

## An assessment of cybersecurity awareness level among Northeastern University students in Nigeria

Adamu Abdullahi Garba<sup>1,2</sup>, Maheyzah Muhamad Siraj<sup>2</sup>, Siti Hajar Othman<sup>2</sup>

<sup>1</sup>Department of Computer Science, Yobe State University, Damaturu, Nigeria

<sup>2</sup>School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru, Malaysia

### Article Info

#### Article history:

Received Mar 23, 2021

Revised Jul 15, 2021

Accepted Aug 2, 2021

#### Keywords:

Cybersecurity awareness  
Cybersecurity knowledge  
Information security  
University students

### ABSTRACT

The world economy today has adopted the internet as a medium of transactions, this has made many organizations use the internet for their daily activities. With this, there is an urgent need to have knowledge in cybersecurity and also how to defend critical assets. The objective of this paper is to identify the level of cybersecurity awareness of students in Northeastern Nigeria. A quantitative approach was used for data collection and cyberbully, personal information, internet banking, internet addiction, and Self-protection were the items ask for cybersecurity awareness level identification. Descriptive analysis was performed for initial result findings using SPSS and OriginPro for graphical design. the preliminary result shows of the students have some basic knowledge of cybersecurity in an item like internet banking, while other items like cyberbully, self-protection and, internet addiction result show moderate awareness, the students' participation based on gender, males constitute 77.1% i.e. (N=340) and females constitute 22.9% i.e. (N=101). Future research would concentrate on designing awareness programs that would increase the level of their awareness especially the students in the Northeastern part of Nigeria.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



### Corresponding Author:

Adamu Abdullahi Garba

School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia

Johor Bahru, Malaysia

Email: adamugaidam@gmail.com

## 1. INTRODUCTION

Technological innovation has created opportunities for companies to carry out online transactions through the internet, which are constantly growing worldwide. For cybercriminals, the internet has become a key medium to perform several cybercrime-related activities. Studies have shown that the lack of understanding of cybersecurity attacks and threats is one of the driving factors leading to the growing number of internet-related attacks [1]. Cybercrime was defined by researchers as any criminal activity in which computers or other network devices are used to conduct illegal activities as a tool or target [2]. Emails are common means by which attackers target their victims to launch cyber-attacks like phishing, IP spoofing, social engineering, denial of service attack, and child pornography. Today, online chat forums, web searching websites, and emails are common. According to [3], Africa is becoming more internet-connected than ever before; for example, In Nigeria, alone internet users have reached 99.5 million in 2020, the figure is projected to grow to 131.7 million by 2023. It is expected that cybercrime rates will increase simultaneously.

Over the decade, cybersecurity attacks in Nigeria have become regular activities that pose a bigger threat to the economy, national security, and damage the nation's integrity. The Globe Cyber Security Agenda [4] has developed security countermeasures and techniques to curb cybersecurity attacks, and these strategies are planned to be applied internationally in the campaign to curb cybercrime activities. However,

as a way of combating cybersecurity threats, cybersecurity awareness programs have not gained much support from both the government and private organizations. Some researchers have indicated a cybersecurity awareness summary that targets a limited number of participants [5]-[7].

There is a famous crime syndicate in Nigeria called Yahoo-boys. These Yahoo-boys include the use of the internet to carry out illegal activities, such activities include account hacking, identity theft, fake relationship, and malware spreading [8]. This act has been victimized many people both locally and globally. This act has led many researchers to examine the effect of individuals or groups of a target audience on cybercrime and cybersecurity knowledge levels, but most research is based on the particular state in which participants shared the same social, economic, and cultural value. Besides, as many cybercrime victims have been identified from the southern part of the country, the government has also provided a lot of research grants and funding to conduct such studies.

This study, however, focuses on large participants of different cultural backgrounds, faith, internet exposure, and lifestyle environments, i.e. university students from the Northeastern part of Nigeria, as many studies have shown that cybercrime is growing exponentially in the region. There is an urgent need to conduct this research to determine the level of awareness of cybersecurity few studies have been published, but in Nigeria, they have concentrated on selected states [7]. University students were selected because of the diversity of the environments where many people with a different culture, faith, lifestyle, and internet exposure live under one roof. The justification of selecting university students also was the result of frequent internet access for either educational activities or pleasure. This factor makes them a prime target for cyberattacks furthermore those students are future perspective staff and scientists in the future. Another explanation for this research is that the government has issued grants through the tertiary education trusted fund (Tetfund) to conduct such research to provide a solution in the Northeastern part of the country to reduce and enhance cybersecurity awareness knowledge in (Nigeria).

