signs of a cyber-attack.	7.4 (23)	25.0 (78)	62.5 (195)	5.1 (16)	2.65	.691
I think the biggest threat for IT systems comes from people within the company.	5.8 (18)	12.2 (38)	71.5 (223)	10.6 (33)	2.87	.665
I feel that any individual within the company are at risk of manipulation from confident tricksters.	3.8 (12)	3.8 (12)	77.6 (242)	14.7 (46)	3.03	.583

Table 4.1: Scale items for the ATC-IB questionnaire continued.

Items	SA %	A %	D %	SD %	M	SD
If there is a significant economic increase in a company, it is an easy target for cybercriminals.	20.2 (63)	73.1 (228)	6.7 (21)		1.87	.502
Only huge establishments are targets for cybercriminals.	17.3 (54)	75.0 (234)	6.7 (21)	1.0 (3)	1.91	.522
I do not know who is accountable for protecting the company from cybercrime.	13.5 (42)	63.5 (198)	17.3 (54)	5.8 (18)	2.15	.719

Note: SA = Strong Agreed; A = Agreed; D = Disagree; SD = Strongly Disagree; % = Percent; M = Mean; SD = Standard Deviation.

In Table 4.1, the frequency alongside valid percentage of every respondent that filled the questionnaire, is solely based on whether they strongly agree, agree, disagree or strongly disagree with every question as regards employees' attitude towards cyber security as well as cybercrime in business-oriented background in general being asked.

Question 1: The first question possessed a total of 152 respondents with a percentage of 48.7 that strongly agreed, then again 156 respondents with 50% basically were of the opinion that they “agreed” with the statement, and finally but not the least, just 4 respondents with 1.3% had thoughts/response as regards the question to strongly disagreed. None of the respondents basically “disagreed” but rather that 1.3% “strongly disagreed” with the fact that they fill that management should possess the obligation to guarantee an organization is protected from cybercrime”.

Based on the summary of responses collated, this simply entails that from the responses, the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 308 respondents and were responsive to the fact.

Question 2: The second question had a total of 11 respondents with a valid percent of 3.5% that strongly agreed, then 13 respondents with 4.2% basically agreed with the question, 217 respondents with 69.6% disagreed and lastly 71 out of 312 respondents with 22.8% strongly disagreed.

This simply depicts that from the responses, frequency count of just 24 respondents, agreed and strongly agreed to the fact that.

Question 3: Here, the corresponding question was asked as regards employees' attitude towards cybersecurity in business. Respondents gave their answers and yet again, they were classified according to how they strongly agree, agree, disagree and strongly disagree. A total of 88 respondents with a percentage of 28.2 that strongly agreed, then again 207 respondents with 66.3% basically were of the opinion that they "agreed" with the statement, 11 of the respondents having 3.5% disagreed and lastly, another 6 out of 312 respondents having basically 1.9% strongly disagreed.

Therefore, with reference to all responses attained with respect to the 3rd question, it can be vividly seen that a maximum total of 295 responses was specifically the combination of respondents that agreed to or strongly agreed to the fact that they believe everyone in the establishment plays a vital role in the protection against threats from cybercriminals.

Question 4: The fourth question attained a total of 40 respondents with a valid percent of 12.8% that strongly agreed, then 218 respondents with 69.9% basically agreed with the question, 42 respondents (employees) with 13.5% disagreed and lastly about 12 out of 312 respondents with 3.8% strongly disagreed.

Now based on the summary of responses collated, this simply entails that from those responses, the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 258 respondents and were responsive to the fact that indeed It is hard to know how they possibly aid to protect the organization from cybercrimes.

Question 5: This is another question thrown to the respondents (employees). Responses attained as regards this was that 41 of the respondents, having a total percent 13.1% strongly agreed to the that fact, then a total of 213 respondents with 68.3% basically agreed

when asked, 44 respondents with 14.1% barely disagreed with that fact, then 14 of the respondents with 4.5% strongly disagreed to that fact.

Hence, with reference to the total responses attained, it is being deduced that a total of 254 respondents was the highest frequency count that basically and strongly agreed to the fact. A combination of those respondents that agreed and strongly agreed were basically summed up and that was what gave us a total of the 254 out of a possible 312 respondents.

Question 6: Feeling that securing IT is a precedence within an establishment was asked to individuals that had some level of experience with the companies/organizations where they work. Out of a possible 312 respondents, 24 of them with a 7.7% strongly agreed to the fact. 73 respondents with 23.4% basically agreed, then again, 122 respondents with 39.1% had the choice to disagree. Finally, 93 out of the 312 respondents with 29.8% “strongly disagreed”.

In other words, after the collated responses were reviewed, it showed again showed that there were positive responses as regards feeling that IT security is an organization’s priority in the sense that the respondents that disagreed and they had the highest frequency count (122) even despite having a combined total (97 out of 312 responses) of respondents that agreed and strongly agreed to that statement.

Question 7: This question as regards Computers offer all the protection a company wants had a total of 47 respondents with a valid percent of 15.1% that strongly agreed, then 177 respondents with 56.7% basically agreed with the statement, 69 respondents having 22.1% disagreed and lastly, another 19 out of a possible 312 respondents having basically 6.1% strongly disagreed.

This simply depicts that from the responses, the highest frequency count was a total of 224 respondents and this number was a combined verdict for those that agreed and strongly agreed to the fact.

