ADENIYI ADEGBOLA
EGBELEKE

INVESTIGATING THE FACTORS THAT PROMOTE
CYBERCRIME AMONG UNIVERSITY STUDENTS

NEU
2019

INVESTIGATING THE FACTORS THAT PROMOTE CYBERCRIME AMONG UNIVERSITY STUDENTS

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

**By
ADENIYI ADEGBOLA EGBELEKE**

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

NICOSIA, 2019

INVESTIGATING THE FACTORS THAT PROMOTE CYBERCRIME AMONG UNIVERSITY STUDENTS

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

By
ADENIYI ADEGBOLA EGBELEKE

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

NICOSIA, 2019

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: Adeniyi Adegbola Egbeleke

Signature:

Date:

ACKNOWLEDGEMENTS

I want to give my appreciation to my great supervisor Prof. Dr. Nadire Cavus, who helped me through all the stages of this Thesis by her continued engagement, support, guidance and tolerance during the process.

I would also like to thank Prof. Dr. Dogan Ibrahim and Assist. Prof. Dr. Seren Basaran for contributing immensely to my knowledge during my Masters' degree at Near East University.

To all my fellow student and staff of the Department of Computer Information Systems and the faculty as a whole, I will like to thank you all for being in my life during my educational journey and helping me grow.

Most importantly, to my dearest parents who were there for me from the beginning to the end of my studies. I will like to thank my friend who helped me through sharing of my questionnaires and data collection as it would have been very stressful without their help.

Finally, I give thanks to the Almighty God for giving me life and strength of good health to complete this thesis.

To my family...

ABSTRACT

The main aim of this study is to investigate the factors that promotes cybercrime among university students. The study purposed to design and test a model that explains the factors that contribute to the intention to commit cybercrime, to ascertain the relationship between the identified factors and perceived cybercrime stimulus. Descriptive survey was adopted as the research design. Random sampling technique was used to select 380 students from Near East University, North Cyprus. Questionnaire was the instrument used for data collection. All hypotheses were constructed based on the previous literature and proposed research model of the study. In order to investigate the relationship between the perceived cybercrime stimulus variable and behavior intention, Pearson correlation was employed and conducted using SPSS. The result indicated that all hypotheses were accepted. It was found out that five factors, which are technological support, peer influence, law and enforcement, technology inclination and economic situation positively influence perceived cybercrime stimulus. Perceived cybercrime stimulus was also found to have a strong positive relationship with behavior intention. Because of lack of existing model to explain the factors that promote cybercrime, this study proposed a model for explaining the factors that promotes cybercrime. We hope that this study helps to enlighten and inform students on the punishment that awaits cybercrime behavior and inform parents and guardians about the factors that makes their ward involve in cybercrime.

Keywords**:** Cybercrime; cyberbully; cyberstalking; internet crime; internet usage; online crime

ÖZET

Bu çalışmanın temel amacı, üniversite öğrencileri arasında siber suçun artmasına neden olan faktörleri araştırmaktır. Çalışmada, siber suçun işlenmesine katkıda bulunan faktörleri açıklayan bir model tasarlamak ve test etmek, belirlenen faktörler ve algılanan siber suç uyarıcıları arasındaki ilişkiyi belirlemek amaçlanmıştır. Araştırma modeli olarak betimsel araştırma modeli kullanılmıştır. Kuzey Kibris Cumhuriyeti Yakın Doğu Üniversitesi'nden 380 öğrenci seçmek için rastgele örnekleme tekniği kullanılmıştır. Veri toplama araci olarak anket kullanilistir. Tüm hipotezler, literatüre dayanarak olvşturuldu ve çalışmanın araştırma modelini test etmek için kullanildi. Algılanan siber suç uyaran değişkeniyle davranış niyeti arasındaki ilişkiyi araştırmak için SPSS kullanılarak Pearson korelasyonu kullanıldı ve uygulandı. Arastirmanin sonunda, tüm hipotezlerin kabul edildiğini belirlendi. Teknolojik destek, akran etkisi, yasa ve uygulama, teknoloji eğilimi ve ekonomik durum olan beş faktörün algılanan siber suç uyaranını olumlu yönde etkilediği sonucuna varilmistir. Algılanan siber suç uyaranının da davranış niyeti ile güçlü bir pozitif ilişkisi olduğu bulunmuştur. Siber suçu teşvik eden faktörleri açıklamada mevcut model bulunmamasından dolayı, bu çalışma siber suçu teşvik eden faktörleri açıklamada bir model önermiştir. Çalışmada elde edilen sonuclarin, öğrencileri siber suç davranışını bekleyen cezalar üzerine aydınlatmaya ve bilgilendirmeye yardımcı olmasi yaninda öğrencilerin velilerinin de bu faktörler hakkında bilgi sahibi olmalarina yaridimci olacaği umut edilmekterdir.

Anahtar Kelimeler**:** Siber suç; cyberbully; İnternet'ten taciz; internet suçu; internet kullanımı; çevrimiçi suç

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

CHAPTER 2: RELATED RESEARCH

CHAPTER 3: CONCEPTUAL FRAMEWORK

CHAPTER 4: RESEARCH METHODOLOGY

CHAPTER 5: RESULTS AND DISCUSSIONS

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

APPENDICES

LIST OF TABLES

LIST OF FIGURE

LIST OF ABBREVIATIONS

BI:	Behavior Intention
ES:	Economic Situation
LE:	Law and Enforcement
NCA:	National Crime Agency
PI:	Peer Influence
SPSS:	Statistical Package for Social Sciences
TAM:	Technology Acceptance Model
TI:	Technology Inclination
TS:	Technological Support

CHAPTER 1

INTRODUCTION

This chapter presents the general overview on the factors that promotes cybercrime among university students.

1.1 Overview

Crime is not new, it started since the creation of humans and it pose a great challenge and threat to the expected human and environmental development. Nations all over the world have used diverse strategy to combat crime based on the intensity of the crime, simply put no country can experience growth or progress with too many crimes. This is because crime destroys what has been developed and makes the country move a step forward and three steps backward, creating serious negative effect on the economic and social aspect of a nation. Another face of crime is being committed over the internet.

The growth of the internet has paved way for new and countless free website over the internet. Along this line, the internet has created another avenue for internet crime known as the cybercrime. Cybercrime is a crime perpetrated using computer tools on the internet. Cybercrime is also referred to as a crime committed using computer and network. The first cybercrime recorded can be dated back to 1820 during the days of abacus computer. The first spam mail was sent over the Arpanet in 1976. The creation of EIK cloner by Rich Skrenta in 1982 brought about the first computer virus spread. The improvement of technology saw programmers writing malicious programs to intercept computer operations (Srikanth et al., 2017).

In today's era of communication, the rate at which companies depend on the internet has raised the security risk involved. Many companies now store important information on the internet as it appears to be cheaper and accessible anywhere especially multinational companies with branches in different countries (Kamini, 2011). This has in many ways increased the risk associated with cyberspace. The rate of online crimes is increasing daily even in the school settings; the student manipulates their grade from the system (Sumanjit and Tapaswini, 2013).

Cyber criminals are now advanced in their operations by targeting both the internet users and organizations. Large corporations have experienced the attacks by cyber criminals in the past. For example, the account of the department of revenue in South Carolina was hijacked in 2012 by gaining access into their computer and stole more than 3 million social security numbers and over 350,000 credit card numbers (Muthusankar et al., 2016). Many times account hijack happens when malicious software are being installed on the victim's computer through mail attachment. The software logs the keys entered into the computer and makes them have access to their password that can be used to access their computer anytime.

Since the advent of internet, the youth has dominated the internet space as they use the internet more than any age group. This has been because of the use of internet for academic, entertainment and social purposes. It is unfortunate that many youths go beyond the benefit the internet offers to using the internet as a medium of committing crime. This study examines the factors that promotes cybercrime among university students.

1.2 Problem Statement

Cybercrime is the new face of crime that can also be called digital crime. The problem of cybercrime has become a serious concern to governments, organizations and individuals over the years. The problem of cybercrime has been increasing and it remains difficult to put a definite end to. This is because the crime can be conducted from any part of the world anonymously. Cybercrime has cost government, organizations and individuals' loss of billions of dollars years, as at 2017, the total loss per year to cybercrime globally had risen to $600 billion (Carlos et al., 2017).

It is not surprising that large number of youths are involved in cybercrime as they are found to constitute the largest user of the internet. According to the NCA report (2018), the average age of people involved in cybercrime are between the ages of 17 and 22 years. This implies that the youths especially the university students dominates the population of cybercriminals. Various studies (Lowry et al., 2016; Emma et al., 2015; Matti et al., 2015) have been conducted to examine cybercrime of different forms among university students. All these studies have focused mainly on a fraction of cybercrime either cyberstalking or cyberbullying among the students. Also, there are studies on the outcome and effect of cybercrime but there are limited studies on the factors that promotes cybercrime among university students. Many of the studies have only examined the awareness of cybercrime among the students; the reason students avoid online services and cybercrime victimization among the students. It is in this light that this study seeks to bridge the research gap to examine the factors that influence cybercrime act among university students.

1.3 Aim of the Study

This study investigated the factors that promotes cybercrime among university students using Near East University, North Cyprus as the research settings.

1.4 Importance of the Study

Cybercrime among the youth have been on the rise recently as cases of cybercrime among the youths are reported on daily basis. However, limited studies were found to examine the factors that promotes cybercrime among the university students. A study by Markus and Rainer (2015) extended the TAM to examine online service avoidance in the light of cybercrime but no study was found to have adopted TAM to particularly investigate the factors that promotes cybercrime among the youth. The originality of this study is investigating the factors that promotes cybercrime among university students. This is important because limited studies exist on the factors that cause or promotes cybercrime among university students. As a result of this, this study is important to fill this gap to provide answers to the factors that promotes cybercrime among university students.

1.5 Limitations of the Study

The researcher encountered some limitations in the course of conducting this study. It is important to note the limitations encountered during this study to help future studies on the same research area. The following limitations encountered are noted:

The limitations of the study:

i. This study is limited to university students in Near East University North Cyprus.

ii. The study duration for this study does not give room to examine multiple countries as it was conducted during the spring semester considering the time and the limited resources to extend the study to other countries. If the study is conducted in the future, extending the study to multiple countries will investigate further the factors that promote cybercrime among university students in different countries.

iii. The number of students covered were limited to Near East University North Cyprus. If other universities are covered, more insight about the topic will be gained.

iv. There is limited model to explain the factors that promotes cybercrime among students.

1.6 Overview of the Thesis

Chapter 1 examined the overview of cybercrime and further defining the problem of the study, the aim of the study, the importance of conducting the study and the limitations of the study. The first chapter lays the background for the study by explaining the overview of crime and cybercrime.

Chapter 2 presented studies on cybercrime and related studies on the factors that promotes cybercrime among the youths. Previous studies carried out on the research area are examined and the missing gaps in the literature are ascertained. The second chapter specifically examined the cyberstalking among the youth and cyberbullying among students.

Chapter 3 presented the conceptual framework of the study by examining the various concepts of cybercrime, the types of cybercrime, the problems associated with cybercrime and the reason undergraduate students involve in cybercrime. Specifically, the third chapter examines types of cybercrime such as hacking, virus dissemination, logic bombs, denial of service attacks (DOS), phishing amongst others. The chapter further presents the reasons for undergraduate students involving in cybercrime and the problem associated with cybercrime.

Chapter 4 is based on the research methodology of the study, as it examines the research model, which guided the study, the research hypothesis that was stated to achieve the aim of the study, the participants, and how the participants were selected, the data collection tools, data analysis method and the procedures followed to conduct this study.

Chapter 5 presented the study findings and discussion. The fifth chapter presented the result of the analysis conducted on the data collected for the study. The hypotheses stated were tested in order to ascertain the factors that promote cybercrime among university students. The results were explained and the similarities of the results to previous studies were ascertained.

Chapter 6 made conclusion on the study and provides recommendations. The final chapter of the thesis concludes the study by examining the outcome of the study in relation to the aim set for the study. The chapter finally recommends solutions to minimize the various factors found to promote cybercrime among university students.

CHAPTER 2

RELATED RESEARCH

This chapter presents previous studies that have been carried out related to cybercrime. The studies are examined to gain in-depth knowledge about the outcome of past studies and the gaps between the studies.

2.1 Cyberstalking Among Youths

Catherine et al. (2014) examined juvenile and cyberstalking occurrence in the United States. The aim of their study was to determine the predictor of cyber stalking behavior among juveniles below the age of 18 years. One thousand six hundred and sixty nine high school students were selected for the study and data was collected using a structured questionnaire. The data collected was analyzed using multiple regression. They found that association with deviant peer and lack of self-control contributed to cyberstalking behavior among juveniles. They recommended that school management should organize a program to sensitize the students on the punishment with cyber stalking, and also cognitive training of self-control should be done to enhance the self-control of the juveniles.

Emma et al. (2015) conducted a study to examine the experience and effect of cyber stalking on victims. Three hundred and fifty three participants were surveyed using online questionnaire. Descriptive statistics was used to analyze data collected, they found that cyber stalking has effect on the mental health of the victims; they also found that victims of cyber stalking experience high level of psychological distress.

Berry and Bainbridge (2017) examined the relationship between cyberstalking victimization and demographic. Hundred people who use internet frequently were surveyed to ascertain their cyberstalking experience and determine if any relationship exist between their demographics and victimization. They found that cyberstalking experience of internet users varies according to their gender. Female tend to have more experience of cyberstalking than male internet users.

Michael (2018) conducted a study that examined how cyberstalking leads to depression among adolescent in United States. He focused on determining the relationship between cyberstalking and unhappiness of victims. Four hundred and thirteen students were surveyed and data collected were analyzed using descriptive statistics. He found out that depression is a serious effect of cyberstalking among adolescents and having such experience has a psychological effect on the victim.

Bradford (2019) examined cybercrime perpetration among college students in Midwest United States. He focused on ascertaining the characteristics of college students who engage in cyberstalking. He found out that cyberstalking behavior is associated with students with low self-esteem and female college students appear to have more low self-esteem while low self-esteem is less related to cyberstalking among male students.

2.2 Cybercrime and Internet Usage

Diana and Sheri (2015) conducted a study to examine the effect of social media engagement on cybercrime involvement among youths. They purposed to examine how sharing of passwords among friends increase the involvement. Data was collected from 1272 youths from grade 3 to 8 and the data was analyzed using descriptive statistics. They found that sharing of passwords among youths is unrelated to cyberbullying involvement. They concluded that youth might have learnt from their previous experience not to share their password and to be careful when on social media.

Markus et al. (2015) examined how cybercrime risk contributes to online service avoidance. Their aim was to identify the factors that reduce the intention of users to use internet services. Survey research method was used to collect quantitative data from 26,593 respondents from all the 27 EU member states. The data was analyzed using structural equation modelling analysis. At the end of the study, they found that perceived cybercrime risk has a negative impact on internet use by respondents. They furthered revealed that only confident users perceive less cybercrime risk when using the internet to extent of shopping online.

Matti et al. (2015) conducted a study that examined the victimization of cybercrime among young people in different nations. The aim of their study was to determine the common cybercrime in the selected countries and the predictors of these crimes in the countries.

Quantitative data was collected from 3505 participants in Finland, US. Germany and UK within the ages of 15 and 30 years. Data was analyzed using descriptive statistics. They found that threat of violence were common in the countries while they experience less of sexual harassment. They found that gender, age, immigration background, unemployment are predictors of cybercrime that are significant to victimization.

Filipa and Marlene (2016) examined fear of internet usage among adolescent in Portugal. They aim of their study was to examine the fear of online usage due to previous cyberstalking experience. Six hundred and twenty seven adolescent were surveyed for the study. They found that more than half of the adolescent sampled have been victim of cyberstalking in the past and the experience they had create fear that make them feel reluctant to make use of the internet.

Ian (2017) investigated the fear of internet use due to previous cybercrime experience. He opined that people with previous experience of cybercrime are more careful when using the internet even if they are able to recover in the shortest time. He furthered that the fear of cybercrime arise from the psychological effect of the past occurrence, which the victim believes may reoccur if he continues to use the internet.