Research in the cybersecurity domain is getting momentum focusing on design and implementing end-to-end security mechanisms to ensure integrity and confidentiality of data and information. Nevertheless, cybersecurity awareness programs are considered as the first line of security defense to avoid security attacks and threat confrontation. Nigeria is among the top African country that is affected by cyber-attacks and threats targeting young students through phishing and scamming attacks. Therefore, this study target University students in the Northeastern part of Nigeria to identify the level of their cybersecurity awareness of the following items, internet banking, self-protection, cyberbully and, internet addiction. The research purpose of conducting this study in the north-eastern states of Nigeria is to investigate cybersecurity awareness of the university students, the objective include: to identify the level of cybersecurity awareness regarding the following items: cyberbully, internet banking, internet addiction, and self-protection of university students in the northeastern states of Nigeria. This paper consists of 5 sections. Sections 2 discussed the existing literature section 3 present research methodology section 4 present result and discussion, section 5 concludes the findings.

## 2. OVERVIEW ON CYBERSECURITY AWARENESS

Cybersecurity awareness programs and training are regarded as one of the first defense lines and also the most effective means of improving cybersecurity practices [9]. Most cybersecurity awareness programs aim to change the security behavior of individuals [10]-[12]. A study conducted by Serianu Agency's Nigeria Cyber Security Study 2016 appointed out an increase in cyber threats and attacks which cost a loss of \$550 million to the Nigerian government. This indicated most users are not aware of the danger of cybercrimes and their implications to the economy of a country. However, from the study, awareness, and training, continuous monitoring and log analysis, vulnerability and patch management, continuous risk assessment and treatment, and managed services and independent reviews are the top 5 2017 cybersecurity challenges [4].

From the African point of view and to the Nigerian context, the best approach in addressing or mitigating cybersecurity issues from the survey was that almost 95 percent of respondents agree that: Awareness training is the primary driving force that will make everyone aware of the problems and danger of cyber-attacks on their businesses. Some respondents also have the view that the IT budget will increase so that technical measures will also be included. Respondents also agree that "Education and knowledge is the best way, once a common man is aware of this, he will be vigilant". The best approach in dealing with cybersecurity in Nigeria from this is to educate both public and private individuals about the possibility of cyber-attacks before it happens. Therefore, according to Ben Robbert, Liquid Telecom Group Chief Technical Officer, Kenya says he answered "My top 3 priorities are education, education, and education". All companies need to make sure that all staff are aware of the danger of cybersecurity and should have a basic knowledge of cybersecurity irrespective of their department.

### 2.1. Cybersecurity awareness program in education domain

The university system is becoming increasingly digitized day by day, as currently in this epidemic, online courses and degree are prevalent, also new learning methods that fully depending on technology has been adopted. Existing research on the security of the online learning system has detailed out some challenges in using online platforms for educational purposes such are attacks on protecting students' examination and processes, content filtration and virus, and malware attacks. There are many motives toward targeting educational institutions as large databases are containing valuable information of students and also a lack of security controls in university on what devices students can bring and use in their learning process environment. This issue makes it important to create a secure learning environment. Many researchers have focused on how to identify the antecedent of cybersecurity awareness and some authors have adopted the theories explained above to assess the impact of individual factors like age and gender on cybersecurity knowledge and behavior [12]. Cybersecurity awareness has been implemented in the educational domain for the purpose to either identify the level of awareness or implementing a program to increase the level of awareness among students and academics as well. Educational establishment offends use the internet in research, therefore they can be victims of cyber-attack, especially the students whose knowledge of cybersecurity is limited as some research pointed [13]. Students mostly engage in social networking using the university internet as such their personal information can be compromised or vulnerable to cyberbullying as there is much available information about hacking skills that can equip potential offenders with knowledge and tools to hack. Therefore universities must provide preventive measures to countermeasure any attack as there is a relationship between preventive measures and information security awareness [14]. Cyber-attacks can be only minimized if people (students) have adequate knowledge and practice good behavior when using the internet as a relationship exists between the two.

### 2.2. Cybersecurity awareness in universities as a case studies

Many researchers have surveyed to identify the level of awareness or implement a program to increase the level of awareness among students and academics as explained before, however in this section, some available studies include that of [15], [16] they perform a survey on computer science students at Yobe State University to identify the level of cybersecurity awareness level and to also know among the student gender who is more vulnerable to cyber-attacks. The results indicated the majority of the students have less or limited basic knowledge on cybersecurity and also female students are more likely to be cyber victims [17]. This result indicated a need for a cybersecurity awareness program to be implemented at the university as a course or frequent workshop that will be explaining the cybersecurity domain. Also, another study was conducted in the Middle East among students and professionals to identify the security awareness level and the results show less inside on the process or method on how it was conducted but the result indicated a need for a cybersecurity awareness program [18]. Security policies should be written when designing and conducting a cybersecurity awareness program for guiding the users on how to use the organizational system (university).