Question 8: The question of Reporting cybercrime is a waste of time was again being answered by various individuals that have been working with the mentioned companies in connection with this study. Out of a possible or total of 312 respondents, a total of 15

respondents with a percentage of 4.8 strongly agreed, then again 103 respondents with 33.0% basically were of the opinion that they “agreed” with the statement, but a total of 135 respondents with the highest value of 43.3% bluntly disagreed as regards the question, and lastly, another 59 out of 312 respondents having basically 18.9% strongly disagreed.

Therefore, with reference to all responses attained with respect to the 8th question, it can be vividly seen that a maximum total of 194 candid responses was specifically the combination of respondents that disagreed to or strongly disagreed to the fact that once a cybercrime is reported, is time wasting.

Question 9: The ninth is yet another question that was suggested to the respondents in the questionnaires and again, there responses was split according to previously stated sections. This question in particular attained a total of 78 respondents with a valid percent of 25.0% that strongly agreed, then 205 respondents with 65.7% basically agreed with the question, then a total of 14 respondents possessing a value of 4.5% disagreed and lastly 15 out of 312 respondents with 4.8% strongly disagreed with the fact that the police lack the capacity to deal with cybercrime effectively.

Now based on the summary of responses collated, this simply entails that from those responses, the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 283 respondents and were responsive to the fact.

Question 10: Now, the tenth one was another vital question exclusively written in the questionnaire. This question in particular attained a total of 84 respondents with a valid percent of 26.9% that strongly agreed, then 203 respondents with 65.1% basically agreed with the question, then a total of 19 respondents with 6.1% disagreed and lastly but not the least, out of 312 respondents, 6 of them with 1.9% strongly disagreed with the fact that the network is thought to reduce the time and effort required to execute the business.

Now based on the summary of responses collated, this simply entails that from those responses, and the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 287 respondents and were responsive to the fact.

Question 11: This one question was added to the questionnaire and the responses attained. Respondents of about 36 in number with a valid percent of 11.5% strongly agreed, then 241 respondents with 77.2% basically agreed with the statement, 33 respondents with 10.6% disagreed and again lastly, another 2 out of 312 respondents having basically 0.6% strongly disagreed to that question as regards being worried as regards the question.

Now after collation, this simply depicts that from the responses, the highest frequency count was a total of 277 respondents and this number agreed and strongly agreed to the fact that damaging the company's reputation would be to report a cyber-attack to the police.

Question 12: This question in particular attained a total of 20 respondents with a valid percent of 6.4% that strongly agreed, then 12 respondents with 3.8% basically agreed with the question, then a total of 236 respondents with 75.6% disagreed with the statement while 44 with 14.1% strongly disagreed with the fact stated.

Now based on the summary of responses collated, this simply entails that from those responses, the highest frequency count for those respondents were those that disagreed (236 employees) but the total of those that disagreed and strongly disagreed was about 280 respondents.

Question 13: Out of a possible 312 respondents, just 1 of them with a valid value of 0.3% strongly agreed to the fact they are conscious of the IT's policy use of the company and effort to trail it, 29 respondents with 9.3% basically agreed with the statement, then again, 245 respondents with 78.5% basically disagreed and lastly, another 37 of these respondents having basically 11.9% strongly disagreed with such statement.

In other words, after the collated responses were reviewed, it showed that respondents didn't support the idea of being mindful of the IT's policy use of the company in order to endeavor making use of it. These responses in total (Strongly disagreed and disagreed) with reference to the statement numbered up to 282 out of a possible 312.

Question 14: Another question in the questionnaire given to respondents had about 38 in number with a valid percent of 12.2% strongly agreed, then 230 respondents with 73.7% basically agreed with the statement, 33 of these respondents with 10.6% virtually disagreed and lastly, another 11 out of 312 respondents having basically 3.5% strongly disagreed to

that question as regards the network is protected from hacking and tampering with information.

Now after collation, this simply depicts that from the responses, the highest frequency count was a total of 268 respondents and this number agreed and strongly agreed to the fact that if a cyber-attack occurred, they would not know how to report it.

Question 15: This statement was yet again, another vital question exclusively written in the questionnaire. This question in particular attained a total of 23 respondents with a valid percent of 7.4% that strongly agreed, then 171 respondents with 54.8% basically agreed with the question, then a total of 85 respondents with 27.2% disagreed and lastly but not the least, out of 312 respondents, 33 of them with 10.6% strongly disagreed with the fact. Now based on the summary of responses collated, this simply entails that from those responses and the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 194 respondents and were responsive to the fact that indeed they wouldn't know for sure that reporting a cyber-attack in the establishment is their obligation in general.

Question 16: Another vital question being included in the questionnaire had responses attained as regards this was that 27 of the respondents, having a total percent (8.7%) strongly agreed in favor of the statement, then 148 respondents with 47.4% basically agreed when asked, 99 respondents with 31.7% barely disagreed with that fact, then 38 respondents with around 12.2% strongly disagreed.

Hence, with reference to the total responses attained, it is being deduced that a total of 175 respondents was the highest frequency count that basically and sincerely agreed to the fact. A combination of those respondents that agreed and strongly agreed were basically summed up and that was what gave us a total of 175 out of a possible 312 respondents.

Question 17: I am confident that I would be able to spot the signs of a cyber-attack was one of the questions asked to individuals that had some level of experience with the aforementioned companies. Out of a possible 312 respondents, 23 of them with a 7.4% strongly agreed to the fact they would be able to spot cyber-attack signs, 78 respondents with 25.0%

basically agreed with the statement, then again, 195 respondents with 62.5% disagreed and then lastly but not the least we had 16 of the respondents having 5.1% strongly disagreed.