Suvi (2017) also examined the fear of cybercrime and the avoidance to use internet among European internet users. He aimed at examining the response of internet users to previous cybercrime experience and how it affects their future use of the internet. He found that, cybercrime victims tends to have fear to make use of the internet because of previous experience of cybercrime as a way of avoiding future occurrence.

2.3 Cyberbullying Among Students

Ruth et al. (2013) examined the relationship between peer influence and cyberbullying among high school students in Germany. They conducted the study to ascertain the forms of peer influence that promotes cyberbullying among high school students. Quantitative data was collected from 276 high school students from the ages of 13 to 19 years using questionnaire as the instrument for surveying the students. Data collected was analyzed using multiple logistics regression analysis. They found that class context contributes to cyberbullying behavior among the students. They also found that the number of cyberbullies in the classroom contributes to influence on other’s behavior. They furthered that the use of social media contributes to cyberbullying and the time spent on the social media increases the risk of victimization among the youngsters.

Hannah et al. (2016) examined the impact of disclosure of cyberbullying on seeking revenge for victims. They aimed at examining whether disclosing cyberbullying incident will make others to commit the act as a way of seeking revenge for the victim. They surveyed 118 Facebook users and the data was analyzed using descriptive statistics. They found out that no relationship exist between cyberbullying incident and seeking revenge by people. This implies that disclosure of cyberbullying incident does not increase the intention to seek revenge.

Lowry et al. (2016) conducted a study that investigated why adults involve in cyberbullying on social media. They aimed at addressing why people are socialized into the act of cyberbullying. Both secondary data and online questionnaire survey were used to collect data from 1003 adults. The data was analyzed using partial least square regression they found that constant social media use combined with anonymity factor social media facilitates cybercrime among adults. They concluded that when adults experience positive outcome from cyberbullying they tend to continue the act.

Sara et al. (2016) examined the effect of cyberbullying exposure on adolescent moral evaluation. they aimed at understanding whether frequent exposure to cyberbullying influence adolescents to bully others online. They surveyed 1412 adolescent between the ages of 10 to 13 years. Descriptive analysis was used. At the end of the study, they found that multiple exposure to cyberbullying increases the chances of adolescents bullying others online

Sebastian et al. (2016) conducted a study to examine the relationship between cyberbullying, victimization, self-esteem and cyber groomer. They sampled 2162 teenagers in the ages of 11 to 19 years from Netherland, Germany and United States. Descriptive statistics was used to analyze data. They found that cyberbullying victimization and low self-esteem contributes to cyber groomer victimization. They recommended that parents and guidance should educate their child and wards on the risk of cyber grooming.

Christopher and Christiana (2017) examined the variables that determine cyberbullying among youth. They used Barlett and Gentile's model to understand the different variables that determine cyberbullying behavior among the youth. They surveyed 167 youth and 552 adults within the ages of 17 to 36 years. Regression analysis was used to analyze the data for the study. At the end of the study, it was found that cyberbullying starts from the youth age up until the adulthood.

Binesh et al. (2018) examined the use of social media for collaborative learning and the effect of cyberbullying on the success of using social media as a tool for learning. They surveyed 360 students from the bachelor's level to PhD level. Descriptive analysis was used to analyze the data collected. They found that social media serve as a tool for improving learning environment of students. They also found that cyberbullying affects the positive relationship between social media and improved learning environment of students.

Diana and Sheri (2018) examined the effect of parental control on cyberbullying involvement among youths. They sampled 800 youth s from the classes of grade 3 to 8 in southwestern United States. Descriptive analysis was used to analyze data collected. They found that parental control affects the involvement of youths in cyber bullying.

2.4 Summary

Previous studies related to cybercrime have been examined in this chapter. Many of the studies conducted have focused on the types of cybercrime and the effect on online users. Studies such as Ruth et al. (2013); Hannah et al. (2016); Lowry et al. (2016); Sara et al. (2016); Sebastian et al. (2016); Christopher and Christiana (2017) focused on cyberbullying and the effect on the juvenile, youths and adults. Other studies such as Catherine et al. (2014) and Emma et al. (2015) focused on cyberstalking among the youths. Studies from Diana and Sheri (2015); Markus et al. (2015); Matti et al. (2015) focused on cybercrime and internet usage. These studies did not specifically examine the factors that promotes cybercrime among the youths or students. Because of this gap, this study is conducted to bridge this research gap to examine the factors that promote cybercrime among university students.

Table 2.1 Summary of related research

Author	Research Type	Demography	Cybercrime Evaluated
Bradford (2019)	Quantitative	Youths	Cyberstalking
Diana and Sheri (2018)	Quantitative	Youth	Cyberbullying.
Binesh et al. (2018)	Quantitative	Youth	Cyberbullying.
Micheal (2018)	Quantitative	Juvenile	Cyberstalking
Berry and Bainbridge (2017)	Quantitative	Youth	Cyberstalking
Christopher and Christiana (2017)	Quantitative	Adult	Cyberbullying.
Ian (2017)	Quantitative	Youth	Cybercrime fear
Suvi (2017)	Quantitative	Youth	Cybercrime fear
Filipa and Marlene (2016)	Quantitative	Juvenile	Cybercrime fear
Sara et al. (2016)	Quantitative	Juvenile	Cyberbullying.
Hannah et al. (2016)	Quantitative	Youth	Cyberbullying.
Lowry et al. (2016)	Quantitative	Adult	Cyber bullying.
Sebastian et al. (2016)	Quantitative	Juvenile	Cyberbullying.
Diana and Sheri (2015)	Quantitative	Youth	Cybercrime involvement.
Emma et al. (2015)	Quantitative	Adult	Cyberstalking.
Markus et al. (2015)	Quantitative	Adult	Cybercrime risk.
Matti et al. (2015)	Quantitative	Adult	Predictor of cybercrime.
Catherine et al. (2014)	Quantitative	Juvenile	Cyberstalking.
Ruth et al. (2013)	Quantitative	Youth	Cyberbullying.

CHAPTER 3

CONCEPTUAL FRAMEWORK

This chapter presents the concept around cybercrime. The chapter goes on furthers to explain the various types of cybercrime, the problem associated with cybercrime, statistics of global cybercrime and the reasons for undergraduate involving in cybercrime.

3.1 Cybercrime

The introduction of technology and internet has made the world a global village. From the comfort of one's home, people can view what is going on in another country, interact with people from another country or race and conduct business tractions with ease. The internet and its technologies has a great impact on individual and nations. This impact has taken different forms. Cyber activates have both the positive and negative effect on the users as an individual, organizations as a group and nations at large. Because of no or insignificant barrier to the use of the internet and its technologies, it has become an open field for everyone, which makes people to use the internet for good and bad intentions. The internet, which remains one of the best element of information technology human existence has experienced, continue to present humans with endless opportunities but the goodness of it have been hijacked by some bad people known as cyber criminals who use the internet for malicious activities.

Amit and Neerja (2017) defined cybercrime as a crime that involves computer and network. They furthered that it is an attack that target information of organizations, individual and government. This attack does not come in form of a physical attack but as a virtual attack on the victim. The main tool used by the perpetrators is the computer. The computer serves as the cover that the cybercriminals hide behind. Cybercrime are of different types such as identity theft, internet fraud, credit card fraud, hacking, phishing, cyberbullying amongst others. All crimes committed over the internet can be categorized as a cybercrime.

Cybercrime also known as a computer-based crime is broadly defined as any crime that involves the use of computers and network. The definition of cybercrime as computer-based crime means that computer may be used for the crime, or a computer is at the receiving end of the crime (Sabillon et al., 2016). Saragih and Siahaan (2017) defined cybercrime as computer related crime that are committed against individual or group with the intention of causing harm to the victim mentally, physically or even financial loss. Cybercrime is capable of affecting the health of the victim. In the case of organizations, cybercrime is capable of causing financial loss or proprietary data loss that may affect the reputation of the organization. Cybercrime are mostly performed over the internet. This is due to the number of daily internet user globally and the reliance on the internet for business transactions and personal communication.

Cybercrime have taken different forms over the years. The initial known cybercrime was the act of hacking that is to gain access into a system without authorization. Cybercrime has taken different forms to include the emotional and sexual abuse of online users over the internet, the use of internet to propagate war and terrorism, the use of internet to bully other users, the use of internet to distribute licensed and copyrighted products, and the use of internet for romance fraud. Virtually all the physical crimes committed before the advent of internet are now being carried out over the internet. The challenges of curbing this crime is the anonymity features of the internet where anyone can sit behind the computer and do anything in hidden.

As reported by MCafee (2014), cybercrime caused the word economy up to the tune of $445 billion as at the end of 2014 of which about $1.5 billion was lost in the U.S to online credit card fraud. As at 2018, the total loss per year to cybercrime globally had risen to $600 billion (Carlos et al, 2017). This cybercrime has posed serious threat to many industries in particular the banking industry. Apart from the financial loss due to cybercrime, cybercrime has caused psychological and emotional damage to many internet users from children to adult age. The various forms of cybercrime are explained in the next section below.

3.2 Types of Cybercrime

Cybercrime as an act takes different forms. Cybercrime simplified as crime committed over the internet or use of computer and network is committed in different ways on the internet. Although a crime is a crime but some of the cybercrime have great effect than others. The different types of cybercrimes as are explained below.

3.2.1 Hacking

Hacking is gaining access to someone's computer without the permission of the owner of the system. Hacking is a popular cybercrime act that has been in existence since the invention of computer. People behind hacking are called hackers. Hackers are mostly computer programmers who have enough knowledge and skills about computer system and make use of this knowledge for harming others. Another variation of hackers is crackers or black hat but seek the knowledge for curiosity sake. Teenagers and the youths are very curious of learning the trick behind hacking. The intention to learn hacking is into either for fun or for personal benefits. Since inception, hacking has been a global threat to both organizations and to individuals who store personal data on the internet (Alsalim et al., 2017).

3.2.2 Virus dissemination

Another popular form of cybercrime is the dissemination of virus over computers connected to a network. Viruses are also computer program developed by a programmer but for evil intention to corrupt a file or system. Computer virus can be spread though mail attachment, by clicking of links or by downloading a wrong or pirated software. Virus works in different ways. First by hijacking the stored data of the system then infecting the file to be unreadable or even entirely wiping the file totally. Another look alike of virus is the worm, the worm gets to the computer just as the virus gets to the computer but instead of attaching to a file, it multiplies itself to eat up all the memory storage of the computer thereby causing it to crash operations (Srikanth et al., 2017).

3.2.3 Logic bombs

An infamous cyber-attack is the logic bomb. The logic bomb is a malicious code inserted into a software for it to start work once the software runs. It cannot be called a virus but also got entrance into a system just the way a virus behaves. Logical bombs are executed when a user unknowingly downloads a malicious software and runs it on his computer. Once the malicious software is installed on the user's computer, it starts to affect the operating system of the computer. This may include messing up the data on the computer, running third party software without authorization or even crashing the operating system (Bobby, 2017).

3.2.4. Denial of service attack (DOS)

Another popular cyber-attack is the denial of service attack. The main aim of this attack is to prevent the computer of a user to gain access to some resources on the network. The denial of service attack floods the user’s computer with excessive request that surpasses what the computer can process at a time making the system to slow and unable to access the needed resources on the network. Denial of service attack use up all the resources available on the network to deny other users access to the computer. Denial of service attacks are strategy to steal information from a system as a backdoor mechanism to gain access into a system (Deshmukh and Devadkar, 2015).

3.2.5 Phishing

Phishing is another common cybercrime committed over the internet. The aim of phishing is to direct a user to a fake and look alike of an original website so that the user can provide the personal information to the phishing website unknowingly. It is most time used to get username and passwords, bank details of users, credit card details and other confidential information. The disguising nature of phishing attacks makes victims to fall easily to fake website used for stealing personal information of users. Phishing has cost big corporations and rich individuals millions of dollars as they are diverted to a a phishing website to make payment for business transactions which turns out to be fake (Lastdrager, 2014).

3.2.6 Email bombing and spamming

Another common cybercrime attack is the email bombing. Cyber criminals perform this act by sending large amount of emails to a target address repeatedly causing the mail server to crash. The content of the mails is irrelevant and usually very longer than what a server can process thereby causing server shutdown. Spamming is another aspect of this where the cybercriminals send unsolicited messages to the recipient consecutively. These messages are many times not requested by the recipient and can be unrelated to the recipient’ interest operations (Srikanth et al., 2017).

3.2.7 Web jacking

Web jacking is another serious cybercrime act. The cyber criminals take control over a website and mess it up writing irrelevant content on the website. In some cases, the cybercriminal redirects the visitors of the website to another website created and managed by him. Webjacking operates similar to similar hijacking of vessels or aircraft which diverts the aircraft and the passengers to a different destination. Different cases of web jacking have been reported such as the hijacking of popular blogs and company website and many more. When web jacking occurs, the owner of the website will not be able to get access to the administrative section of the website as all is taken over by the cybercriminals (Animesh et al., 2017).

3.2.8 Cyberstalking

Cyberstalking is a new crime online where the criminal follows and monitors the victim just as criminals monitor and tails victim in physical world, then the cybercriminal make use of the victims online activities and information to harass the victim and make verbal threats and intimidation operations. Cyberstalking has a serious psychological effect on victims as many who have the experience feel depressed after the occurrence. Cyberstalking also makes users to have fear of using the internet in the future as they try to be careful of any future victimization (Emma et al., 2015).

3.2.9 Cyberbullying

Cyberbullying is the use of information and Communication Technology to abuse or harass another person. Cybercrime is also known as cyber harassment or online bullying. A common definition of cybercrime is the intentional or aggressive behavior that is performed repeatedly over the internet by an individual or group against a person who cannot defend him or herself (Pettalia, 2013). The national crime commission defined cybercrime specifically to the process of using mobile phone to send posts or messages with the intention to harm or harass another person (Moreno, 2014). Cyberbullying commonly occurs on the social media sites when a teenager bullies or harasses his or her fellow online users. Cyberbullying is perpetrated through posting rumors, threats, hate speech or even sexual remarks about another online user. The main intention of

Cyberbullying is to harm the victim. The effect of cyberbullying ranges from low self-esteem, depression to even suicidal ideation.

3.2.10 Identity theft and crediting card fraud

Another popular cybercrime attack is identity theft and credit card fraud. Cybercriminals perpetrate this by stealing the identity of people to gain access to a system. The identity the criminals steal are credit cards, bank details and names. The details of the victims stolen are used to impersonate the victim in making transaction under the disguise of the real owner of the information. Popular ways cybercriminals make use of personal and bank details stolen are for making inline purchase. The banking industry has lost millions of dollars due to identity fraud in recent decade (Animesh et al., 2017).

3.2.11 Salami slicing attack

Salami attack is an attack that cybercriminals also use in stealing from the victim. The criminals steal money bit by bit that the owner will not notice. Salami attack is very common in the banking industry as they have large amount of customers who save their money with the bank. In many cases the bank customer account is the target of the attackers. Since banks make calculation by rounding off the figure to the nearest number, the remaining money is not taking accounted for or ignore. Salami slicing attack is unnoticed if organizations do not make proper auditing of their company account periodically. Salami attack sometimes go as far as months or years before being noticed by the organization that is the victim (Sai et al., 2014).

3.2.12. Software piracy

Software piracy is a very common type of cybercrime that many young ones are unintentionally involved in. software piracy is the unauthorized use of software or the unauthorized duplication of a licensed software. Any distribution of software without the permission of the owner is called piracy. Software piracy is widespread on the internet and there are lots of website that people can download cracked version of a licensed software. This affects the owner of the software as it reduces the expected revenue from the work done operations (Srikanth et al., 2017).