Another study was also conducted to identify the risk of social networking site among students a survey was conducted in Malaysia, the results show many students have been a victim of this scam i.e. one-third of 295 participants [19], this indicates the need for a security awareness campaign to the students. Moreover, in the US Pacific Northwest University, students participated in a survey to identify cybersecurity awareness and the result from 498 students shows they were not familiar with some basic cybersecurity terms, among the terms are Trojan horses (55%), phishing (50%) and worms (17%) [20]. This indicated a need for a cybersecurity awareness program at that the university. All these case studies have clearly shown how cybersecurity awareness programs are needed in many universities in the world to increase the level of cybersecurity knowledge and also to minimize the frequent basic cyber-attacks on students' information and universities' infrastructures. Games have been used to see their effectiveness at its early stage by many researchers. From this stage, many other fields of studies have been using games as an alternative or additional mode of education, particularly at this present time of the COVID-19 pandemic as physical interaction is restricted as Frameworks have been constructed to analyze games in the education sector by many researchers such as [21]-[24]. Many studies were conducted to identify the cybersecurity awareness of university students as explained above, but specifically to the universities located in northeast Nigeria is limited as more researchers focus on the southern part of the country. The gap here is there is no much related work covering the northeastern students as many cybercrimes were reported in the region. This study aims to fill this gap by conducting this study and survey to identify the awareness level of the students studying in the region.

## 3. METHOD

The quantitative data collection approach is commonly used in data collection and analysis as reported in [25]-[27]. Similarly, this study adopted a similar research method for data collection and analysis from

participants. The question used in this research was adapted from a study of [28] where they try to investigate University students' cybersecurity awareness level on the following item personal information, internet banking, cyberbully, internet addiction, and self-protection, in Universiti Kebangsaan Malaysia. Based on the context of this research objective the following items are been investigated: Personal information, internet banking, self-protection, cyberbully and, internet addiction of university students in the North-eastern states of Nigeria. The paper adopted [29] for data collection and processing to make it easier to be repeated and generalized.

### 3.1. Instrument design

The questionnaire was designed using Google form and distributed via various platforms. The questions were organized under the above items, each item consists of four questions making a total of twenty questions. All these questions were asked to answer the research objective. To answer the question each participant is required to indicate the level of agreement and disagreement with the statements using the concept of a five-point Likert scale from strongly disagree "1" to strongly agree "5" as Table 1 shows the instrument used in data collection.

More than 600 participants were selected to participate (July to September 2020), 500 feedback were returned, and 51 feedbacks were deleted after filtering the completed questionnaires. Therefore 441 feedbacks were used for the analysis. The surveyed states include Adamawa, Borno, Bauchi, Gombe, Taraba, and Yobe. Due to Covid 19 pandemic, all universities are closed, therefore. The expected time to complete the questionnaire is estimated to be 20 minutes. Table 2 shows the responders' representation details.

Table 1. Measurement scale

Scale	1	2	3	4	5
Measurement	Disagree	Disagree	Neutral	Agree	Strongly agree

Table 2. Distributed sample description

University	Sample Size 600 (minimum)
Yobe	100
Borno	100
Gombe	100
Adamawa	100
Bauchi	100
Taraba	100
Discarded	59
Total	441

## 4. RESULTS AND DISCUSSION

This section analyses the feedbacks obtained from the items (questionnaire distributed to the students) i.e. demography analysis, internet banking, self-protection, cyberbully and, internet addiction. Demographic analysis. This section explains the participants that participated in the survey, the information includes gender, age, and university type. Figure 1 shows the age group. Figure 1 shows the three categories of age groups and the number of participants, the number of respondents between 18-20 age group is 17.9% i.e.79 respondents, the age group between 21-25 is 45.6% i.e. 201 respondents and lastly, the age group between 26-30 is 36.6% which 161 respondents.

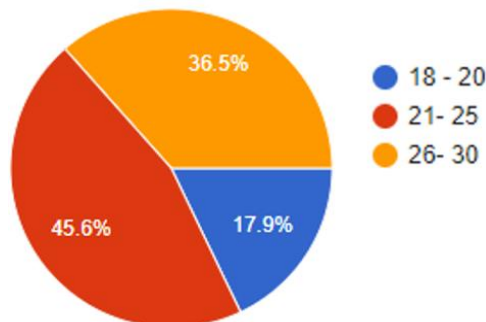


Figure 1. Age group analysis

#### 4.2. Gender group analysis

This section explains the gender group of the participants and the number of each gender that has participated in the survey. Figure 2 shows the gender type. Figure 2 shows the number of participants based on gender, males constitute 77.1% i.e. 340 and females constitute 22.9% i.e. 101 individuals. This has indicated male is more interested in cybersecurity awareness, as the results show more than 77% is the male respondent.