In other words, after the collated responses were reviewed, it showed again showed that there were responses as regards the question of being be able to spot cyber-attack signs in the sense that the respondents that disagreed or strongly disagreed to a large extent to that statement and it was numbered up to 211 out of a possible 312.

Question 18: This question, was again being answered by various individuals that have been working with the civil registry. Out of a possible or total of 312 respondents, a total of 18 respondents with a percentage of 5.8 that strongly agreed, then again 38 respondents with 12.2% basically were of the opinion that they “agreed” with the statement, 223 respondents with 71.5% had to disagreed and lastly, another 33 out of 380 respondents having basically 10.6% strongly disagreed.

Therefore, with reference to all responses attained with respect to the 18th question, it can be vividly seen that a maximum total of 256 candid responses was specifically the combination of respondents that disagreed to or strongly disagreed to the fact that they think the major hazard for IT systems originates from individuals inside the establishment.

Question 19: This is yet another question in the questionnaire given to respondents. Respondents (employees) of about same number both agreed and strongly disagreed respectively. 12 in number with a valid percent of 3.8% strongly agreed, then again 12 respondents with 3.8% basically agreed with the statement. Now, 242 respondents with 77.6% had to bluntly disagree and furthermore, another 46 out of 312 respondents having basically 14.7% strongly disagreed to that statement as regards feeling that any person inside the establishment are at danger of manipulation from confident frauds.

Now after collation, this simply depicts that from the responses, the highest frequency count was a total of 288 respondents and this number disagreed and strongly disagreed to the fact that they sense that any person inside the establishment are at danger of manipulation from confident swindlers.

Question 20: Now this question was again included in the questionnaire for those that picked it up to fill. It had a total of 63 respondents with a valid percent of 20.2% that strongly agreed, then 228 respondents with 73.1% basically agreed with the question, 21 respondents with 6.7% disagreed. None of the said employees “strongly disagreed” to the statement provided.

This simply depicts that from the responses, the highest frequency count was a total of 291 respondents and this number agreed and strongly agreed to the fact.

Question 21: Again, this question was directed to the employees based on their perspective towards cybersecurity in business. Now this was another vital question exclusively written in the questionnaire. This question in particular attained a total of 54 respondents with a valid percent of 17.3% that strongly agreed, then 234 respondents with 75.0% basically agreed with the question, then a total of 21 respondents with 6.7% disagreed and then lastly but not the least, out of 312 respondents, 3 of them with 1.0% strongly disagreed with the fact.

Now based on the summary of responses collated, this simply entails that from those responses, the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 288 respondents and were responsive to the fact that indeed they believe only large companies are targeted by hackers and cybercriminals.

Question 22: No this was the last but not the least question to be asked in the questionnaire and it subsequently attained a total of 42 respondents with a valid percent of 13.5% that strongly agreed, then 198 respondents with 63.5% basically agreed with the question, 54 respondents with 17.3% disagreed and lastly 18 out of 312 respondents with 5.8% strongly disagreed.

Now based on the summary of responses collated, this simply entails that from those responses and the highest frequency count for those respondents that agreed (Strongly Agreed & Agreed) was a total of 240 respondents and were responsive to the fact that indeed they were not aware of who is responsible for securing the establishment from cybercrimes.

In conclusion/summary of all results collated, it can be seen that a total of 245 (78.5%) out of 312 participants disagreed to the fact that they are not aware of the company's IT policy. Another total of 234 (75%) participants agreed this time to the fact that they are indeed confident of spotting signs of cyber-attacks. Then again, 218 (69.9%) participants claimed not to know how best they can protect the organization from cybercrimes/attacks. In other words, they agreed to that.

Now in contrast to finding the largest numbers of participants that agreed or disagreed to some questions, 3 lowest values were attained from the results collated. Just 3 (1%) participants out of 312 believed that huge companies are targeted by hackers and cybercriminals. Furthermore, a total of 2 (0.6%) participants strongly disagreed to the question of being worried about damaging the reputation of the company when or after reporting a cybercrime/attack to the police. Then again, 1 (0.3%) individual strongly agreed.

4.2 Analysis of the Result and Hypothesis Testing

In other to test the validity of the hypothesis, analysis using Pearson correlation were performed so as to determine the correlation amongst the variables (dependent and independent). Respectively, the variable (dependent) is based on the "attitude towards cyber security in business (ATC-IB)" while the independent variables are age, gender, position at work and experience. Denotation of the correlation coefficient is known "cc". At this point, we would test two hypothesis one of them possessing the null and the other the alternative hypothesis. Hence if the significant value is virtually less than 0.05, then it shows that its significant and should accept the alternative hypothesis while rejecting the hypothesis possessing the null attributes, In essence " $P < 0.05$ ".

4.2.1 Employees' age on attitude towards cybercrime/cybersecurity

For the first hypothesis, analysis between the employees' age and the attitude towards cybercrime as well as cybersecurity would be carried out using "*Pearson's correlation*" method.

H₀: There is no relevant impact that exists between Employees' age and attitude towards cybercrime/cybersecurity.

H₁: There is relevant impact that exists between Employees' age and attitude towards cybercrime/cybersecurity.

Table 4.2: Pearson's correlation (employees' age and attitude towards cybercrime/cybersecurity in business)

		Correlations	
		ATC-IB	Age
	Pearson Correlation	1	.569**
Age	Sig. (2-tailed)		.000
	N	312	312

*. Correlation is significant at the 0.01 level (2-tailed).