3.3 Global Cyber Attacks

Cyber attacks have been of concern to corporations large or small and individuals. The development of internet technologies has seen a rise in the number of attacks experienced by organizations and individuals. Cyber attacks have focused on different IT environments. The results from Figure 3.1 shows the IT environment targeted by cybercrime globally in the year 2017 by industry. The retail and payment industry recorded more attack from the e-commerce platform, hospitality industry recorded more attacks from the point of sale platform, finance and insurance recorded more from the corporate and internal network side, food and beverage industry also recorded more attacks from the point of sale platform, service provider recorded more attacks from the corporate and internal network side, professional services, healthcare and others also recorded more attacks of 15% from the corporate and internal network side

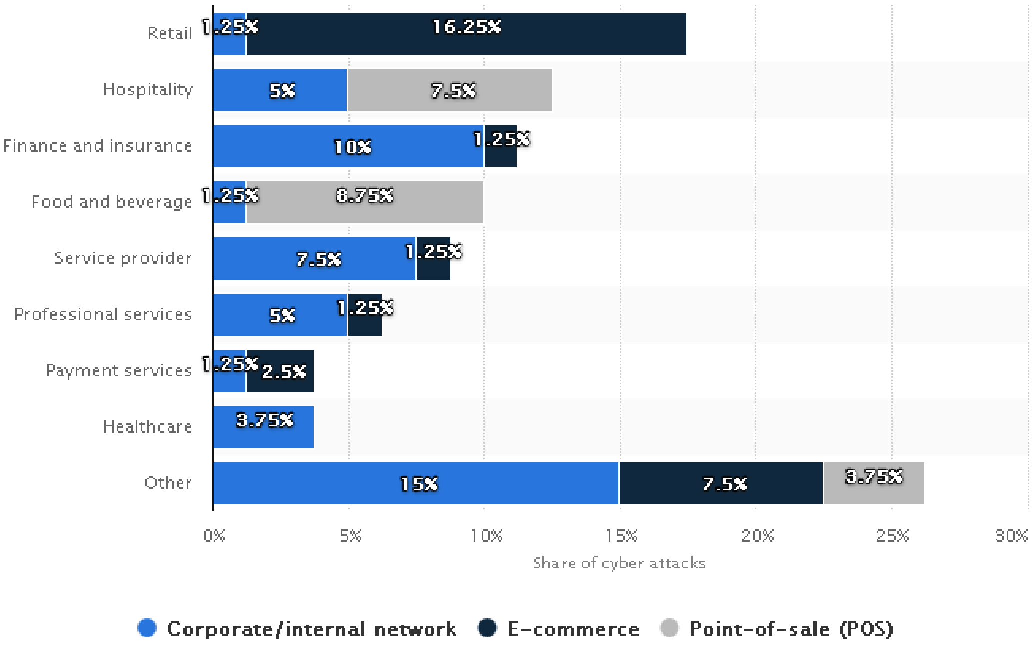


Figure 3.1: IT environments targeted by cyber-attacks worldwide in 2017, by industry (Statista, 2018)

Cyber attacks as earlier stated is global issue of which no region is exempted. All regions of the globe have experienced cyber attacks but varies in the degree or amount cyber attacks recorded. The results from Figure 3.2 also shows the IT environment targeted by cybercrime globally in the year 2017 but by region. The North America region recorded

36% attacks from the corporate and internal network side, 22% attack from the e-commerce platform and 42% attacks from the point of sale platform. The Asia pacific region recorded 67% attacks from the corporate and internal network side and 33% from the e-commerce platform. The Europe Middle East and Africa recorded 61% of attack from the corporate and internal network side and 39% from the e-commerce platform. Latin America recorded equal cyber-attack from the ecommerce platform and the point of sale platform of 50% each. This implies that the Asia Pacific experienced more of cyber attacks within the year 2014 to year 2017.

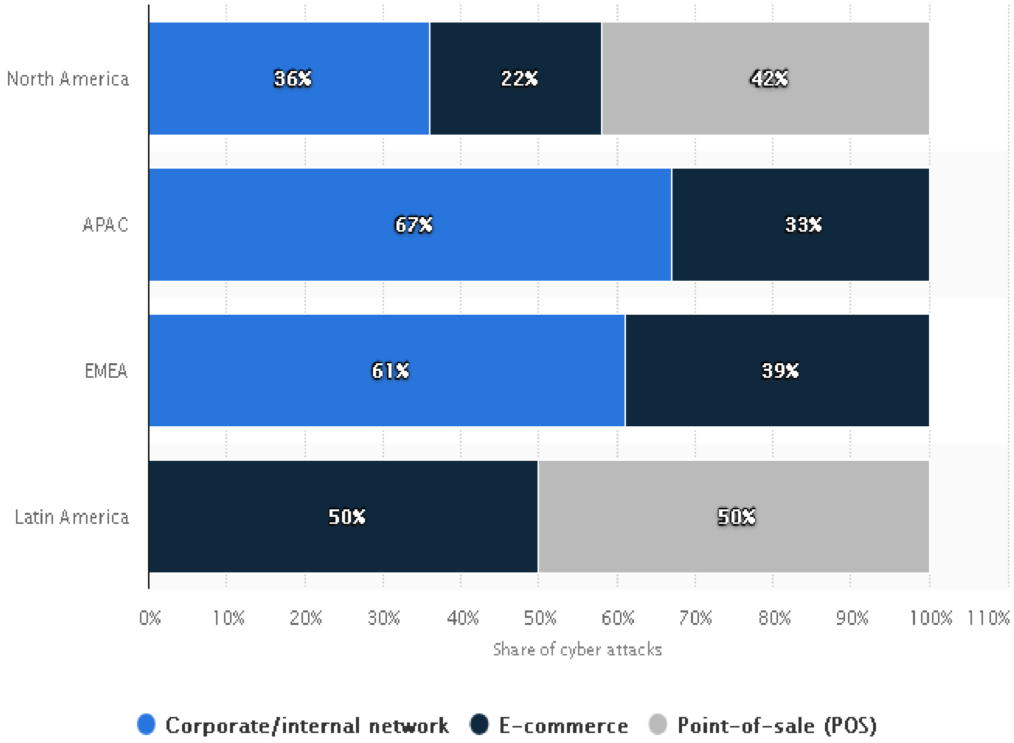


Figure 3.2: IT environments targeted by cyber-attacks worldwide in 2017, by region (Statista, 2018)

In order to examine the degree and amount of cyber attacks experienced globally in the past years, cyber attacks recorded with three years 2014 to 2017 are examined. The results from Figure 3.3 shows the IT environment targeted by cybercrime globally from the year 2014 to 2017. In the year 2014, cyber-attacks were 18% from the corporate and internal network side, 42% from the e-commerce platform and 40% from the point of sale platform. In the year 2015, cyber-attacks were 40% from the corporate and internal network side, 38% from the e-commerce platform and 22% from the point of sale platform. In the year 2016, cyber-attacks were 43% from the corporate and internal network side, 26% from the e-commerce platform and 31% from the point of sale platform. In the year 2017, cyber-attacks were 50% from the corporate and internal network side, 30% from the e-commerce platform and 20% from the point of sale platform. This implies that corporate network experienced the highest attack so far in the year 2017.

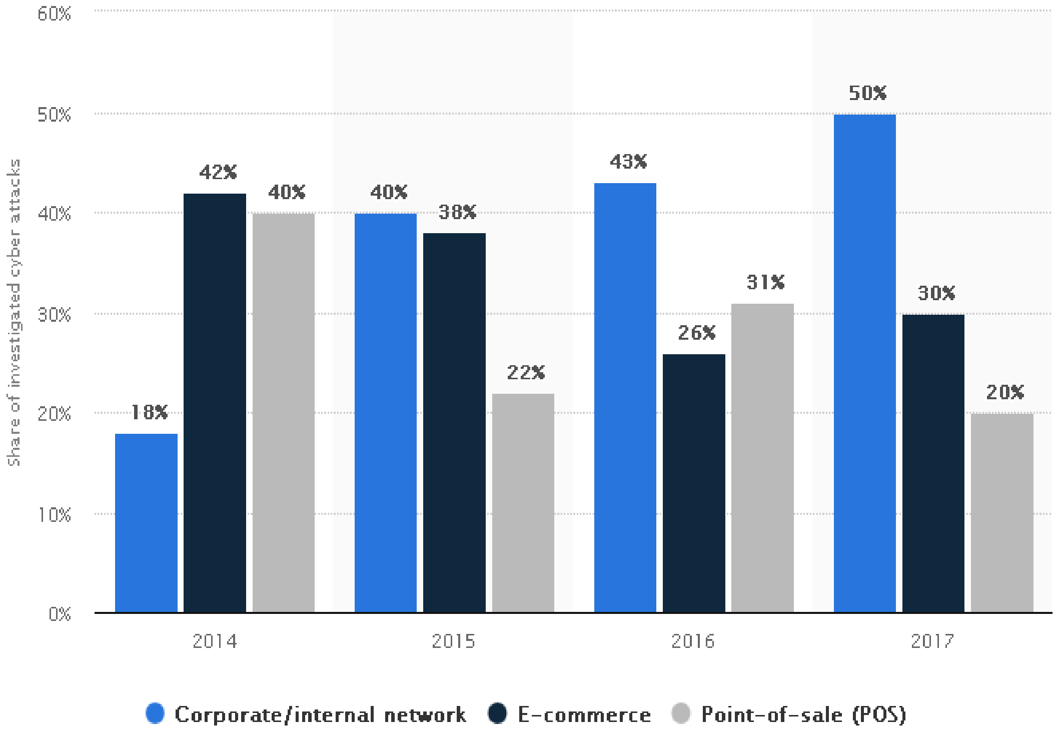


Figure 3.3: IT environments targeted by cyber-attacks worldwide from 2014 to 2017 (Statista, 2018)

3.4 Problems Associated with Cybercrime

Life is a good and bad mixture. The internet has its dark side, despite its advantages. The costs of cybercrime are not free of costs. Cybercrime shows up in a number of ways, such as death, dignity loss and job loss. Cybercrime has an impact not only on the victim but also on society. Including loss of revenues, wasted time, reputation and lower productivity have been impacted as a result of cybercrime. Some of the problems associated with cybercrime as explained by Igba et al. (2018) are reviewed below:

3.4.1 Loss of revenue

The loss of revenue is one of the major consequences of cybercrime for an economy. An external party which obtains sensitive financial information and uses it to withdraw funds of the account of such an institution can cause, for instance, loss of revenue in financial institutions or international cooperation. Cyber criminality may occur if a business' e-commerce site is compromised, and if consumers cannot use the site, valuable income is lost.

3.4.2. Damaged reputation

In cases where customer records are affected by a cybercrime-related security breach, the reputation of a company can suffer significantly. Customers who are intercepted by hackers and other infiltrators with a credit card or other financial information lose faith in such a company and often start their business elsewhere. Foreign investors often consider developing nations because of these problems.

3.4.3 Reduce productivity

Due to the action many companies have to take to prevent cybercrime, the productivity of employees is often negatively affected. This is because employees need to enter more passwords and perform other time-consuming acts to do their job because of security measures. Each second wasted task is a second not spent productive work. Cyber crime's impact on developing nation's citizenship / economics already has an adverse effect. Developing countries have been listed among the most corrupt countries in the world by the global anti-corruption body such as Transparency International. Worldwide, private companies are starting to take steps to obstruct email traffic. Financial instruments are now extremely well received by diligence worldwide and some international banks have denied their financial institution full access.

3.5 Reasons for Undergraduates Participating in Cybercrime

The founding fathers of the internet, when the Internet was developed, were not willing to misuse the internet for criminal activities. Nowadays in cyberspace, there are numerous troubling events. Scholars have nevertheless attributed the world's causes of cybercrime to the following: unemployment, the negative role model, insufficient police facilities and social gratification are causes of cybercrime. All these reasons, according to him, are used in most parts of the world to facilitate cybercrime. The major causes of cybercrime in most countries around the world are widespread corruption, harsh economic conditions, high employment, disregard for the law, lack of transparency and accountability in governance. Two primary and secondary causes could be associated with cybercrime. Poverty prevail and the weak education system are the main causes (Folashade and Abimbola, 2013).

Habitat, corruption and rapid syndrome are the secondary cause. In Nigeria for example, the high level of corruption and the spread of poverty is seen by university undergraduates as the principal cause of cybercrime. The majority of Nigeria students live below the poverty line (less than one dollar a day (#360.50)). Over five million University undergraduates in Nigeria have no hope of what they do when they are university graduates, as a means of paving the way forward, they use cybercrime (Szde, 2014).

3.6 Technology Acceptance Model (TAM)

Information system research has been highly interested in explaining people's usage technology. Different authors from groups and individual research have examined several factors that promote new technologies usage. Several models have also been introduced to explain why people use or do not use new technologies. The popular model employed to explain technology usage is TAM. David (1989) developed the TAM with the aim of explaining user's intention toward information technology use and the reason they behave in certain ways when using the technology.

Technology Acceptance Model is the bases for this study to explain the reason university students involve in cybercrime. Technology is widely used to explain technology usage behaviors from standalone computers to computers over the internet. TAM adopts the Reasoned Action theory that explains how actions are affected by human reasoning, but the TAM aimed at explaining the acceptance and usage of technology with the associated behaviors. The TAM uses the Perceived Ease-of-Use (PEU) and Perceived Usefulness (PU) of a technology to explain the behavior towards the use of the technology (Markus et al., 2015).

Perceived Ease-of-Use (PEU) is the level to which a user believes a system will be easy to use and effortless while Perceived Usefulness (PU) is the degree to which user believes using a system will be beneficial to his/her job or task (Muk and Chung, 2015). Other component of the TAM are the external factors, attitude toward using a system and behavioral intention. External factors are other factors external to the system that may influence the user's acceptance to use the system. Factors such as the social, cultural and political are external to the system but may influence the acceptance of the system (Sila, 2015).

The attitude towards using a system is the perspective and the users reaction towards using a system. The attitude can also be explained as the assessment of user's desirability to use a system (Bing and Xiaohui, 2017). Behavioral intention is the evaluation of the user's usage of the system. This examines the motive of the user to the actual use the system (Araimi et al, 2015). The effect of the PEU and PU is the Behavioral Intention that is the behavior of the user.
Figure 3.4 below shows the Technology Acceptance Model.

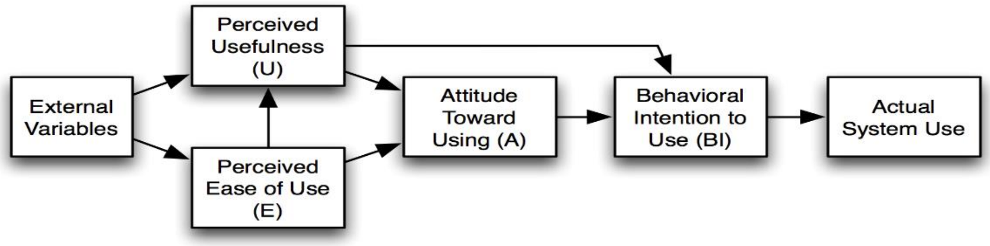

Perceived Usefulness (U)
External Variables
Attitude Toward Using (A)
Behavioral Intention to Use (BI)
Actual System Use
Perceived Ease of Use (E)

Figure 3.4: Technology acceptance model (Davis, 1989)

3.7 Extended Technology Acceptance Model

Although TAM has been developed to explain the adoption and usage of software and other technologies, different researchers have developed several extended TAM. The aim of extended TAM is developed to suit the variables understudy, which does not completely match the actual TAM. The extended TAM is the adoption of some element of the TAM and adding other variables or factors which do not surface in the actual TAM. Due to the different version of extended TAM, this study adopted an extended TAM developed by (Markus et al., 2015) in their study to measure cybercrime that is similar to the aim of this study. The extended TAM by (Markus et al., 2015) examined perceived cybercrime risk in online service avoidance. In order to align the model with this study, the perceived cybercrime risk was modified to perceived cybercrime stimulus since this study aimed at investigating the factors that promote cybercrime and not the risk. The behavior intention in the extended TAM was maintained, as it is eligible to measure the behavior intention behind cybercrime act. Precisely, the model adopted for this study is extended TAM. Figure 3.5 below depicts the perceived cybercrime risk Extended TAM by (Markus et al., 2015) which was adopted and modified for this study.