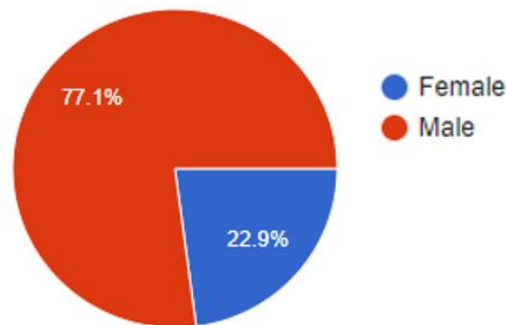


Figure 2. Gender group analysis

#### 4.3. University type analysis

This section explains the type of responders' Universities, as in Nigeria, there are three types of Universities: private, state, and federal. Figure 3 shows the university categories. Figure 3 shows the type of universities the survey responders come from, students from the private University are 18.1%, i.e. N=80 State Universities are 33.1% i.e. N=147 and federal Universities are 48.5% i.e. N=214 respectively. Figure 4 indicated a large share of federal universities has participated more than the other Universities.

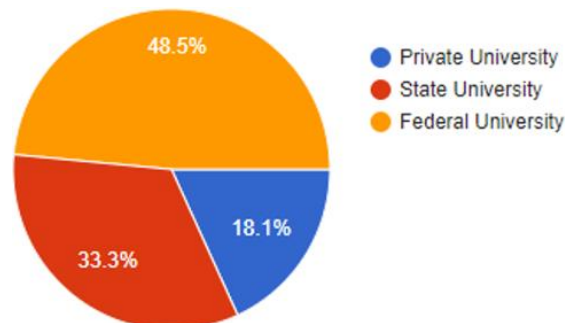


Figure 3. Responders University categories

#### 4.4. Awareness of internet banking

This part also analyses the students' feedback from the conducted survey on how students behave when using internet banking. Internet banking has now become a major part of everyone's life, therefore more cybercrimes are been reported regarding the use of internet banking, cyber-attacks related to internet banking include internet scams, denial of service attacks, and phishing emails. Hence, there is a need for students to be aware of the dangers of using internet banking and also how to protect their financial information. Figure 4 illustrates all the questions results from the survey.

– Q1: *I will only make an online purchase after inspecting the seller's background*

The question is about making a purchase online without understanding the background of the seller (N=219, 49.7%) majority of the student make sure they are familiar with the seller before making any purchase, while (N=23, 5.2%) just make online payment without checking the seller information. The analysis has demonstrated around 50% of the responders are careful when making any online transaction and seller information is doable checked before making payment. The participants have indicated they are aware of online scammers and are diligent when making an online payment.

- *Q2: I will not make any online purchase if I found the quality of the good is unreliable*

The result indicates a higher awareness when it comes to online purchases (N=270, 61.2%) strongly agree on only buying what is reliable, while (N=28, 6.3%) show less interest in checking items before buying. This point to that the majority of the students have some basic knowledge of internet scammers like the previous question analysis as more than 60% purchases good of good quality and after knowing the sellers' information, it further points out knowing online fraudulent.

- *Q3: I am worried when I received any suspicious online advertisement*

The answer to the question on receiving any suspicious online advertisement indicated (N= 180, 40%) a large number of students are worried about receiving unwanted messages across their account, while (N=107, 24.3%) also agree with the statement, and (N=34, 7.7%) do not worry or care on receiving any kind of message. This result proves how students are careful of what they see and receive from an unwanted source as phishing email has become the simplest way criminal uses to get information from their target, this has shown a large proportion of the responders are aware of such attack.

- *Q4: I will provide my personal information whenever I received calls from banking organizations*

The question describes how the students feel or act when they received a call from banks asking for personal information (N=212, 48.1%) disagree with the questions while only (N=68, 15%) just agree to the questions. The analysis confirms that the majority of the students are very aware and familiar with yahoo-boys' methods of scamming victims as 68% attested to that, however, more cybersecurity awareness program is needed to educate the remaining 48% of the student as shown in Figure 4.