As seen in Table 4.2, Computation so as to analyze the relationship that exists between Employees' age and their attitude towards cybercrime and cybersecurity in business (ATC-IB) more accurately. As seen clearly from the same Table (Table 4.2), there is a moderate positive correlation existing between the two variables (employees' age and ATC-IB) with $cc = .569$, $N = 312$, $P = .000$. Now this analysis clearly states that there is indeed a positive relationship that exists between the two variables that is Employees' age and their ATC-IB respectively with the value quite close to 1. Additionally, Sig. 2-tailed indicates that there is significant relationship between both mentioned variables. Hence, the H₁ of the hypothesis is selected and accepted.

A similar study by Neiss et al. (2009) also proposed the difference in attitude and perception to cybercrime among different age groups. They further stated that the difference is as a result of dissimilarities in perspective between young people and old age group. Younger people are driven by their emotional perception which is different from the older adults.

4.2.2 Employees' gender on attitude towards cybercrime/cybersecurity

For the next hypothesis, analysis between the employees' gender and the attitude towards cybercrime as well as cybersecurity would be carried out using the “*independent t-test*” method.

H₀: There is no relevant impact that exists between Employees' gender and attitude towards cybercrime/cybersecurity.

H₁: There is relevant impact that exists between Employees' gender and attitude towards cybercrime/cybersecurity.

Table 4.3: Statistical difference between employees' gender and attitude towards cybercrime/cybersecurity (Independent t-test)

Gender	N	Mean	SD	Mean Difference	t	P
Male	184	2.94	0.72	.17	-2.30	0.20
Female	128	2.77	0.57			

As seen in Table 4.3, the independent t-test was used so as to analyze the relationship that exists between every gender of the Employees as well as their ATC-IB generally so as to prove consistency. In other-words, the researcher conducted an independent t-test using the main hypothesis earlier mentioned, testing each dimension in order to assess if the hypothesis is valid or not satisfying each parametric test. Referring to Table 4.3 above, Results attained shows that again, there is no significant difference between the two variables ($t = -2.30$, $p=0.20$) in the outputs for males ($M=2.94$, $SD=0.72$) and females ($M=2.77$, $SD=0.57$) in as much as the number of the male counterpart is more than that of the females. Yet again, these clear results show that there is no significant difference between gender and their attitude towards cybersecurity in business-related environments. Furthermore, Sig. 2-tailed indicates that there is significant relationship between both mentioned variables (Attitude towards Cybersecurity in business [ATC-IB] and the gender of every Employee).

On the contrary, a research carried out by Hasanet et al. (2015) proposed that there are discrepancies between females and male's perception to cybersecurity and females are more aware of the cyber regulations and stick to cyber ethical values compared to the male counterpart. Previous literary studies have illustrated that sex group is an often-mentioned demographic background that is related with discrepancies in Life styles. So, in comparison with the previous study by those researchers, it shows that the male counterpart in this study has more attitude projected towards cybersecurity in business than their female counterparts.

4.2.3 Employees' position at work on attitude towards cybercrime/cybersecurity

In this section, analysis between the mentioned variable is been achieved using ANOVA. The research tends to find out if there is any significant value that would stand out between the employees' position at work (Manager, Supervisor, Senior Laborer, and Junior Laborer) and their attitude towards cybersecurity in business (ATC-IB).

H₀: There is no relevant impact that exists between Employees' position at work and attitude towards cybercrime/cybersecurity.

H₁: There is relevant impact that exists between Employees' position at work and attitude towards cybercrime/cybersecurity.

Table 4.4: One-way ANOVA on the impact of the position at work towards the attitude of cybercrime and cybersecurity in business.

	Position	N	Mean	SD	F	Sig.
ATC-IB	Manager	52	0.58	0.491		
	Supervisor	165	2.25	0.745		
	Senior laborer	80	1.88	0.522	3.889	0.009
	Junior laborer	15	0.15	0.647		
	Total	312	1.22	0.515		

*The mean difference is significant at .05 level

From Table 4.4, the impact of the positions at work towards ATC-IB has been analyzed and tabulated and it was used to test the differences between two or more means. A one-way ANOVA between groups analysis of variance was conducted to explore if the position has an impact on the attitude towards cyber-crime and cyber security. Employees (participants) were divided into four groups according to their various positions (Manager, Supervisor, Senior Laborer and Junior Laborer) and as seen, there was a statistically significant difference between position and attitude towards cyber-crime and cyber security with ANOVA statistics ($F = 3.889$, $p = .009$; indicating that $p < .05$).

As we have clearly seen from the same Table (Table 4.4), Post hoc comparisons using Tukey HSD test indicated that the mean score for Manager was ($M= 0.58$, $SD=0.491$), for Supervisor, results show ($M=2.25$, $SD=0.745$), for Senior Laborer ($M=1.88$, $SD=0.522$) and then for Junior Laborer ($M=0.15$, $SD=0.647$). From the results, it can be seen that customers with the Supervisor's position attained the highest mean score (2.25) than the rest in the region of the general attitude toward cybercrime and cybersecurity. Hence, the alternative hypothesis (H_1) which states that there is relevant impact of position at work of employees on s ATC-IB is accepted.