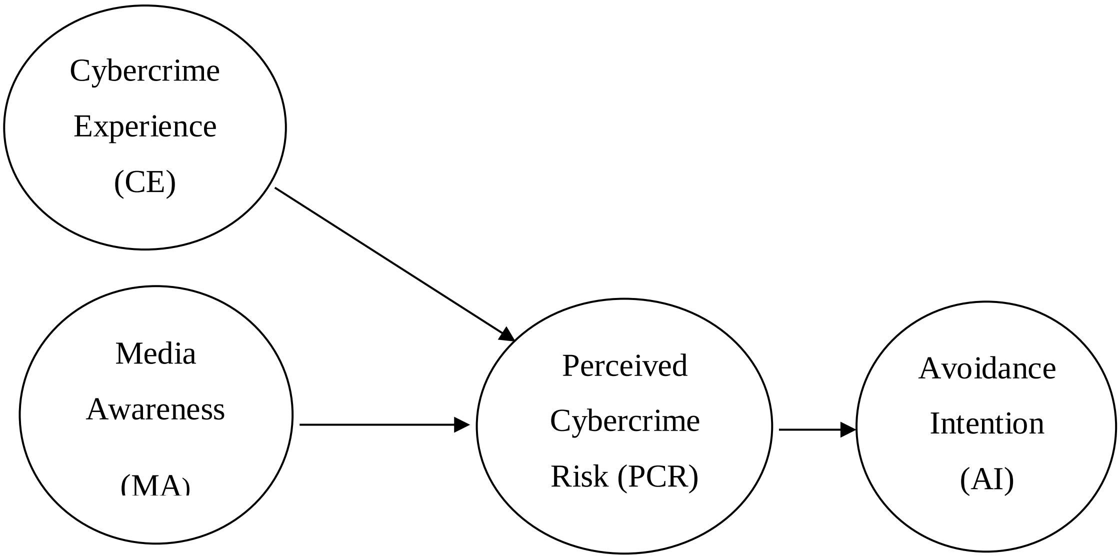


Figure 3.5: Perceived cybercrime risk extended TAM (Markus et al., 2015)

CHAPTER 4

RESEARCH METHODOLOGY

This chapter presents the methodology that was used to conduct the study. This section presents the research model that guided the study, the information of the participant surveyed for the study, the tools that were used for collecting data for the study, the data analysis method, the procedure the researcher followed in conducting the study and the scheduled for the study.

4.1 Proposed Research Model

For this purpose of this study, a model was proposed because there was no model that explains factors that promote cybercrime among university students. The TAM by Davis (1989) was extended with perceived cybercrime stimulus as a modification of the original TAM because the study tries to investigate the factors that make students involve in cybercrime which is lacking in available models. Aside behavior intention adopted from TAM (Davis, 1989), the author and the thesis supervisor created other factors. The perceived cybercrime stimulus is the cause and the behavior intention is the effect or outcome. Five external factors affect perceived cybercrime stimulus.

The Technological Support (TS) is the availability of software and tools that makes committing cybercrime easy, and deduced from previous studies such as Michel and Wannes (2011); Simplice and Christine (2018); Nora et al. (2016); Ahmed et al. (2015). Peer influence (PI) is the peer pressure from mates either in classroom or in online environment and deduced from studies such as Donna et al. (2015); Sara et al. (2016); Zhiyong et al. (2015); Enrica and Andrea (2014). The Law and Enforcement (LE) is the knowledge of any law that punishes cybercrime behavior and deduced from studies such as Nora et al. (2016); Philmore et al. (2015); Mohammad and Sharmin (2015); Simplice (2015); Byeng-Hee et al. (2017). Technology Inclination (TI) is the technology background or experience of people which is acquired through technology learned from classroom and deduced from studies such as Michel and Wannes (2011); Srinivasan et al. (2018); Xiang and Sooun (2016); Byeng-Hee et al. (2017); Nicolas et al. (2015). Economic Situation (ES) is the availability of funds to purchase product without having to steal or pirate a digital product and deduced from studies such as Nera et al. (2016); Mohammad and Sharmin (2015); Simplice et al. (2018); Nicolas et al. (2015).

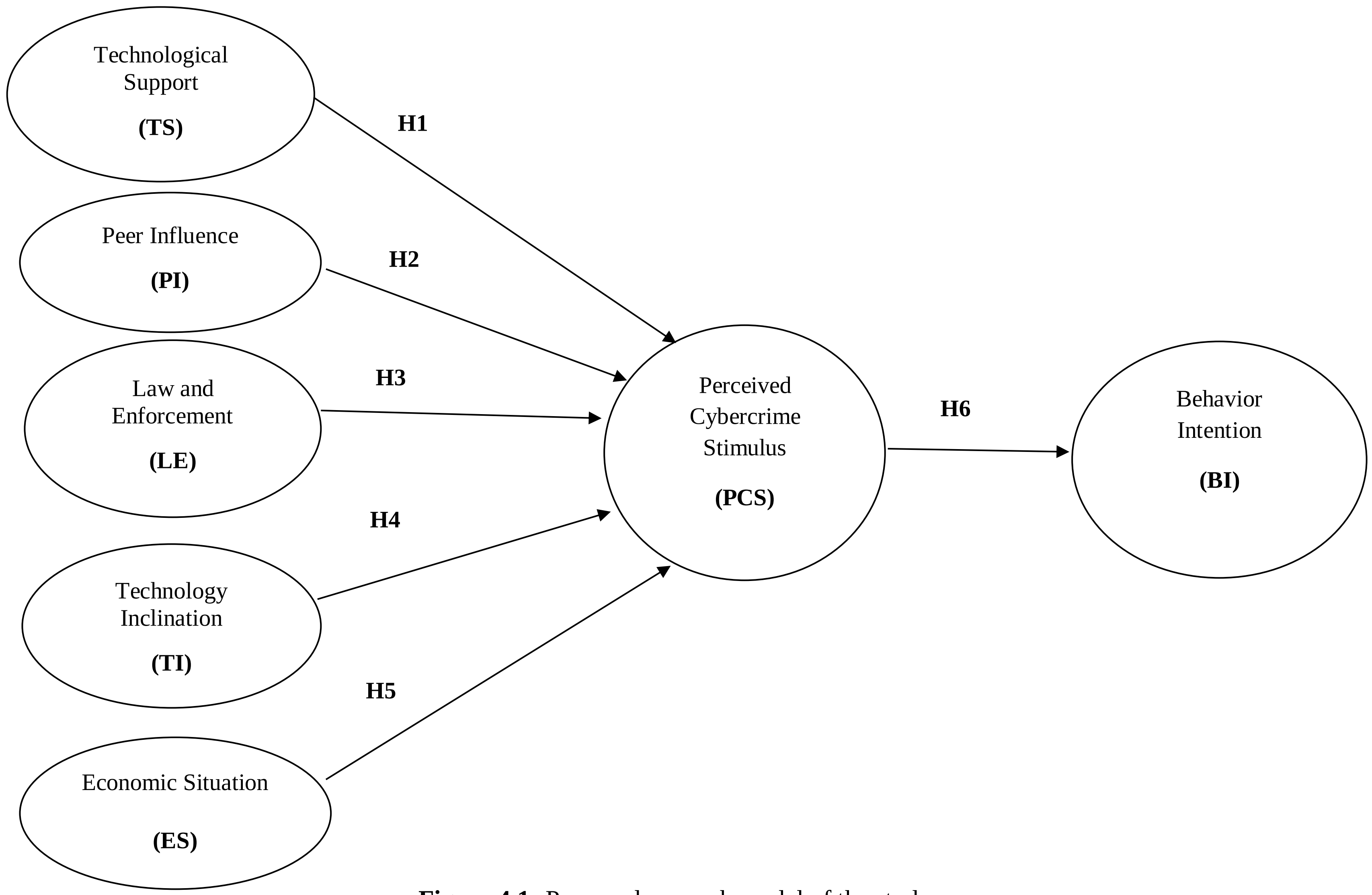


Figure 4.1: Proposed research model of the study

4.2 Research Hypothesis

In order to investigate the factors that promotes cybercrime among university students, six hypothesis were tested:

H1: *Technological support is significantly related to perceived cybercrime stimulus*

The first hypothesis is stated to ascertain if there exist any relationship between technological support and perceived cybercrime stimulus. One of the factors identified to promote cybercrime among cybercrime stimulus is the technological support. Limited studies have directly examined the relationship between technological support and perceived cybercrime stimulus among university students. A similar study conducted by Omale and Mogom (2016) examined how the introduction of fiber optic technology breeds cybercriminals in Africa. Their study revealed that the rate of cybercrime increased with the introduction of Fiber optic technology. Similarly, this hypothesis is stated to ascertain if there is any relationship between technological support and perceived cybercrime stimulus.

H2: *Peer influence is significantly related to perceived cybercrime stimulus*

The second hypothesis is stated to ascertain the relationship between peer influence and perceived cybercrime stimulus. The second factor identified to promote cybercrime among university students is peer influence. A study by Ruth et al. (2013) examined peer influence and cyberbullying among adolescents. The outcome of their study was that adolescents are influenced with cyberbullying from the classroom and through close or distant friends. The hypothesis was put forward to confirm this finding and examine the relationship between peer influence and perceived cybercrime stimulus among university students.

H3: *law and enforcement is significantly related to perceived cybercrime stimulus*

The third hypothesis is stated to examine the relationship between law and enforcement and perceived cybercrime stimulus. Law and enforcement which means the awareness of any law that punishes cybercrime behavior serves as a factor that promotes cybercrime among university students. A study conducted by Hannah et al. (2016) examined the impact of law on reducing cyberbullying behavior among middle school students in Australia. They found that the lack of awareness of cyberbullying laws promotes cyberbullying behavior among students. In line with this, this hypothesis aimed at testing the relationship between law and enforcement and cybercrime behavior among university students.

H4: *Technology inclination is significantly related to perceived cybercrime stimulus*

Another factor identified to promote cybercrime among university students is their inclination towards the use of technology. This hypothesis is stated to examine the relationship between technological inclination of student and cybercrime stimulus. A study by Omale and Mogom (2016) revealed that availability and technology experience of students increases cybercrime behavior. In line with this, this hypothesis is put forward to confirm the assertion by the authors and examine the relationship between technological inclination and perceived cybercrime stimulus.

H5: *Economic situation is significantly related to cybercrime stimulus*

Economic situation is another factor identified to promote cybercrime among university students. The aim of this hypothesis is to examine the relationship between economic situation and perceived cybercrime stimulus. A study by Asongu (2014) examined poverty in relation to software piracy in Africa. He found that software piracy is prevalent high poverty rate countries because of lack of funds to purchase licensed software. In line with this finding, this hypothesis is stated to test the connection between economic situation and perceived cybercrime stimulus.

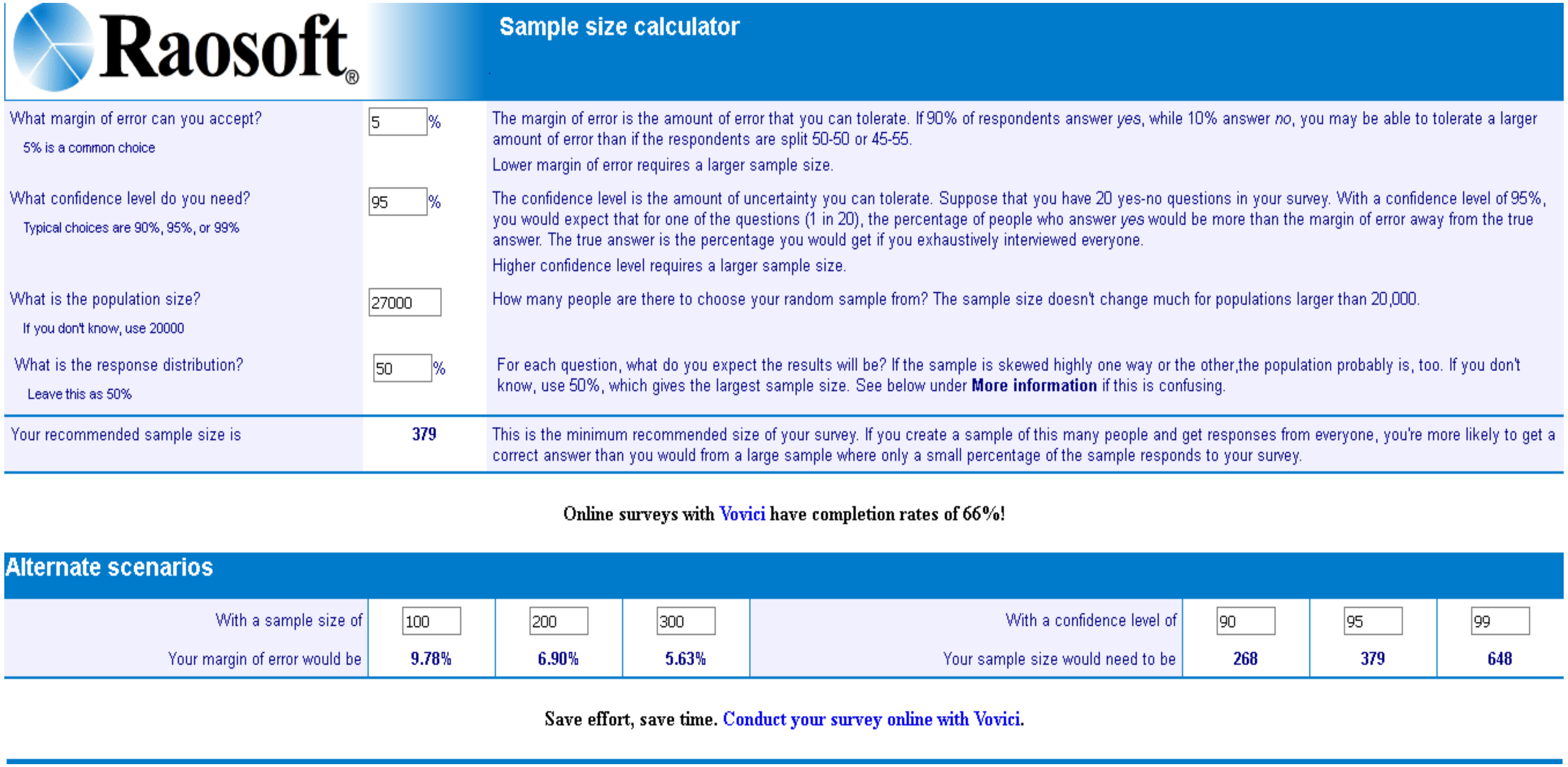
H6: *Perceived cybercrime stimulus is significantly related to behavioral Intention*

The final hypothesis is stated to examine the relationship between perceived cybercrime and behavior intention. The aim of this hypothesis is to ascertain how perceived cybercrime stimulus influence cybercrime behavior among students.

4.3 Research Participants

The researcher surveyed students from Near East University in North Cyprus only. The students were drawn from Near East University in both the graduate and undergraduate level from different departments. Students were chosen from different department to have representative data of the entire students. In order to examine the factors that influence cybercrime among university students, 380 students were randomly sampled for the study.

The researcher arrived at the sample size of 380 using Raosoft sample size calculator, Figure 4.2 depicts the Raosoft calculator output. In order to collect data needed for the study, the students were approached on the campus and aim of the study was briefed to them, the students were then given the questionnaire to answer to the best of their knowledge. Not all the students agreed to participate in the study, the ones that did not agree to participate in the study were not forced to participate in the study. Out of the 400 questionnaires distributed, 380 were retrieved which amount to 95% response rate. The 380 questionnaires retrieved has been used for analysis in this study.