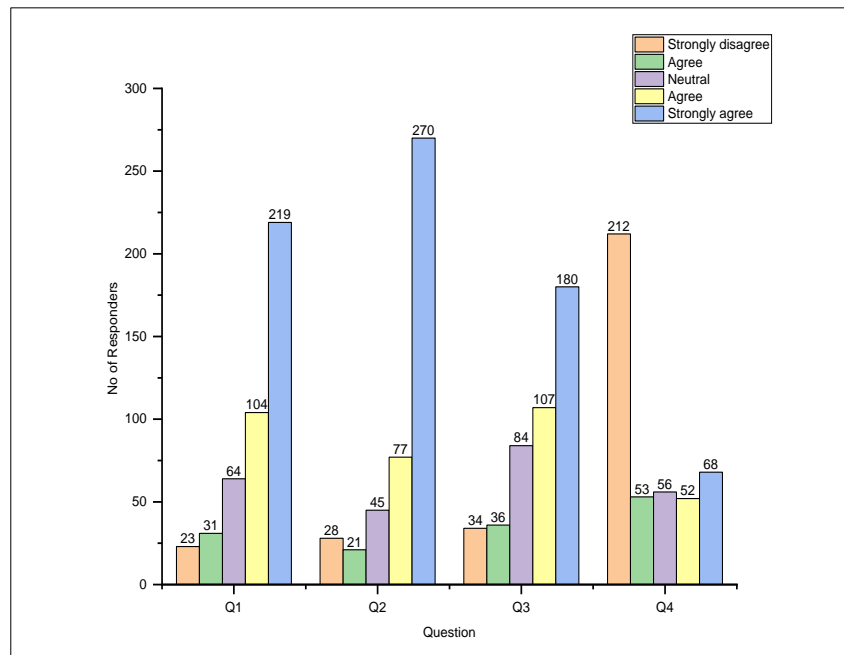


Figure 4. Respond to internet banking

#### 4.5. Awareness of self-protection

Awareness of Self-protection is significant, as many attacks can be successful if an individual has fallen to protect their data. Therefore this section evaluates the responses from the responders on how well are they aware of self-protection when it comes to cybersecurity. Figure 5 shows all four questions with their analyzed results.

- *Q1: I will only add new friends to my social media after inspecting their background*

The results shows (N=185, 42.2%) have strongly agreed to check any friend request before adding, while (N=96, 21.5%) are neutral, and only (N=30, 6.8%) strongly disagree. The analysis shows that 50% of the students check friend request background before accepting or rejecting as many cybercriminals use social media to lunch social engineering attacks, this has confirmed the responders are aware of such attacks and are careful of who to befriend. However, more awareness is needed to practically demonstrate how such an attack occurs.

– *Q2: I think I will consider meeting my new online friend alone*

The result on whether students can meeting a friend made online alone (N=122, 27.7) selected “neutral”, this indicates they do not mind. While another (N=94, 21.3%) and (N=66, 15%) disagree on meeting a friend made online alone. The analysis revealed around 50% have agreed while another 50% disagreed on meeting new online friends alone, this has indicated urgent awareness is needed here to enlighten the danger of that to the students who agree to the question as many criminals take this advantage to kidnap and demand a ransom.

– *Q3: I will not share my contact number with a person whom I newly know when asked*

The responders' response as (N=155, 35.1%) and (N=94, 20.9%) have agreed (both “strongly agree” and “agree”) not to share contact number with a new person made online, while only (N=37, 8.4%) strongly disagree with the question. The outcome of the analysis has indicated that the majority of the students are vigilant to whom they can share their personal information as more than 50% affirmed that, this is a clear indication that reveals the responders have basic awareness on how to interact with people made on social media platforms.

– *Q4: I will inform my parents when my online friends want to meet me up*

The analysis of the question shows (N=169, 38.3) and (N=78, 17.9%) have selected “agree”, this shows that they would notify their parents when meeting an online friend, while (N=98, 22.2%) are neutral and (N= 52, 11.8%), (N=44, 10%) have disagreed with the question. The result in Figure 5 indicated the responders can meet an online friend with their parents' consent as 56.2% agreed to that, this implies parents are aware when it comes to meeting new people, and is good to avoid being kidnaped or harass.