An essential outcome from the exploration the employees' attitude according to a researcher and his team shows the seeming intellect of decentralized obligation they possess as regards responsibilities involving cyber security in an organization. This theoretically aligns with proposals from Tischer al. (2016) that entities are entrusting duties for their cyber security to methodological mediations as well management in senior positions. The approach looks to be that as soon as they resume official duties, they cease to perceive cyber security as their main fear especially when they occupy higher positions. This would also be suitable into a framework based on risk benefit, where some persons that trusts they are well-sheltered by technical involvements offered by their primary organization might in turn employ in an extra dangerous cyber security activity (Hadlington and Parsons, 2017).

Hence, it can be seen from the results obtained in this research that positions at work has an impact towards the attitude of cybersecurity in business today.

4.2.4 Employees' experience on attitude towards cybercrime/cybersecurity

Again, for the next hypothesis, analysis between the employees' experience and the attitude towards cybercrime as well as cybersecurity would be carried out using the "the one-way ANOVA" method. This would ascertain if the experiences of these employees can be influential on the attitude of cybersecurity in business.

H₀: There is no relevant impact that exists between Experience and attitude towards cybercrime/cybersecurity.

H₁: There is relevant impact that exists between Experience at work and attitude towards cybercrime/cybersecurity.

Table 4.5: One-way ANOVA on the impact of the experience towards the attitude of cybercrime and cybersecurity in business.

	Years of experience	N	Mean (M)	SD	F	Sig.
ATC-IB	Less than 5 years	105	0.89	0.501		
	5-10 years	155	1.82	0.534		
	10-15 years	40	1.92	0.513	2.753	0.043
	Above 15 years	12	1.90	0.575		
	Total	312	1.64	0.522		

*The mean difference is significant at .05 level

In Table 4.5, A one-way Analysis of Variance (ANOVA) between groups was conducted to explore if the number of years of experience has an effect on attitude towards cybercrime and cyber security. Participants were divided into four groups according to their years of experience in the organization (less than 5 years, 5-10 years, 10-15 years, and above 15 years). As shown in Table 4.5, there was a significance in their differences with ANOVA statistics ($F = 2.753$, $p = 0.043$ showing that $p < .05$). Again, Post hoc contrasts via Turkey HSD test specified the mean score employees with experience less than 5 years has ($M = 0.90$, $SD = 0.501$), for experiences of 5-10 years, results show ($M = 1.82$, $SD = 0.534$), for 10-15 years ($M = 1.92$, $SD = 0.513$) and then for 15 years and above ($M = 1.90$, $SD = 0.575$). From the results, it can be seen that employees with 10-15 years, attained the highest mean score (1.92) than the rest in the region of the general attitude

toward cybercrime and cybersecurity. Hence, the alternative hypothesis (H_1) which states that there is relevant impact of experience of employees on the ATC-IB is accepted.

4.3 Hypothesis Test Summary

Subsequently, when the “non-parametric” test was carried out on the hypothesis and exactly conferring to the various Tables that has to do with the Employees’ ATC-IB with Age, Gender their respective positions at work and experiences, Table 4.14 undoubtedly portrays if the null hypothesis was retained or rejected and same ideology is applied for the alternative hypothesis.

Table 4.6: Hypothesis Test Summary

Valid Hypothesis	Verdict (Decision)
H_1 : There is relevant impact that exists between Employees’ age and attitude towards cybercrime/cybersecurity.	Alternate hypothesis = Accepted Null hypothesis = Rejected
H_0 : There is no relevant impact that exists between Employees’ gender and attitude towards cybercrime/cybersecurity	Alternate hypothesis = Rejected Null hypothesis = Accepted
H_1 : There is relevant impact that exists between Employees’ position at work and attitude towards cybercrime/cybersecurity.	Alternate hypothesis = Accepted Null hypothesis = Rejected
H_1 There is relevant impact that exists between Employees’ experience at work and attitude towards cybercrime/cybersecurity.	Alternate hypothesis = Accepted Null hypothesis = Rejected

Furthermore, Figure 4.1 vividly exemplifies the block diagram of the summary of the hypothesis results attained earlier with respect to the independent variables (Age, Gender, position at work and Experience) and the dependent variable (ATC-IB).