Raosoft®

Sample size calculator

What margin of error can you accept? 5% is a common choice	5 %	The margin of error is the amount of error that you can tolerate. If 90% of respondents answer *yes*, while 10% answer *no*, you may be able to tolerate a larger amount of error than if the respondents are split 50-50 or 45-55. Lower margin of error requires a larger sample size.
What confidence level do you need? Typical choices are 90%, 95%, or 99%	95 %	The confidence level is the amount of uncertainty you can tolerate. Suppose that you have 20 yes-no questions in your survey. With a confidence level of 95%, you would expect that for one of the questions (1 in 20), the percentage of people who answer *yes* would be more than the margin of error away from the true answer. The true answer is the percentage you would get if you exhaustively interviewed everyone. Higher confidence level requires a larger sample size.
What is the population size? If you don't know, use 20000	27000	How many people are there to choose your random sample from? The sample size doesn't change much for populations larger than 20,000.
What is the response distribution? Leave this as 50%	50 %	For each question, what do you expect the results will be? If the sample is skewed highly one way or the other,the population probably is, too. If you don't know, use 50%, which gives the largest sample size. See below under **More information** if this is confusing.
Your recommended sample size is	**379**	This is the minimum recommended size of your survey. If you create a sample of this many people and get responses from everyone, you're more likely to get a correct answer than you would from a large sample where only a small percentage of the sample responds to your survey.

Online surveys with Vovici have completion rates of 66%!

Alternate scenarios

With a sample size of	100	200	300	With a confidence level of	90	95	99
Your margin of error would be	**9.78%**	**6.90%**	**5.63%**	Your sample size would need to be	**268**	**379**	**648**

Save effort, save time. Conduct your survey online with Vovici.

Figure 4.2: Sample size calculation (Retrieved 15 April 2019 from http://www.raosoft.com/samplesize.html)

4.3.1 Demographic data of research participants

Result from Table 4.1 shows the gender distribution of students surveyed at Near East University. 42.1% of the students are female while 57.9% are male. On the nationality distribution of the respondents, 74 students representing 19.5% are from Middle East, 200 students representing 52.6% are from Africa, 20 students representing 5.3% are from Europe while 86 students representing 22.6% are from Asia. on the age distribution of students, 7.4% are 18 years of age, 6.3% are 19 years of age,10.5% are 20 years of age,13.2% are 21 years of age, 14.5% are 22 years of age 15.5% are 23 years of age, 15.5% are 24 years of age while 17.1% are 25 years and above. On the departments of the students surveyed, 31.6% are from the computer engineering department, 26.3% are from IT and IS department while 42.1% are from other departments of the university. This result shows the distribution of demography of the students. This is important to ensure the researcher targets the right respondents.

Table 4.1: Demographic details of research participants

Demographic Variables		Number	Percentage (%)
Gender	Female	160	42.1
	Male	220	57.9
Nationality	Middle East	74	19.5
	Africa	200	52.6
	Europe	20	5.3
	Asia	86	22.6
Age	18	28	7.4
	19	24	6.3
	20	40	10.5
	21	50	13.2
	22	55	14.5
	23	59	15.5
	24	59	15.5
	25+	65	17.1

Table 4.1 Continued…

Demographic Variables		Number	Percentage (%)
Department	Computer Engineering	120	31.6
	IT and IS	100	26.3
	Others	160	42.1
Year	1	46	12.1
	2	67	17.6
	3	82	21.6
	4	84	22.1
	Masters	101	26.6

4.4 Data Collection Tools

Considering the research topic and the research setting to the study, the researcher settled on the use of questionnaire for data collection. The questionnaire was designed by the assistance of the thesis supervisor and it followed a five likert scale pattern with responses ranging from *strongly agree (5 point), agree (4 point), undecided (3 point), disagree (2 point) and strongly disagree (1 point)*. The items on the questionnaire comprises of two dimensions with items under each dimension.

Section I: Personal Information: During data collection, the student's personal information were collected. Personal information of the students collected were gender, nationality, age, department and year, making it five items under this section. This data was collected to ensure the study collects data from the intended demographic population.

Section II: Factors that Promotes Cybercrime: The aim of this section was to understand the factors that promotes cybercrime among university students. This section encompasses the different factors that promotes cybercrime among students. The section has 7 sub-categories with 30 five likert items in total with responses from *strongly agree, agree, undecided, disagree and strongly disagree*.

Dimension 1: Technological support: The first dimension of the questionnaire is technological support with the aim of examining how technological support affect cybercrime behavior. Technological support is the availability of technology such as software that makes carrying out cybercrime easy. This dimension is important to examine one of the technological support factor that promotes cybercrime. In order to measure technological support, this dimension is important.

Dimension 2: Peer influence: The second dimension of the questionnaire is peer influence as one of the factors that promotes cybercrime among university students. Peer influence is the peer pressure that arise from wanting to do what other fellow students and friends do. It is necessary to measure peer influence as it a factor which is believed to promote cybercrime among university students. This dimension ask questions that bring to light the view of the students whether they would like to involve in cybercrime if their friends or class mates also involve in it.

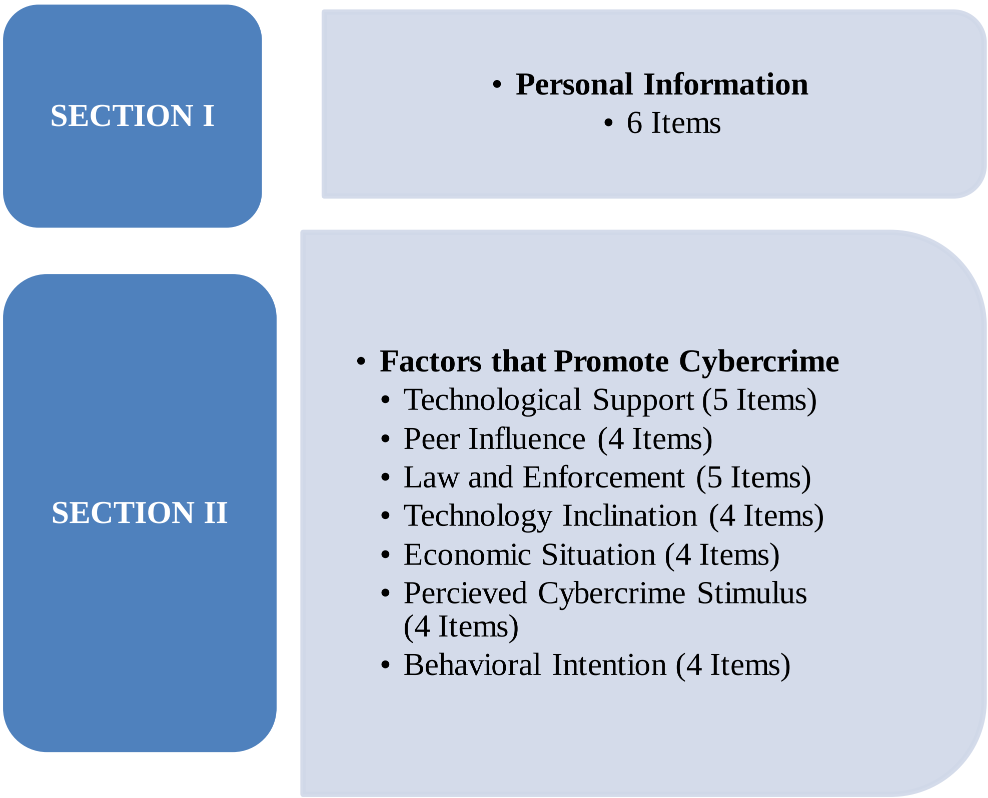
Dimension 3: Law and enforcement: The third dimension of the questionnaire is on law and enforcement. Law and enforcement as related to this study is one of the factors that promotes cybercrime. Law and enforcement is the lack of awareness of any law that punishes cybercrime behavior. This dimension ask questions as to whether the lack of knowledge about any law that punish cybercrime behavior makes students want to involve in cybercrime. This dimension is important to this study as it measures the law and enforcement factor believed to promote cybercrime.

Dimension 4: Technology inclination: The fourth dimension of the questionnaire is on technological inclination as a factor that promote cybercrime. This dimension asked questions on how technology inclination of the students influence cybercrime behavior. Technological inclination is the technology experience of the student gotten from either classroom or personal learning. This dimension is necessary to examine whether having prior knowledge about technology influence students to perpetrate cybercrime behavior.

Dimension 5: Economic situation: The fifth dimension of the questionnaire is about economic situation and how it influence cybercrime behavior among students. Economic situation is the financial status of the students and how it influence them to involve in cybercrime for financial gains. This dimension is important to this study as it measures economic situation, which is one of the factors believed to promote cybercrime among university students.

Dimension 6: Perceived cybercrime stimulus: The sixth dimension is about perceived cybercrime stimulus and how it relates to cybercrime behavior intention. Perceived cybercrime stimulus is the believed motivation behind cybercrime behavior. Perceived cybercrime stimulus is the drive to commit cybercrime. The aim of this dimension is to examine the motivations behind cybercrime behavior. The perceived cybercrime stimulus dwells on the external factors earlier identifies such as technological support, peer influence, law and enforcement, technology inclination and economic situation. All these factors are believed to influence the stimulus to commit cybercrime.

Dimension 7: Behavior intention: The last dimension is about behavior intention to commit cybercrime. Behavior intention is the aim or urge to commit cybercrime. This dimension measures the final stage of committing cybercrime act. This dimension is important to this study as it measures the actual cybercrime act that serves as the major aim of this study. The questionnaire is attached to the appendix section of this study. Figure 4.3 below describe the dimensions in the questionnaire.



SECTION I

- **Personal Information**
  - 6 Items

SECTION II

- **Factors that Promote Cybercrime**
  - Technological Support (5 Items)
  - Peer Influence (4 Items)
  - Law and Enforcement (5 Items)
  - Technology Inclination (4 Items)
  - Economic Situation (4 Items)
  - Percieved Cybercrime Stimulus (4 Items)
  - Behavioral Intention (4 Items)

Figure 4.3: Structure of questionnaire

4.4.1 Reliability

In other to access the reliability of the research instrument that is the questionnaire, Cronbach alpha was calculated for all the items to ascertain how relevant and reliable they are to the research topic. In the opinion of Hair et al. (1998), according to George and Malley (2003), the level of the reliability must not be lower than .70, reliability score lesser than .50 are unacceptable and a poor reliability at the level between .50 and .60. They furthered that the acceptable reliability level is between .70 and .80 while having higher than .80 shows the items meet satisfactory level and consistent. In the event the acceptable level of reliability is not met, the items must be adjusted.

Table 4.2: Questionnaire construct and reliability test results

Construct	Number of items	Cronbach Alpha
Technological Support	5	.971
Peer Influence	4	.977
Law and Enforcement	5	.970
Technology Inclination	4	.969
Economic Situation	4	.963
Perceived Cybercrime Stimulus	4	.972
Behavioral Intention	4	.963
Total	30	.995

4.5 Data Analysis Methods

The data collected using questionnaire were analyses using

- Descriptive statistics for the personal data of the students
- Pearson correlation to determine the relationship between the variables (independent and dependent)
- Items on the questionnaire were coded according to tone of the questions; negatively worded questions were codded in reverse order

4.6 Research Procedure

The researcher followed the following steps in conducting this study:

i. Past literature on the research area were reviewed extensively to draw knowledge needed to write this thesis.

ii. A research proposal summarizing the thesis was prepared by the researcher and submitted to the department of Computer Information Systems.

iii. The supervisor responded constantly with feedbacks on suggestions to enhance the quality of the proposal.

iv. Draft version of the questionnaire was developed with the help of the thesis supervisor.

v. Three IT and IS experts from the computer information systems department and assessment and evaluation experts from the education faculty evaluated the questionnaire.

vi. The ethical committee reviewed application that comprises of the questionnaire developed and ethical forms.

vii. Upon approval by the ethical committee, the questionnaire was distributed physically to the students both undergraduate and graduate at the university campus.

viii. After the data collection was completed, the data collected entered into the SPSS for analysis.

ix. Data was analyzed using the appropriate data analysis method followed by presentation of results.

x. At each stage of the study, the supervisor was well informed and involved by giving feedback and needed suggestions that helped the completion of this thesis.

xi. The final version of the thesis was presented to the jury for defense and the thesis was amended based on the feedbacks and corrections made by the jury, after which the final thesis was approved.