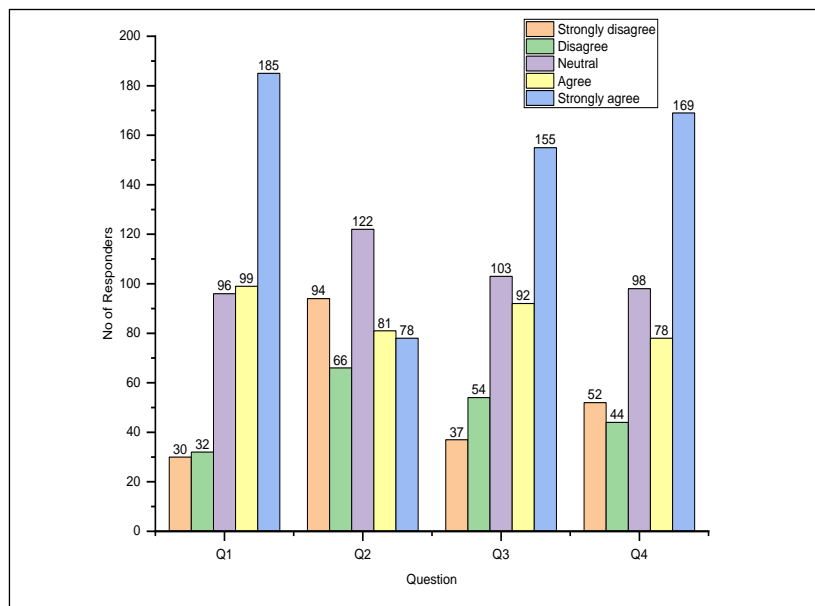


Figure 5. Respond to self-protection

#### 4.6. Awareness of cyberbully

Cyberbully is among the top cybercrime that affects the young generation i.e. students due to their excessive usage of social media platforms, victims are usually threatened to do or give something in exchange for their stolen information, therefore is urgent to know the impact of this attack on the students as there is less program that tackles cyber harassment awareness courses that focus the perpetrators of these crimes [30]. Figure 6 shows the analysis of all the questions' feedback.

– *Q1: although I felt unsatisfied with someone, I will never express it through social media*

The result shows that (N=180, 40%), (N=97, 22%) have agreed not to express their hatred to some online, while the same proportion (N=97, 22%) are neutral to the expression. (N=42, 9.5%) and (N=25, 5.7%) disagree with the question. This shows that they do not mind expressing their feelings to a person through social media. Overall indication concludes that the majority of the responders agreed not to express dissatisfaction with someone via social media, also the analysis proofs student might likely not be involved in that act of cyberbully.

- *Q2: I think giving harsh comments to my friends on social media is not a good thing to do*

The analysis indicated (N=266, 60.3%) and (N=91, 20.6%) have agreed is not a good idea to write a harsh comment to a friend when replying to his/her post or message, however, a small percentage have disagreed with the question (N=20, 4.5%) and (N18, 4.1%). The outcome shows that 80% of the responders have agreed not to use harsh wording when replying to a post, this question also indicated the surveyed students might likely not be involved in a cyberbully act.

- *Q3: I think it is not acceptable to criticize someone when they uploaded their controversial photos*

The analysis shows (N=176, 39.9%) and (N=106, 24%) that accounts to 63% of the responders have agreed is not good to criticize someone for uploading a provocative photo on social media, while only a few have disagreed with the question and those account 8.6% of the total responders, likewise 22.9% are neutral which implies they can either be of agreeing or disagree section. The overall analysis displays majority would not be involved in criticizing someone just because they uploaded a provocative photo or even statement, this means the surveyed responders are well-mannered individuals.

- *Q4: I will never express my anger to someone through social media*

This question was asked to know if the students can ever going to express their anger on social media and the results indicated (N=166, 37.65) and (N=91, 20.6%) have agreed to that while (N=104, 23.6%) are neutral to the question, however, 17% of the responders have differed to the question. This outcome in Figure 6 shows responders would not express their anger to anyone through social media as 57% have agreed to that, this implies how the responders can control their anger via social media.