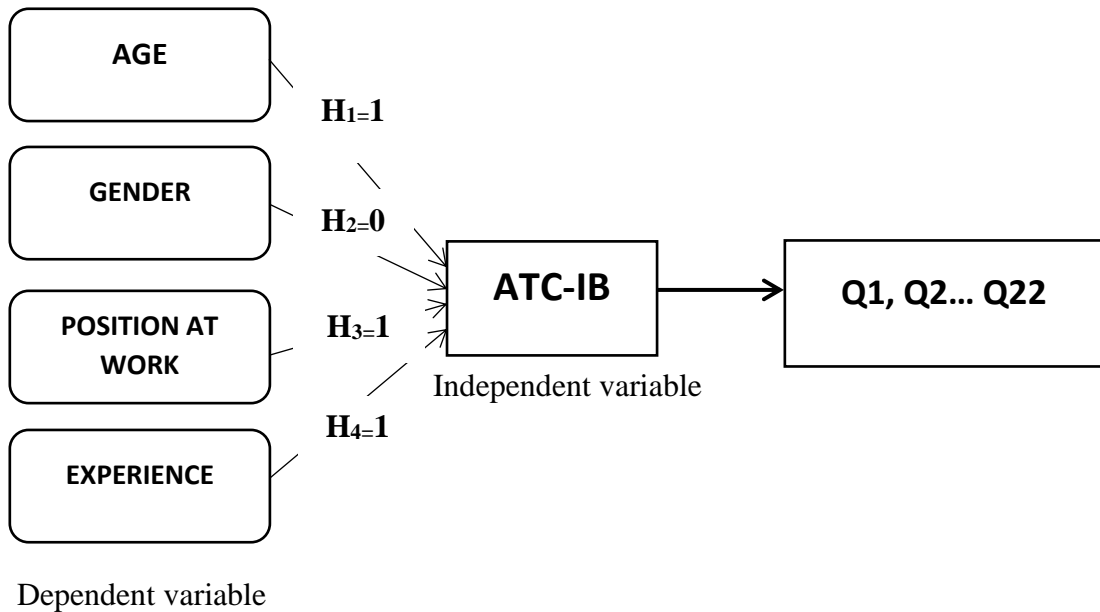


Figure 4.1: Block diagram of the summary of the hypothesis result

Now, with reference to Figure 4.1, it can be seen that the Beta value as regards age frame used in the attitude towards cybercrime/cybersecurity in business “H₁: 0.569 ” is attached to the alternate hypothesis which was accepted, depicting that there was a positive significance and this implies that employees were totally satisfied with the impact of ATC-IB on the ages of the employees in certain organizations.

For the dependent variable gender which is attributed to the null hypothesis accepted, shows that there is little or no significance. Thus, employees had no positive perspective with the ATB-IC with reference to their respective gender.

For the dependent variable position of work this time shows that the significance was positive enough and then gives rise to the fact that the employees, with reference to their various positions, were again quite very satisfied with the general perception of the

Attitude towards Cybersecurity in businesses (ATC-IB) and hence, the alternative hypothesis was accepted.

Lastly but not the least, after the analysis using ANOVA of the last dependent variable experience again shows that the significance was positive enough and then gives rise to the fact that the employees, with reference to their various experience especially when they have more experience in an organization, were again quite very satisfied with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB).

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

In this concluding chapter, all that was obtained as regards results and how they were gotten are discussed here and they are being compared with past results gotten by other researchers.

5.1 Conclusion

As seen in the descriptive analysis, the Pearson correlation analysis as well as the ANOVA detailed analysis, there seemed to be positivity that depicted signs of good attitude towards cybercrime/security amongst employees that were participants in the questionnaires meant for this study. Furthermore, the gender of every Employee basically signifies that the male counter parts (with a descriptive analysis of 184) enjoyed or took part in stating their opinions about their respective attitude towards Cybersecurity in business in various businesses of today.

Additionally, this study has proved via analysis that indeed, these attitudes being showed towards cybersecurity in business is significant as regards the impact it has on Employees with different age, gender as well as different positions at work and various levels of experience.

Four hypotheses were stated in general; Three alternative hypothesis were accepted while just one null hypothesis was accepted. Hence, this study achieved its aim that indicated in general that the attitude towards cybersecurity in business had significant impact on just the Employees Age, Positions at work and Experience except for the Gender of the employee which indicated no impact which led to the null hypothesis being accepted.

With just three (3) dependent variables and one (1) dependent variable, it was noted that the Beta value “ $H_1: 0.569$ ” as regards age frame implemented towards ATC-IB is attached to the alternate hypothesis which was accepted, depicting that there was a positive significance and this implies that employees’ age had relevant impact on ATC-IB. The age in question is basically attributed to every employee in question that had to take out time to fill the questionnaire.

Additionally, for the dependent variable gender which is attributed to the null hypothesis being accepted, shows that there is no positive significance. This simply entails that the gender of every employee that was issued the questionnaire, felt that indeed, no positivity should be maintained towards the attitude of cybercrime/security in business. Thus, these employees' gender produced no significance according to the results in this research on the outcome produced towards the ATC-IB.

For the dependent variable position of work this time shows that the significance was positive enough and then gives rise to the fact that the employees, with reference to their various positions, were again quite very satisfied with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB) and hence, the alternative hypothesis was accepted

Lastly but not the least, after the analysis using ANOVA of the last dependent variable experience again shows that the significance was positive enough and then gives rise to the fact that the employees, with reference to their various experience especially when they have more experience in an organization, were again quite very satisfied with the general perception of the Attitude towards Cybersecurity in businesses (ATC-IB).

Thus, desired outcome by which these corresponding results shows a rather positive significant effect is as follows; that a null hypothesis was accepted (the alternate was rejected) but the three hypotheses as well as the alternates were accepted (their null was rejected). Indicating that the dependent variables (Age, Experience and Position at work) of the employees portrayed a relationship which is quite resilient as regards the Attitude towards the Cybersecurity in today's businesses except for the Employees' gender which showed no positivity towards ATC-IB.

5.2 Recommendations

After series of tests, analysis and verification in this study, it has been noted that in all questions referred to respondents (employees) with respect to the four hypothesis that has to do with the "Age", "Gender", "Position at work" and "Experience" of the Employees in question which was in turn attributed to the Attitude towards Cybersecurity in business, most respondents tend to merely "agree" on the questions provided rather than "strongly

agree". This may be due to the fact that they were not entirely conversant or even satisfied with the attitude in general in connection to Cybersecurity in business so it is recommended that in Libya, introduction and creating some attitudes of some modern technology has to be integrated in our workplaces that would be able to enhance the perception that employees have towards Cybersecurity in businesses of today. This would definitely affect the positivity of the output in our work places. In the case of workplaces already having them, it should better still be improved so as to better the chances of letting employees know that it is key to serve them at all cost.

5.3 Future Study

Again, after verification of results attained in this research, this study's researcher has deemed it fit to suggest that further research be carried out in more cities in Libya to be able to practically analyze and ascertain the impact of any attribute that would be in connection towards the attitude of Cybersecurity in businesses (ATC-IB).