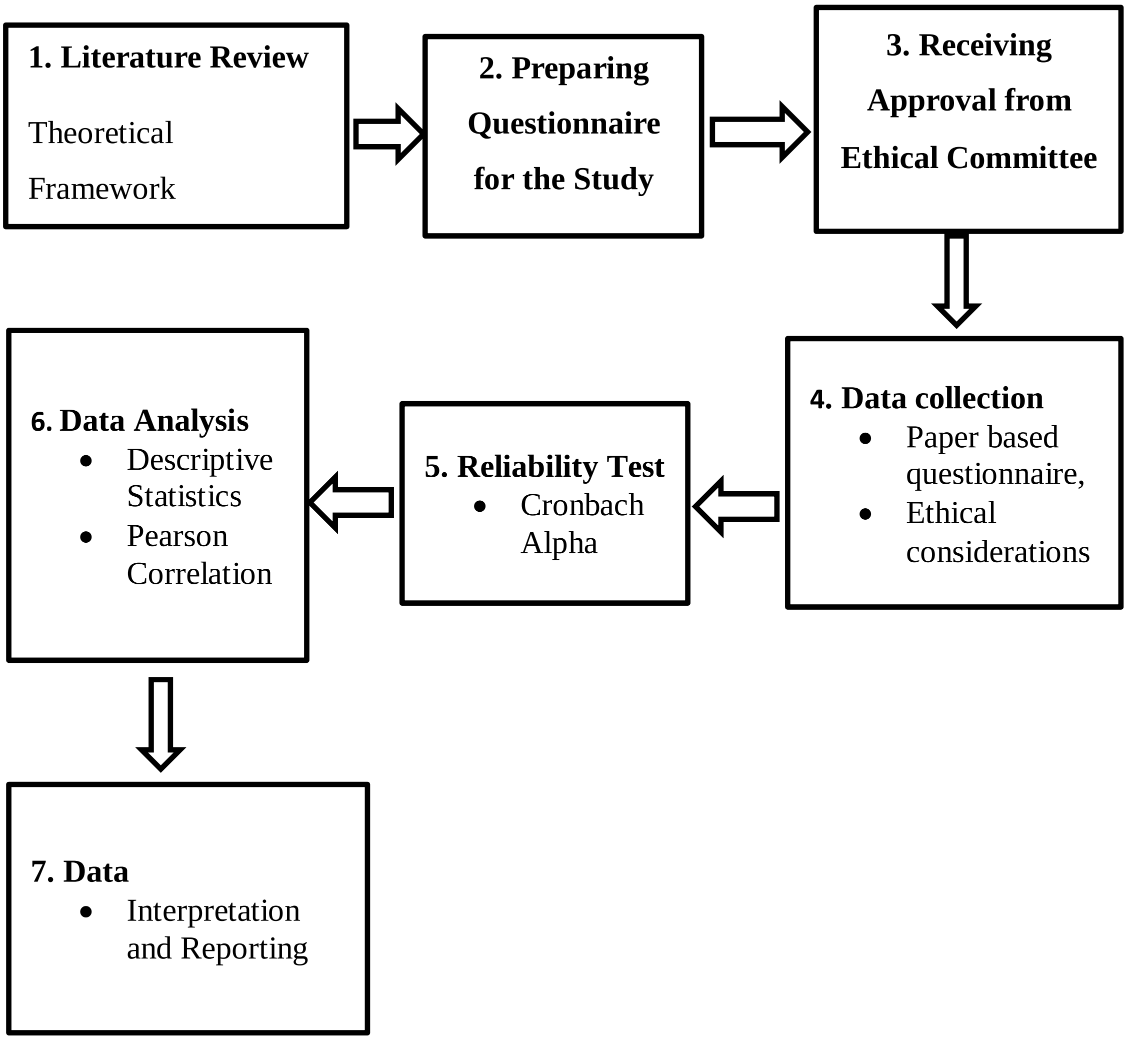


Figure 4.4: Research procedure

4.6.1 Ethical consideration

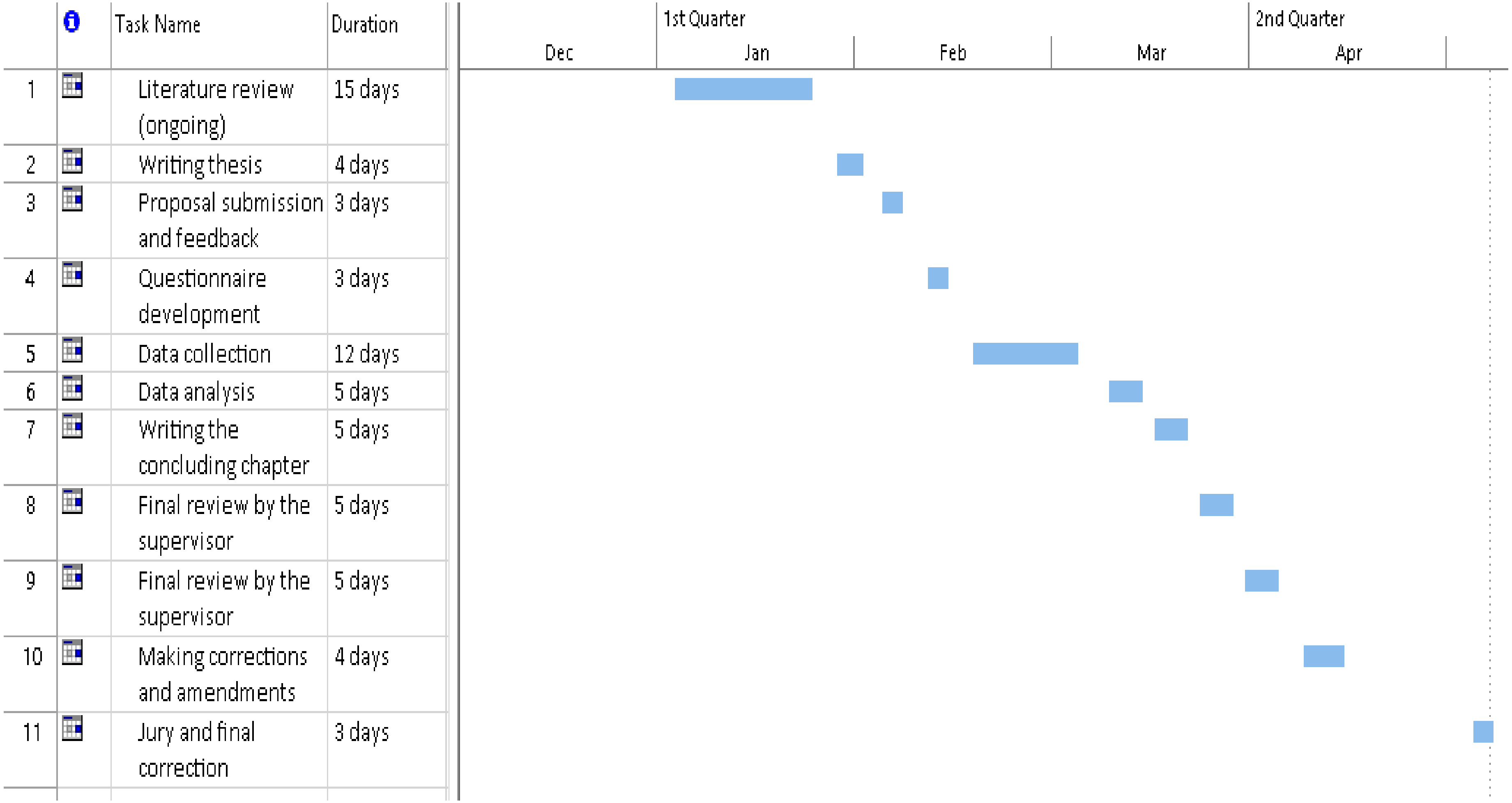
In order to conduct a safe, free and unbiased study, it is paramount to take ethical considerations as mandated in social science research. In conducting this study, ethical considerations were not left out. First, the researcher ensured the ethics committee Near East University governing every research in the school evaluates and approved the ethical forms used for the study that is attached in Appendix 1. Second, the researcher ensured the participants were briefed about the study and their consent was taken before they were allowed to participate in the study. Students surveyed were informed about the aim of the study and what the data collected will be used for. This allows the researcher prevent any form of deception in the data collection. Third, the researcher ensured all students participating in the study do so as anonymous that is, their names or any traceable information were not collected. Lastly, the study ensured no participant was forced or induced in any form to participate in the study.

4.7 Research Schedule

Every study follows a research plan or schedule for effective time and resource management. The thesis commenced early November 2018 and finished in May 2019. Each stage of the thesis was assigned a time of completion to enable smooth planning for the thesis. Some stages of the thesis have to run after the previous stages are completed while some runs concurrent with an ongoing stage. The literature review stage as an ongoing stage runs concurrent with other stages of the thesis without any problem or challenges. The schedule of the thesis is presented in the Table 4.4 below:

Table 4.3: Research schedule

Schedule	**Duration (Weeks)**
Literature review (ongoing)	15
Writing thesis proposal	4
Proposal submission and feedback	3
Questionnaire development	3
Data collection	12
Data analysis	5
Writing the concluding chapter of the thesis	5
Final review by the supervisor	5
Making corrections and amendments	4
Jury and final correction	3
Total	59 Weeks



	Task Name	Duration
1	Literature review (ongoing)	15 days
2	Writing thesis	4 days
3	Proposal submission and feedback	3 days
4	Questionnaire development	3 days
5	Data collection	12 days
6	Data analysis	5 days
7	Writing the concluding chapter	5 days
8	Final review by the supervisor	5 days
9	Final review by the supervisor	5 days
10	Making corrections and amendments	4 days
11	Jury and final correction	3 days

Figure 4.5: Gantt chart of the study

CHAPTER 5

RESULTS AND DISCUSSIONS

This section presents the result of the data analyzed from this study. Furthermore, the results from this study are also compared with the existing literature on the research topic in order to ascertain the similarities and differences to the previously known knowledge about the research area.

5.1 Relationship Amongst Technological Support and Perceived Cybercrime Stimulus

H1: Technological support is significantly related to perceived cybercrime stimulus.

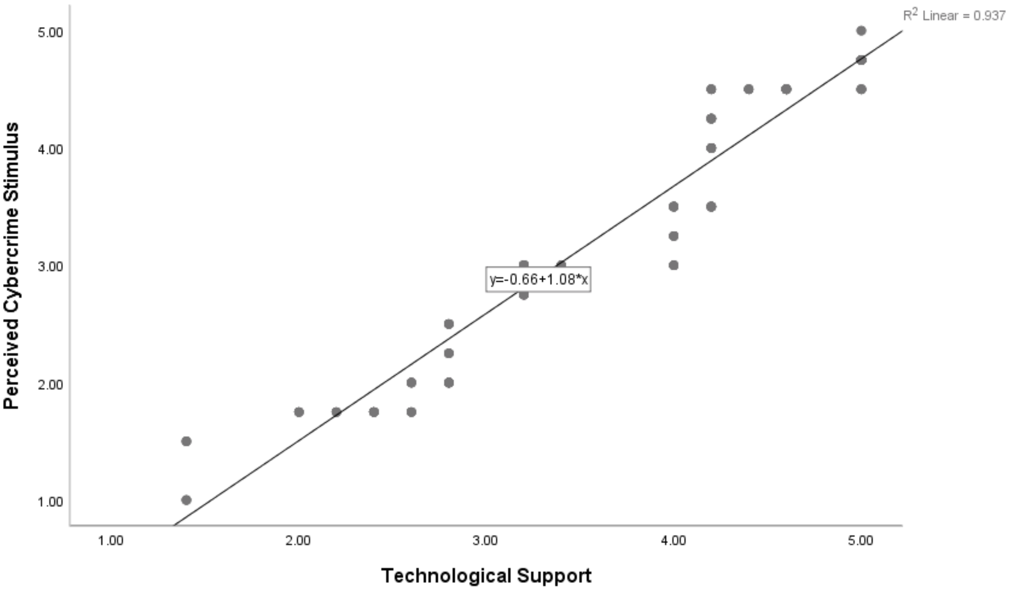
In order to examine the relationship between technological support and perceived cybercrime stimulus, Pearson correlation between the two variables (technological support and perceived cybercrime stimulus) was conducted. The result from Table 5.1 depicts that there exist a strong positive correlation between technological support and perceived cybercrime stimulus with r=.968, n= 380 and p =.000. Since there exist a positive correlation between technological support and perceived cybercrime stimulus at .968 and p<= .01, we therefore accept the hypothesis that technological support is significantly related to perceived cybercrime stimulus among students. In addition, the results from Figure 5.1 depicts the scatter plot graph of positive relationship between the technological support and perceived cybercrime stimulus. The scatter plot shows that as technological support increases, so as the stimulus to commit cybercrime increases at ($r^2 = 0.937$) which shows a strong positive linear relationship between technology support and perceived cybercrime stimulus.

The results implies that technological support in terms of availability of tools, software and website provides the platform to easily perpetrate cybercrime acts. This is evident from the studies of Diana and Sheri (2015) which says that internet tools such as social media and software serves as a platform for youths to engage in cybercrime and they can also be a victim through the platform.

Table 5.1: Pearson Correlation between Technological Support and Perceived stimulus

		Technological Support	Perceived Cybercrime Stimulus
Technological Support	Pearson Correlation	1	.968**
	Sig. (2-tailed)		.000
	N	380	380
Perceived Cybercrime Stimulus	Pearson Correlation	.968**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.1: Scatter plot of technological support and perceived cybercrime stimulus

5.2 Relationship Amongst Peer influence and Perceived Cybercrime Stimulus

H2: Peer influence is significantly related to perceived cybercrime stimulus

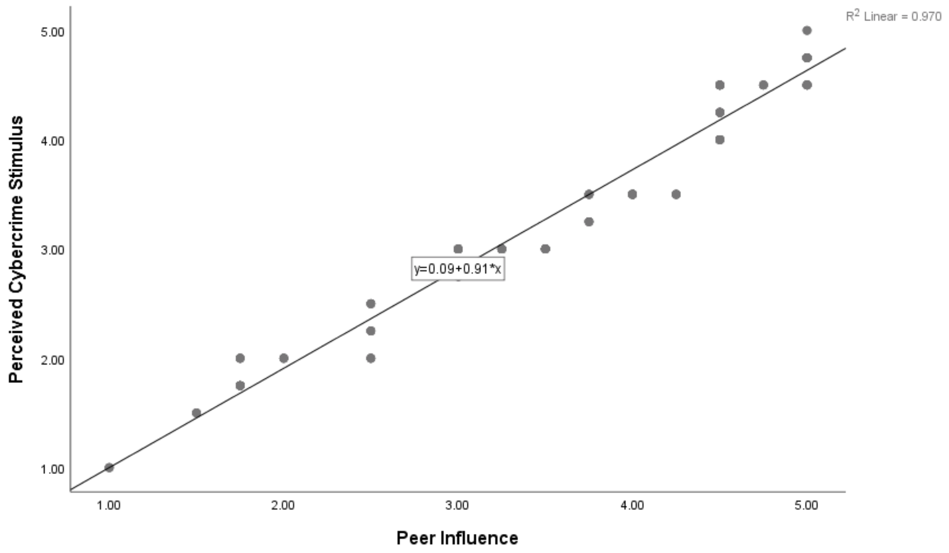
In order to examine the relationship between peer influence and perceived cybercrime stimulus, Pearson correlation between the two variables (peer influence and perceived cybercrime stimulus) was conducted. The result from Table 5.2 depicts that there exist a strong positive correlation between peer influence and perceived cybercrime stimulus with r=.985, n= 380 and p =.000. Since there exist a positive correlation between peer influence and perceived cybercrime stimulus at .985 and p<= .01, we therefore accept the hypothesis that peer influence is significantly related to perceived cybercrime stimulus among students. In addition, the results from Figure 5.2 depicts the scatter plot graph of positive relationship between peer influence and perceived cybercrime stimulus. The scatter plot shows that as peer influence increases, so as the stimulus to commit cybercrime increases at (r^2 = 0.970) which shows a strong positive linear relationship between peer influence and perceived cybercrime stimulus.

The results implies that peer influence contributes to some extent the intention to commit cybercrime. This is evident from the study by Catherine et al. (2014) which says that teenagers tend to learn cyberbullying from the classroom and practice what their mates does.

Table 5.2: Pearson correlation between peer influence and perceived cybercrime stimulus

		Peer Influence	**Perceived Cybercrime Stimulus**
Peer Influence	Pearson Correlation	1	.985**
	Sig. (2-tailed)		.000
	N	380	380
Perceived Cybercrime Stimulus	Pearson Correlation	.985**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.2: Scatter plot of peer influence and perceived cybercrime stimulus

5.3 Relationship Amongst Law and Enforcement and Perceived Cybercrime Stimulus

H3: law and enforcement is significantly related to cybercrime stimulus

In order to examine the relationship between law and enforcement and perceived cybercrime stimulus, Pearson correlation between the two variables (law and enforcement and perceived cybercrime stimulus) was conducted. The result from Table 5.3 depicts that there exist a weak positive correlation between law and enforcement and perceived cybercrime stimulus with r=.988, n= 380 and p =.000. Since there exist a positive correlation between law and enforcement and perceived cybercrime stimulus at .988 and p<= .01, we therefore accept the hypothesis that law and enforcement of cybercrime is significantly related to perceived cybercrime stimulus among students. In addition, the results from Figure 5.3 depicts the scatter plot graph of positive relationship between law and enforcement and perceived cybercrime stimulus. The scatter plot shows that as law and enforcement increases, so as the stimulus to commit cybercrime increases at (r^2 = 0.976) which shows a strong positive linear relationship between law and enforcement and perceived cybercrime stimulus.

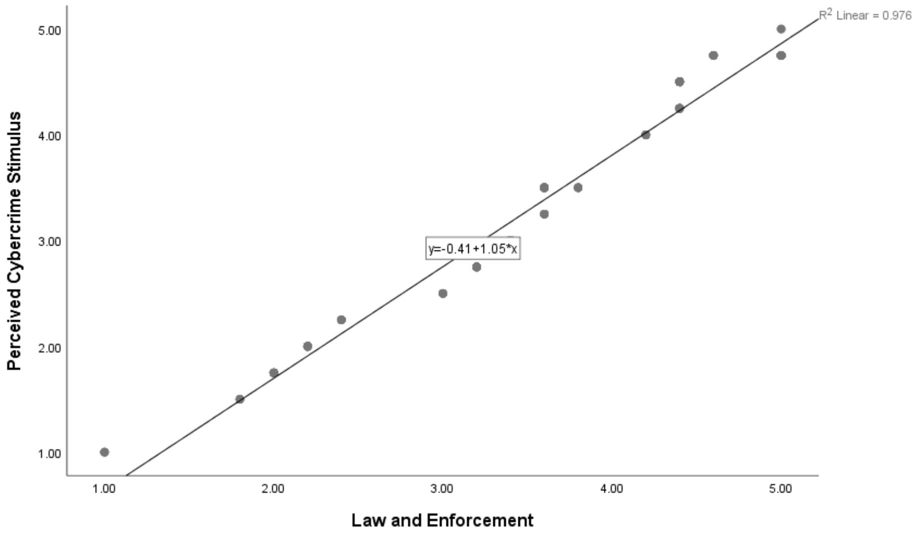
The results implies that the lack of knowledge about any cybercrime law and enforcement contributes to cybercrime act among the youths. This result is consistent with study from

Matti et al. (2015) which revealed that many youth are unaware of any law and the punishment from committing cybercrime. As a result of this, the youth continues to perpetrate the act because they believe there is no law to punish their behavior.