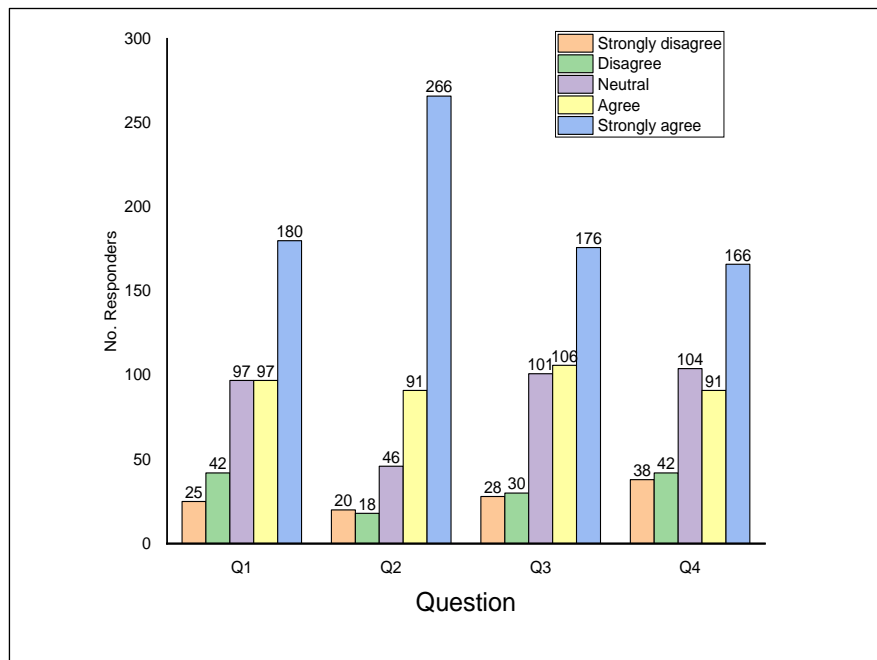


Figure 6. Respond to cyberbully

#### 4.7. Awareness of internet addiction

The internet has become part of almost everyone's lives, as many businesses, works, interaction has turned to be performed through the internet, in this context, and the internet is a vital medium in researching by educational initiations. To identify the impact of internet addiction the question was asked. Figure 7 shows an analysis of the surveyed feedback collected from the participants.

- *Q1: I will be extra excited when I use the Internet*

The question would determine how occupied students are well using the internet, the results show (N=148, 33.6%) and (123, 27.9%) have agreed to be excited when using the internet, while 11% of the responders disagree with the question and also 23.4% have shown less interest on the question. The analysis shows that almost 60% of responders are happy when using the internet, this entails if cybersecurity awareness is less there might be at risk of cyber-attacks, therefore proper enlightenment on how to use the internet safely without being a victim of cyber threat.



– *Q2: The time spent without surfing the Internet is the most boring moment*

This questions the result affirms that (N=111, 33.6%) and (N=98, 22.25) have agreed that they are happier when spending their time on the internet, while 29% differ with the question and a fraction of some students 23.3% are neutral to the question. The feedback indicated that 55% of the students' life is boring when not using the internet, however, it also supports the previous question was almost 60% of the responders are extra excited when using the internet, it implies students should be careful when interacting with people as many criminals as turn to the internet to get their victim.

– *Q3: Without the Internet, there is nothing I can do*

The result remarkably indicates students can be engaged in another thing if there is no internet as the result shows (N=122, 27.9%) and (93, 21.1%) disagrees with the statement they cannot do anything without the internet, while a small percentage i.e. 29.9% have supported to the questions and another 21.1% are neutral to the statement. The last question was asked to see if students prefer outdoor activities or just spending time on the internet at home, looking the feedback from Q1 and Q2 were it indicate how happy they are when using the internet, but here it also shows they can still do other things apart from spending much of their time surfing the internet.

– *Q4: I would spend more time on social media than having outdoor activities*

The result surprisingly indicates (N=120, 27.2%) are neutral, this shows majority can be both i.e. can spend time on the internet and also can do some other outdoor activities, but the overall results of those that agreed with the statement are 37% which are higher than the neutral responders, however, a small segment which accounts up to 35.1% have disagreed with the questions. This question is among the close range number of responders to each Likert scale, but here the highest one is the agreed section with 37%, it shows a quite number of students can do other outdoor activities as well. These show the relationships between each question and the link between them in other to identify how addicted students are to the internet as indicated in Figure 7. The objective of the study is to identify the level of cybersecurity awareness regarding the following items: Self-protection, cyberbully, and internet addiction of university students in the north-eastern states of Nigeria this section discusses the results obtained from the survey feedback and also addressing the research objectives.