REFERENCES

- Ash, C. G., & Burn, J. M. (2003). A strategic framework for the management of ERP enabled e-business change. *European journal of operational research*, 146(2),374-387.
- Asokhia, M. (2010). Enhancing National Development and Growth through Combating Cybercrime/Internet Fraud: A Comparative Approach. *Journal of Social Sciences*, 23(1), 13-19.
- Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cyber crime in South Africa. *In Proceedings of the 2nd International Conference on Information Management and Evaluation*, 27-28 (p. 62) : Ryerson University, Toronto, Canada.
- Cao, J., & Yang, M. (2013). Energy internet--towards smart grid 2.0. *In Proceedings of 2013 Fourth International Conference on Networking and Distributed Computing* (pp.105-110). IEEE.
- Chen, T., Sanchez-Aarnoutse, & Buford, J. (2011). Network modeling of cyberphysical attacks on smart grid. *IEEE Transactions on Smart Grid*, 2(4), 741-749.
- Deibert, R., & Rohozinski, R. (2010). Risking security: policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1), 15-32.
- Dodel, M., & Mesch, G. (2019). An Integrated Model for Assessing Cyber-Safety Behaviors: How Cognitive, Socioeconomic and Digital Determinants Affect Diverse Safety Practices. *Computers & Security*, 86, 75-91.
- Donalds, C., Osei-Bryson, K. M., & Samoilenko, S. (2019, May). Exploring the Impacts of Intrinsic Variables on Security Compliance Efficiency Using DEA and MARS. *In Proceedings of International Conference on Social Implications of Computers in Developing Countries* (pp. 751-762). Springer, Cham.
- Ericsson, G. (2010). Cyber security and power system communication-essential parts of a smart grid infrastructure. *IEEE Transactions on Power Delivery*, 25(3), 1501-1507.

- Gefen, D., & Straub, D. (1997). Gender difference in the perception and use of e-mail: an extension to the technology acceptance model. *MIS Quarterly*, 21(4), 389-400.
- Gordon, S., Ford, R..(2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2(1), 13-20.
- Hadlington, L., & Parsons, K.(2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security?.*Cyberpsychology, Behavior, and Social Networking*, 20(9), 253-259.
- Hasan, M., Rahman, R., Abdillah, S., & Omar, N.(2015). Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. *Journal of Social Sciences*, 11(4), 395.
- Herath, T., & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.
- Hogan, H. (2013). Met to Tackle the wave of cybercrime with ‘world-leading unit’ published in the Evening Standard, Retrieved 21st, June 2019 from <http://www.standard.co.uk/news/crime/commentary-sir-bernard-hoganhowe-on-new-cybercrime-push-8954716.html>.
- Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice* , 47, 44-57.
- Jahankhani, H., & Al-Nemrat, A. (2011). Cybercrime profiling and trend analysis. *In Intelligence Management* (pp. 181-197)..
- Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Systems*, 35(5), 368-279.
- Lee, H. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346

- Li, C., Chen, C., Lee, C., Weng, C., & Chen, C. (2018). A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. *Soft Computers*, 22(8), 2495-2506.
- Li, C., Lee, C., & Weng, C. (2018). A secure three party node authentication and key establishment scheme for the internet of things environment. *Journal of Information Technology*, 19(1), 147-155.
- Neiss, M. B., Leigland, L. A., Carlson, N. E., & Janowsky, J. S. (2009). Age differences in perception and awareness of emotion. *Neurobiology of aging*, 30(8), 1305-1313.
- Mishra, D., Das, A., & Mukhopadhyay, S. (2014). A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards. *Expert Systems with Applications*, 41(18), 8129-8143.
- Ning, H., Liu, H., & Yang, L. (2013). Cyberentity security in the Internet of Things. *Computer*, 46(4), 46-53.
- Reddy, A., Das, E., Yoon, K., & Yoo, A. (2016). A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. *IEEE Access*, 4394-4407.
- Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
- Shapsough, S., Qatan, F., Aburukba, R., Aloul, F., & Al Ali, A. (2015). Smart grid cyber security: Challenges and solutions. *In Proceedings of 2015 international conference on smart grid and clean energy technologies (ICSGCE)* (pp. 170-175). IEEE.
- Srinivas, J., Das, A., Kumar, N., & Rodrigues, J. (2018). Cloud Centric Authentication for Wearable Healthcare Monitoring System. *IEEE Transactions on Dependable and Secure Computing*, 458-462.
- Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Jouranal of Networking Computer Application*, 34(1), 1-11.

- Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments. *In Proceedings of 2010 International Conference on Availability, Reliability and Security* (pp.196-203). IEEE
- Tischer, M., Durumeric , Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *IEEE Symposium on Security and Privacy*, (pp. 306-319).
- Wang, K., Yu, J., Yu, Y., Qian, Y., Zeng, D., Guo, S.,Wu, J. (2017).A survey on energy internet: Architecture approach, and emerging technologies. *IEEE System Journal*, 12(3), 2403-2416.
- Wazid, M., Zeadally, S., & Das, A. K. (2019). Mobile banking: evolution and threats: malware threats and security solutions.*IEEE Consumer Electronics Magazine*, 8(2), 56-60.
- Zhao, D., Peng, H., Li, L., & Yang, Y. (2014). A secure and effective anonymous authentication scheme for roaming service in global mobility networks.*Wireless Personal Communications*, 78(1), 247-269.
- Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. *In Proceedings of 2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557-564). IEEE.
- Zhou, X., Wang, F., and Ma, Y. (2015). An overview on energy internet, in: *Mechatronics and Automation. In Proceedings of 2015 IEEE International Conference on Mechatronics and Automation (ICMA)* (pp. 126-131). IEEE.