Table 5.3: Pearson correlation of law and enforcement and perceived cybercrime stimulus

		Law and Enforcement	**Perceived Cybercrime Stimulus**
Law and Enforcement	Pearson Correlation	1	.988**
	Sig. (2-tailed)		.000
	N	380	380
Perceived Cybercrime Stimulus	Pearson Correlation	.988**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.3: Scatter plot of law and enforcement and perceived cybercrime stimulus

5.4 Relationship Amongst Technology Inclination and Perceived Cybercrime Stimulus

H4: Technology inclination is significantly related to perceived cybercrime stimulus

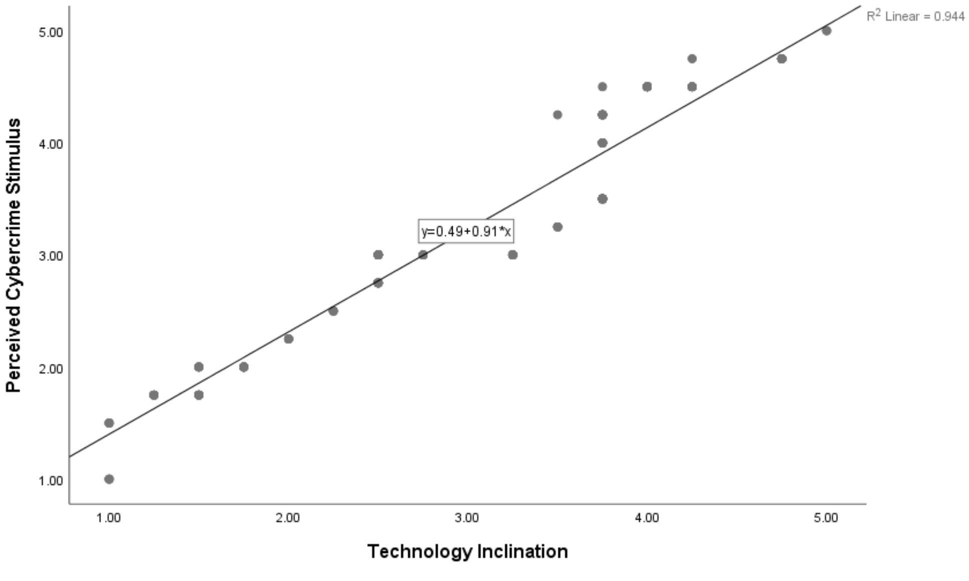
In order to examine the relationship between technology inclination and perceived cybercrime stimulus, Pearson correlation between the two variables (Technology inclination and perceived cybercrime stimulus) was conducted. The result from Table 5.4 depicts that there exist a positive correlation between technology inclination and perceived cybercrime stimulus with r=.972, n= 380 and p =.000. Since there exist a positive correlation between technology inclination and perceived cybercrime stimulus at .972 and p<= .01, we therefore accept the hypothesis that technology inclination is significantly related to perceived cybercrime stimulus among students. In addition, the results from Figure 5.4 depicts the scatter plot graph of positive relationship between technology inclination and perceived cybercrime stimulus. The scatter plot shows that as technology inclination increases, so as the stimulus to commit cybercrime increases at (r^2 = 0.944) which shows a strong positive linear relationship between technology inclination and perceived cybercrime stimulus.

The results implies that students familiar with technology from classroom finds it handy to download pirated products and make use of cracked software amongst other minor cybercrime act. This result is evident from the studies by Katherine et al. (2019) which revealed that having prior knowledge about computer makes it easier to manipulate computer related contents.

Table 5.4: Pearson correlation of technology inclination and perceived cybercrime stimulus

		Technology Inclination	**Perceived Cybercrime Stimulus**
Technology Inclination	Pearson Correlation	1	.972**
	Sig. (2-tailed)		.000
	N	380	380
Perceived Cybercrime Stimulus	Pearson Correlation	.972**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.4: Scatter plot of technology inclination and perceived cybercrime stimulus

5.5 Relationship Amongst Economic situation and Perceived Cybercrime Stimulus

H5: Economic situation is significantly related to perceived cybercrime stimulus

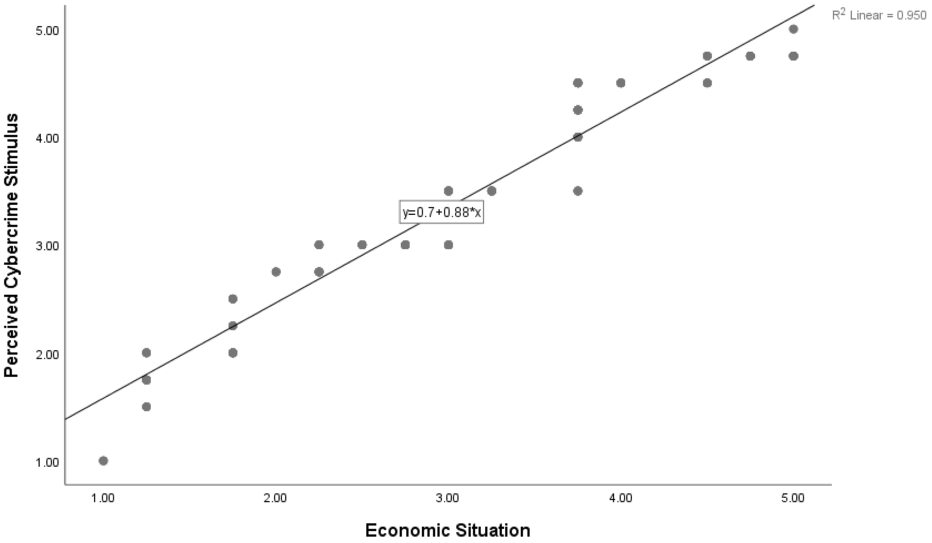
In order to examine the relationship between Economic situation and perceived cybercrime stimulus, Pearson correlation between the two variables (Economic situation and perceived cybercrime stimulus) was conducted. The result from Table 5.5 depicts that there exist a positive correlation between Economic situation and perceived cybercrime stimulus with r=.974, n= 380 and p =.000. Since there exist a positive correlation between economic situation and perceived cybercrime stimulus at .974 and p<= .01, we therefore accept the hypothesis that economic situation is significantly related to perceived cybercrime stimulus among students. In addition, the results from Figure 5.5 depicts the scatter plot graph of positive relationship between Economic situation and perceived cybercrime stimulus. The scatter plot shows that as economic situation increases, so as the stimulus to commit cybercrime increases at (r^2 = 0.950) which shows a strong positive linear relationship between economic situation and perceived cybercrime stimulus.

The results implies that economic situation such as the lack of money to purchase licensed software encourages the cybercrime act of cracking licensed software for free. This study is evident from the studies of Folashade and Abimbola (2013) which revealed that poverty and lack of finance contributes to the rate of cybercrime act among the youths in developing countries.

Table 5.5: Pearson correlation of economic situation and perceived cybercrime stimulus

		Economic Situation	**Perceived Cybercrime Stimulus**
Economic Situation	Pearson Correlation	1	.974**
	Sig. (2-tailed)		.000
	N	380	380
Perceived Cybercrime Stimulus	Pearson Correlation	.974**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.5: Scatter plot of economic situation and perceived cybercrime stimulus

5.6 Relationship Amongst Perceived Cybercrime Stimulus and Behavioral Intention

H6: Perceived cybercrime stimulus is significantly related to behavioral Intention

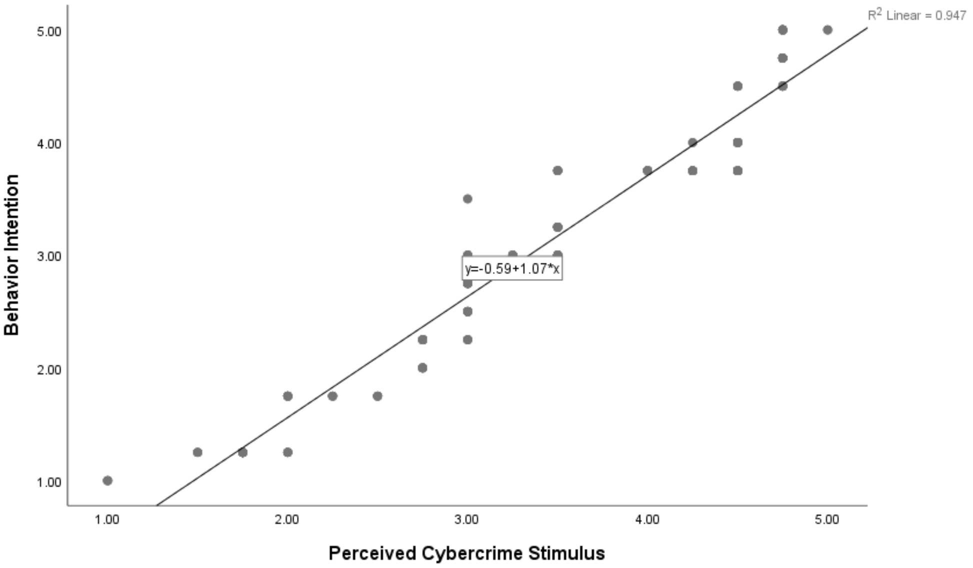
In order to examine the relationship between Perceived cybercrime stimulus and behavioral intention, Pearson correlation between the two variables (Perceived cybercrime stimulus and behavioral intention) was conducted. The result from Table 5.6 depicts that there exist a strong positive correlation between Perceived cybercrime stimulus and behavioral intention with r=.973, n= 380 and p =.000. Since there exist a positive correlation between Perceived cybercrime stimulus and behavioral intention at .973 and p<= .01, we therefore accept the hypothesis that perceived cybercrime stimulus is significantly related to behavioral Intention. In addition, the results from Figure 5.6 depicts the scatter plot graph of positive relationship between perceived cybercrime stimulus and behavioral Intention. The scatter plot shows that as perceived cybercrime stimulus increases, so as the behavior intention to commit cybercrime increases at (r^2 = 0.947) which shows a strong positive linear relationship between perceived cybercrime stimulus and behavior intention.

The results implies that the stimulus to involve in cybercrime act has a significant effect on the intention to commit cybercrime. The different factors such as the technological support, peer influence, law and enforcement, technology support, economic situation joined together formed the stimulus behind the intention to commit cybercrime.

Table 5.6: Pearson correlation of perceived cybercrime stimulus and Behavior Intention

		Perceived Cybercrime Stimulus	**Behavior Intention**
Perceived Cybercrime Stimulus	Pearson Correlation	1	.973**
	Sig. (2-tailed)		.000
	N	380	380
Behavior Intention	Pearson Correlation	.973**	1
	Sig. (2-tailed)	.000	
	N	380	380

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



1.00: Strongly Disagree; **2.00**: Disagree; **3.00:** Undecided; **4.00:** Agree; **5.00:** Strongly Agree

Figure 5.6: Scatter plot of perceived cybercrime stimulus and behavior intention

5.7 Summary of Findings

This study aimed at investigating the factors that promotes cybercrime among university students of Near East University, North Cyprus. In order to achieve the objectives set for the study, six hypotheses were tested and the summary of the results are presented in Table 5.7 below.

Five factors were tested as some of the factors that promote cybercrime among university students which are: technological support; peer influence; law and enforcement; technology inclination; economic situation. All the factors were found to promote cybercrime, with all showing a positive relationship with perceived cybercrime stimulus. All the factors showed a strong positive correlation with perceived cybercrime stimulus. All the hypotheses stated for the study were accepted.

Table 5.7: Summary of findings

Hypothesis	IV	DV	Supported	Correlation coefficient (+/- Positive / Negative)	R value
H1	TS	PCS	Yes	Strong+	.968
H2	PI	PSC	Yes	Strong+	.985
H3	LE	PSC	Yes	Strong+	.988
H4	TI	PSC	Yes	Strong+	.972
H5	ES	PSC	Yes	Strong+	.974
H6	PSC	BI	Yes	Strong+	.973

CHAPTER 6
CONCLUSION AND RECOMMENDATIONS

This chapter presents the conclusion of the study based on the results of the analysis conducted. The chapter goes further to make recommendations for future studies.

6.1 Conclusion

Day by day, the rate of cybercrime among student increases. In order to know what cause cybercrime among students, many scholars have examined various types of cybercrime among students. However, limited studies were found to have specifically examined the factors that promote cybercrime among students. In addition, no model was found to explain the various factors that promote cybercrime among students. Based on this gap, the author proposed a model to explain the factors that promote cybercrime among students. Five factors were proposed as factors that promote cybercrime among students. The proposed model of this study was tested and used for examining the factors that promote cybercrime among students. From the hypotheses tested and results of the study, all the five factors proposed in the model promotes cybercrime behavior among students. However, the degree of the effect of each of the factors on cybercrime act varies. This implies that the proposed research model and the questionnaire used in this study is acceptable to examine the factors that promotes cybercrime among university students.

6.2 Recommendations

Based on the results of the study, the study makes the following recommendations:

- This study covered students from Near East University in North Cyprus only. Further studies on related topic is recommended to cover more universities from different countries to get more insight about the different factors that may promote cybercrime among students.
- The factors revealed from the study should be used as reference on how to reduce cybercrime among university students. Factors such as law and enforcement should be taken into consideration by including it in the school curriculum if not currently present in school or department curriculum.

- Other factors such as the technology inclination should be addressed by advising students with more technology related background to make use of the knowledge they have in a positive way rather than for crime.

REFERENCES

Ahmed, D., Mingzhu, W., and Tarik, D. (2015). Determinants of software piracy under risk aversion: a model with empirical evidence. *European Journal of Information Systems, 24*(5), 519-530.

Alraimi, M., Zo, H., and Ciganek, P. (2015). Understanding the MOOCs continuance: The role of openness and reputation. *Computers and Education*, *80*, 28-38.

Amit, W., and Neerja, A. (2017). A review on cybercrime major threats and solutions. *International Journal of Advanced Computer Research*, *8*, 2217-2221.

Berry, M., and Bainbridge, S. (2017). Manchester's Cyberstalked 18-30s: Factors affecting cyberstalking. *Advances in Social Sciences Research Journal*, *4*(18), 4-15.

Binesh, S., Salman, Z., Saira, A., and Khurram, E. (2018). Usage of social media tools for collaborative learning: the effect on learning success with the moderating role of cyberbullying. *Journal of Educational Computing Research, 1*(2), 1–34.

Bing, W., and Xiaohui, C. (2017). Continuance intention to use MOOCs: Integrating the Technology Acceptance Model (TAM) and Task Technology Fit (TTF) model. *Computers in Human Behavior, 67*. 221-232.

Bradford, R. (2019).Online pursuit in the twilight zone: cyberstalking perpetration by college students. *Victims and Offenders*, *14*(2), 183-198.

Byeng-Hee, C., Sang-Hyun, N., Shin-Hye, K., and Sylvia, M. (2017). Toward an integrated model of software piracy determinants: A cross-national longitudinal study. *Telematics and Informatics, 34*(7), 1113-1124.

Carlos, G., Hanif, M., Cetin, O., Moore, T., and Eeten, M. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys*, *49*, 1-27.

Catherine, D., George, E., and Melissa, L. (2014). Juveniles and cyber stalking in the United States: an analysis of theoretical predictors of patterns of online perpetration. *International Journal of Cyber Criminology, 8*(1), 10-22.

Christopher, P., and Christiana, C. (2017). Examining cyberbullying across the lifespan. *Computers in Human Behavior, 71*, 444-449.

Dale, W., and Jeffrey, N. (2016). The use of specialized cybercrime policing units: an organizational analysis. *Criminal Justice Studies, 29*, 105-214.

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly. 13*(3), 319-340.

Diana, J., and Sheri, B. (2018). Moral disengagement about cyberbullying and parental monitoring: effects on traditional bullying and victimization via cyberbullying involvement. *Journal of Early Adolescence, 38*(3), 303–326.

Donna, C., Amy, B., Alana, P., Kate, H., Lydia, H., and Leanne, L. (2015). A social–ecological framework for understanding and reducing cyberbullying behaviors. *Aggression and Violent Behavior, 23*, 109-117.

Emma, S., Andrew, G., Jacqui, A., and James, B. (2015). The impact of cyberstalking *Studies in Media and Communication*, *3*(2), 12-21.

Enrica, C., and Andrea, B. (2014). Emotion-related personality traits and peer social standing: Unique and interactive effects in cyberbullying behaviors. *Cyberpsychology, Behavior, and Social Networking, 17 (9),* 584-590.

Filipa, P., and Marlene, M. (2016). Cyber-stalking victimization: What predicts fear among Portuguese adolescents? *European Journal on Criminal Policy and Research*, *22*(2), 253-270.

Folashade, B., and Abimbola, K. (2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna State, Nigeria. *American International Journal of Contemporary Research*, *3*(9), 14-17.

George, D., and Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference.11.0 update (4th ed.). Boston, MA: Allyn & Bacon.

Hannah, L., Shayna, G., and Jaana, J. (2016). Who is to blame? the effects of victim disclosure on bystander reactions to cyberbullying. *Computers in Human Behavior, 57*, 115-121.

Hannah, Y., Marilyn, C., Barbara, S., Des, B., Donna, C., and Phillip, S. (2016). Cyberbullying and the role of the law in Australian schools: Views of senior officials. *Australian Journal of Education*, *60*(1), 86-101.

Ian, B. (2017). Fear 2.0: worry about cybercrime in England and Wales. *The Routledge International Handbook on Fear of Crime*, 113-125.

Igba, D., Elizabeth, C., Aja, S., Simon, C., Egbe, E., and Ogodo, J. (2018). Cybercrime among university undergraduates: implications on their academic achievement. *International Journal of Applied Engineering Research, 13*(2), *1144-1154.*

Kamini, D. (2011). Cybercrime in the society: problems and preventions *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

Katherine, T, Amie, J., Leigh, J., and Lawrence, M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society, 17*(1), 42-60.

Lowry, P., Zhang, J., Wang, C., and Siponen, M. (2016). Why do adults engage in cyberbullying on social media? An integration of online disinhibition and deindividuation effects with the social structure and social learning (SSSL) model. *Information Systems Research*, *27,* 962-986.

Markus, R., Rainer, B., and Tyler, M. (2015).Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing, 6,* 13-21.

Matti, N., Oksanen, A., Keipi, T., and Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *10*(10), 15-17.

McAfee (2014). The economic impact of cybercrime-no slowing down. McAfee cybercrime report 2014. Retrieved 12th February 2019 from https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf

Michel, W., and Wannes, H. (2011). Cyberbullying: Predicting victimization and perpetration *Children and Society, 25*(1), 59-72, 2011

Michelle, F. (2018). Cyberstalking victimization, depression, and academic performance: The role of perceived social support from parents. Cyberpsychology. *Behavior, and Social Networking, 21*(2), 110-116.

Misbah, Z., Gulikers, J., Maulana, R., and Mulder, M. (2015). Teacher interpersonal behaviour and student motivation in competence-based vocational education: Evidence from Indonesia. *Teaching and Teacher Education, 50,* 79-89.

Mohammad, A., and Sharmin, S. (2015). Software piracy in BangladeSh: the Student perceptions study on two selected public universities in Dhaka city. *Manarat International University Studies, 4*(1), 148-157.

Moreno, M.A. (2014). Cyberbullying. *JAMA Pediatr. 168* (5), 500.

Muk, A., and Chung, C. (2015). Applying the Technology Acceptance Model in a two-country study of SMS advertising. *Journal of Business Research*, *68*(1), 1-6.

Muthusankar D., Kalaavathi, B., and Deepa, M. (2016). Cybercrime risk and cyber security on online service avoidance. *Middle-East Journal of Scientific Research, 24*, 92-97.

Nicolas, D., Pedro, C., and Luís, A. (2015). A survey on software piracy empirical literature: Stylized facts and theory. *Information Economics and Policy, 32*, 29-37.

Nora, E., Antonio, R., and Ronia, H. (2016). Explaining software piracy using a new set of indicators. *Journal of the Knowledge Economy, 7*(2), 526-544.

Omale, J., and Mogom, A. (2016). Fiber optics technology and cybercrimes in Calabar metropolis Nigeria. *International Journal of Social Relevance and Concern, 4*(4), 1-16.

Pettalia, J., Levin, E., and Dickinson, J. (2013). Cyberbullying: eliciting harm without consequence. *Computer In Human Behavior*, *29*(6), 2758-2765.

Philmore, A., Sherlexis, S., and Terry, H. (2015). Predicting accounting students' intentions to engage in software and music piracy. *Journal of Academic Ethics, 13*(4), 291-309.

Ruth, F., Scharkow, M., and Quandt, T. (2013). Peer influence, internet use and cyberbullying: a comparison of different context effects among German adolescents. *Journal of Children and Media*, *7*, 446-462.

Sabillon, R., Cano, J., Victor, C., and Jordi, S. (2016). Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security*, *4*(6), 165–176.

Sara, P., Heidi, V., Karolien, P., Katrien, V., and Sara, B. (2016). Exposure to cyberbullying as a bystander: An investigation of desensitization effects among early adolescents. *Computers in Human Behavior, 62*, 480-487.

Sara, B., Sara, P., Heidi, V., Karolien, P., Katrien, C., Ann, D., and Ilse, B. (2016). From normative influence to social pressure: How relevant others affect whether bystanders join in cyberbullying. *Social Development*, *25*(1), 193-211.

Saragih, Y. M., and Siahaan, A. P. (2017). Cyber Crime Prevention Strategy in Indonesia. *International Journal of Humanities and Social Science*, *3*(6), 22-26.

Sebastian, W., Gabriela, K., Alexander, T., Karsten, D., and Marianne, J. (2016).A cross-national study of direct and indirect effects of cyberbullyingon cybergrooming victimization via self-esteem. *Psicología Educativa, 22*, 61–70.

Sila, I. (2015). The state of empirical research on the adoption and diffusion of business-to-business e-commerce. *International Journal of Electronic Business, 12*(3), 258-301.

Simplice, A. (2015). Fighting software piracy in Africa: how do legal origins and IPRs protection channels matter?. *Journal of the Knowledge Economy, 6*(4), 682-703.

Srikanth, T. N., Aishwarya, J. S., Irshad, J., Shruthi, B., and Bhoomika, G. Y. (2017). Explicit study on cybercrimes using internet. *International Journal of Management and Applied Science, 3*(9)*, 5-14.*

Simplice, A., and Christine, M. (2018). Technology and persistence in global software piracy. *NETNOMICS: Economic Research and Electronic Networking, 19*(1-2), 43-63.

Simplice, A., Pritam, S., and Sara, R. (2018). Fighting software piracy: Some global conditional policy instruments. *Journal of Business Ethics*, *152*(1), 175-189.

Srinivasan, V., Christy, C., Zach, L., Fred, D., and Viswanath, V. (2018). The darth side of technology use: An inductively derived typology of cyberdeviance. *Journal of Management Information Systems, 35*(4), 1060-1091.

Sumanjit, D., and Tapaswini, N. (2013). Impact of cybercrime: issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies, 6*(2), 142-153.

Suvi, M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities *Psychiatry, Psychology and Law, 24*(3), 323-338.

Szde, Y. (2014). Fear of Cyber Crime among College Students in the United States: An Exploratory Study. *International Journal of Cyber Criminology, 8*(1)*, 36–46.*

Xiang, F., and S, Lee. (2016). Comparative empirical analysis on computer software piracy behaviors between China and the United States: An exploratory study. *Journal of International Technology and Information Management, 25*(2), 4.

Zhiyong, Y., Jingguo, W., and Mehdi, M. (2015). Effect of peer influence on unauthorized music downloading and sharing The moderating role of self-construal. *Journal of Business Research, 68*(3), 516-525.

APPENDICES

APPENDIX 1

ETHICAL APPROVAL LETTER

YAKIN DOĞU ÜNİVERSİTESİ

BİLİMSEL ARAŞTIRMALAR ETİK KURULU

22.01.2019

Dear Adeniyi AdegbolaEgbeleke

Your application titled **“Investigating The Factors That Promote Cybercrime Among University Students”** with the application number YDÜ/FB/2019/56 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

Direnc Kanol

APPENDIX 2

QUESTIONNAIRE

INVESTIGATING THE FACTORS THAT PROMOTE CYBERCRIME AMONG UNIVERSITY STUDENTS

Dear Student,

The aim of this questionnaire is to understand the factors that promote cybercrime among university students. This questionnaire does not attempt to indict you as a cybercriminal but to get your general opinion on what promotes cybercrime among university students by choosing the answer that you feel closest to. The result of this questionnaire will be used for analysis of educational research report only and not be made available to other institution.

Thank you for your interest to answer this questionnaire

Adeniyi Adegbola EGBELEKE

Prof. Dr. Nadire CAVUS

SECTION I: Personal Information

1. Gender a) Female b) Male
2. Nationality a) Middle East b) Africa (Nigeria, Ghana, Zimbabwe, Cameroon, Congo, Rwanda…..) c) Europe d) Asia (India, China,,,,,,)
3. Age a) 18 b) 19 c) 20 d) 21 e) 22 f) 23 g) 24 h) 25+
4. Department a) CIS b) Computer Engineering c) IT d) MIS e) others
5. Year a) 1 b) 2 c) 3 d) 4 e) Masters

SECTION II: Factors that Promote Cybercrime

	Strongly Agree	**Agree**	**Undecided**	**Don't Agree**	**Strongly Disagree**
Technological Support					
1. I think the availability of software and tools makes cybercrime act easy to perform by students					
2. I have come across tutorials on how to download licensed software for free on the internet					
3. I think new software makes it easy for students to copy digital products					

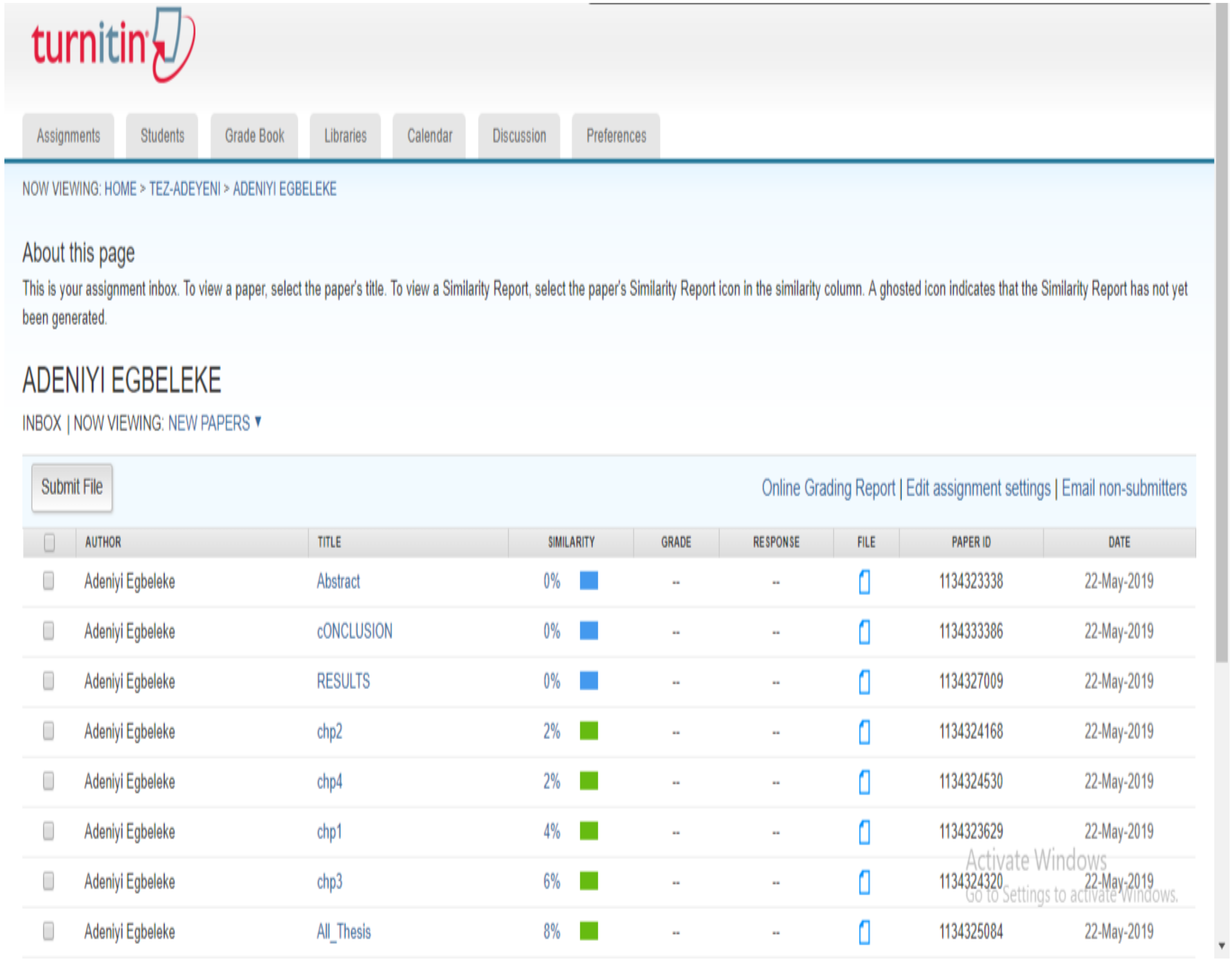
4. I know of websites that offer cracked software for free					
5. I know of websites I can get free product key for licensed software					
Peer Influence					
1. I have friends that also use licensed software for free					
2. I think many students into cybercrime have mentors that guide them					
3. I think students generally like to do what their classmates do					
4. I think some students involve in cybercrime when they see friends profit from the act					
Law and Enforcement					
1. I think low or no punishment from cybercrime act promote the act					
2. I think many students are not aware of any law and punishment behind cybercrime					
3. I think when a student is punished others would stop					
4. I think students involve into cybercrime because they believe they won’t be caught					
5. I think students continue when they know no punishment will arise from the act					
Technology Inclination					
1. I think student with more of technology background find it easy to commit cybercrime					
2. I think student in IT field are taught about types of cybercrime					
3. I think students familiar with cybercrime from classroom will know how to perpetrate the act					
4. I think students in IT field use cybercrime as a means of practicing what they were taught					
Economic Situation					
1. I think many students prefer to crack software because no money to buy					
2. I think many students involved in online scam do for financing their study					
3. I think some students from poor homes use money from internet scam to support their family					
4. I think many students resell copyrighted product to make money					
Perceive Cybercrime Stimulus					
1. I think there is a motive behind cybercrime					
2. I think students commit cybercrime known or unknown to them					
3. I think there is pathway into cybercrime					
4. I think cybercrime is a trend among students					
Behaviour Intention					
1. I think student will want to involve in cybercrime if it is easy to commit					

2. I think student will not want to involve in cybercrime if they have knowledge about the harm it cause					
3. I think students will not want to involve in cybercrime if they are not reinforced					
4. I think students will want to commit cybercrime if they will profit from it					

Thank You For Your Time

APPENDIX 3

SIMILARITY REPORT



NOW VIEWING: HOME > TEZ-ADEYENI > ADENIYI EGBELEKE

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.

ADENIYI EGBELEKE

INBOX | NOW VIEWING: NEW PAPERS ▾

Submit File
Online Grading Report | Edit assignment settings | Email non-submitters

□	AUTHOR	TITLE	SIMILARITY	GRADE	RESPONSE	FILE	PAPER ID	DATE
□	Adeniyi Egbeleke	Abstract	0% 🟦	--	--	▯	1134323338	22-May-2019
□	Adeniyi Egbeleke	cONCLUSION	0% 🟦	--	--	▯	1134333386	22-May-2019
□	Adeniyi Egbeleke	RESULTS	0% 🟦	--	--	▯	1134327009	22-May-2019
□	Adeniyi Egbeleke	chp2	2% 🟩	--	--	▯	1134324168	22-May-2019
□	Adeniyi Egbeleke	chp4	2% 🟩	--	--	▯	1134324530	22-May-2019
□	Adeniyi Egbeleke	chp1	4% 🟩	--	--	▯	1134323629	22-May-2019
□	Adeniyi Egbeleke	chp3	6% 🟩	--	--	▯	1134324320	22-May-2019
□	Adeniyi Egbeleke	All_Thesis	8% 🟩	--	--	▯	1134325084	22-May-2019