APPENDICES

APPENDIX 1
QUESTIONNAIRE

ATTITUDES OF EMPLOYEES TOWARDS CYBERSECURITY

Dear participant:

The aim of this study ATTITUDES OF EMPLOYEES TOWARDS CYBERSECURITY.

All information you provide in this survey will be protected and not shared with a third party.

Master students: Mohamed Elbelekia 20175286
Assoc. Prof. Dr. Fezile Ozdamli

SECTION A:

Demographics of respondents

Please tick (✓) the appropriate space.

- | | | |
|---|---|---|
| 1- What is your age?
(.....)
Pleas indicate... | 3- what is your level
level of education?
<input type="radio"/> high school
<input type="radio"/> Bachelor
<input type="radio"/> Master
<input type="radio"/> PhD | 5- how long have you
Worked at organization
<input type="radio"/> less than 5 years
<input type="radio"/> 5 to 10 years
<input type="radio"/> 10 to 10 years
<input type="radio"/> 15 years and more |
| 2- What is your gender?
<input type="radio"/> Male
<input type="radio"/> Female | 4- position in organization?
<input type="radio"/> Manager <input type="radio"/> senior labourer
<input type="radio"/> Supervisor <input type="radio"/> junior labourer
<input type="radio"/> Others | |

SECTION: B

Please tick appropriately based on the level of your agreement.

NO	Scale items for the Attitudes towards Cyber security and Cybercrime Questionnaire (ATC-IB).	Strongly Agree	Agree	Disagree	Strongly Disagree
1	I think that management have the responsibility to ensure a company is protected from cybercrime				
2	I am aware of my role in keeping the company protected from potential cybercriminals.				
3	I believe everyone in the company has a role to play in protecting against threats from cybercriminals.				
4	It is hard to know how I can help protect the organization from cybercrime.				
5	I don't have the right skills to be able to protect the organization from cybercrime.				
6	I do not feel that IT security is a priority within my organization.				
7	Computer systems provide all the protection a company needs.				
8	I think that reporting cybercrime is a waste of time.				
9	The Police lack the capacity to deal with cybercrime effectively.				
10	I believe that cybercriminals are more advanced than the people who are supposed to be protecting us.				
11	I worry that if I report a cyber-attack to the Police it might damage the reputation of the company				
12	I think more could be done to communicate the risks from cybercrime to individuals in the organization.				
13	I am aware of the company's IT use policy and attempt to follow it.				
14	I would not know how to report a cyber-attack if one happened.				
15	I don't think that reporting a cyber-attack on the company is my responsibility.				
16	I don't pay attention to company material about the threats				

	from cybercrime.				
17	I am confident that I would be able to spot the signs of a cyber-attack.				
18	I think the biggest threat for IT systems comes from people within the company.				
19	I feel that any individual within the company are at risk of manipulation from confidence tricksters.				
20	I think that cybercriminals only target a company when there is a substantial financial gain.				
21	I believe only large companies are targeted by hackers and cybercriminals.				
22	I don't think I know who is responsible for protecting the company from cybercrime.				

Thank you for participating

APPENDIX 2
ETHICAL APPROVAL LETTER



BİLİMSEL ARAŞTIRMALAR ETİK KURULU

06.05.2019

Dear Mohamed Elbelekia


Your application titled “attitudes of employees towards cybersecurity” with the application number YDÜ/FB/2019/61 has been evaluated by the Scientific Research Ethics Committee and granted approval. You can start your research on the condition that you will abide by the information provided in your application form.

Assoc. Prof. Dr. Direnç Kanol

Rapporteur of the Scientific Research Ethics Committee

Note: If you need to provide an official letter to an institution with the signature of the Head of NEU Scientific Research Ethics Committee, please apply to the secretariat of the ethics committee by showing this document

APPENDIX 3 PLAGIARISM REPORT



[Assignments](#) | [Students](#) | [Grade Book](#) | [Libraries](#) | [Calendar](#) | [Discussion](#) | [Preferences](#)

NOW VIEWING: HOME > THESIS-CIS > MOHAMED ELBELEKIA

About this page
 This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

Mohamed Elbelekia

INBOX | NOW VIEWING: NEW PAPERS ▾

Online Grading Report | [Edit assignment settings](#) | [Email non-submitters](#)

SUBMIT FILE	AUTHOR	TITLE	SIMILARITY	GRADE	RESPONSE	FILE	PAPER ID	DATE
<input type="checkbox"/>	Mohamed Elbelekia	Abstract	0% ■	--	--	<input type="checkbox"/>	1238661470	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia	Chp1	0% ■	--	--	<input type="checkbox"/>	1238661542	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia Mo...	Chp5	0% ■	--	--	<input type="checkbox"/>	1238661678	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia Mo...	Chp3	3% ■	--	--	<input type="checkbox"/>	1238661616	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia Mo...	Allthesis	5% ■	--	--	<input type="checkbox"/>	1238661772	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia Mo...	Chp2	6% ■	--	--	<input type="checkbox"/>	1238661604	29-Dec-2019
<input type="checkbox"/>	Mohamed Elbelekia Mo...	chp4	6% ■	--	--	<input type="checkbox"/>	1238661654	29-Dec-2019