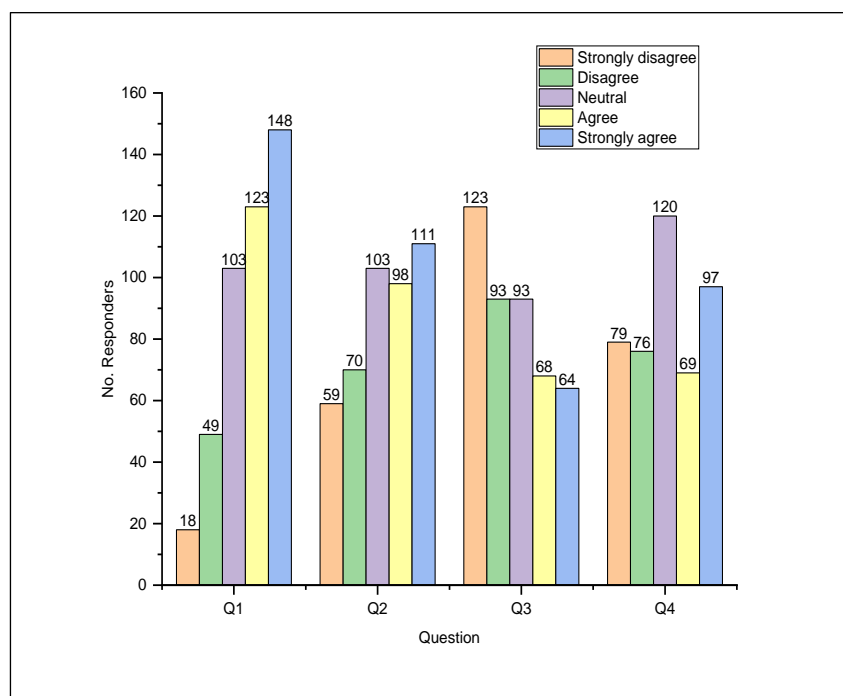


Figure 7. Respond to internet addiction

#### 4.8. Level of cybersecurity awareness among students in the north-eastern states of Nigeria

This section explains the method used in discussing the result obtained. Mean and standard deviation are used to analyze the result.  $M$ =Mean is the average and is obtained as the sum of all observed

outcomes from simple divided by the total number of events. We use the  $\bar{X}$  bar as the symbol for the sample mean where n is the sample size and the xi corresponds to the observed valued.

$$\bar{X} = \frac{1}{N} \sum_{i=1}^N xi \quad (1)$$

SD = standard deviation is used to measure the amount of variability or dispersion from the individual data values to the mean, it also indicates how accurately the mean represents sample data.

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^N (xi - \bar{X})^2} \quad (2)$$

Variance =  $\sigma$ , where  $X_1, X_2, X_3, \dots, X_n$  is the sample and  $\bar{X}$  is the mean of the sample? The denominator N-1 is the number of degrees of freedom in the vector. We calculate M based on our questionnaire as 5 points Likert scale was used. The method used in calculating is described as follows: To determine the minimum and maximum length of 5 points Likert scale, we calculate the range by (5-1=4) then we divided by 5 as it is the greatest value of the scale (4/5=0.8), then 1 which is the least value on the scale was added to identify the maximum of the cell. The cell determined below:

- From 1 to 1.80 is (strongly disagree)
- From 1.81 to 2.60 is (disagree)
- From 2.62 to 3.40 is (neutral)
- From 3.41 to 4.20 is (agree)
- From 4.21 to 5.00 is (strongly agree)

While for SD based on the rule of thumb, an SD  $\geq 1$  indicates a relatively high variation, while SD  $< 1$  can be considered low. This indicates the distribution with variation higher than 1 are considered to be high variance while those with SD lower than 1 are considered to be low-variance. However, there is no such term as good or bad SD, it only shows how to data is spread out.

#### 4.9. Discussion on internet banking item students' awareness level

Internet banking has become the easiest method of making transactions without physically going to the bank, in this section Student feedback was discussed to see how aware they are in terms of internet banking-related cyber-attacks. The question "I will only make an online purchase after inspecting the seller's background" has a mean value of (M=4.05, SD=1.180) this indicates that almost all the students are aware of the online purchases principle, also the section question got a mean of (M=4.22, SD=1.195) indicating higher awareness when it comes to online purchase. However, the third question got an average mean of (M=3.82, SD=1.26), this means shows not all students are worried about receiving suspicious advert, this indicates a need for an awareness program even though the mean is on an average level.

The last question was meant not to have a higher mean if the students are aware as the question "I will provide my personal information whenever I received calls from banking organizations" the mean value is (M=2.34, SD=1.53), the lower mean indicate student strongly disagree with providing personal information when they receive a call from banks, however, the SD also indicate the responders' results are not concentrated around the mean value. This item feedback from students has indicated that the majority of the students are consciously aware of the related cybercrime on internet banking, taking in mind only Q3 might need an awareness program, Table 3 summarizes all the results.

Table 3. Internet banking item

S/No	item	N	Mean	SD
1	I will only make an online purchase after inspecting the seller's background	441	4.05	1.180
2	I will not make any online purchase if I found the quality of the good is unreliable.	441	4.22	1.195
3	I am worried when I received any suspicious online advertisement	441	3.82	1.261
4	I will provide my personal information whenever I received calls from banking organizations.	441	2.34	1.534

#### 4.10. Discussion on self-protection item students' awareness level

Self-protection is the fundamental item that must be known by all, however the result from the feedback indicated all the questions have an average mean value of (M=3, SD=1.3), however, only Q2 got a less mean of (M=2.96). These items indicated the surveyed students have average knowledge on self-protection, it also indicates there is a need to conduct a cybersecurity awareness program to educate them on the dangers and methods to protect their personal information. Table 4 provides more details on the results obtained.

Table 4. Self-protection item

S/No	item	N	Mean	SD
1	I will only add new friends to my social media after inspecting their background	441	3.85	1.233
2	I think I will consider meeting my new online friend alone	441	2.96	1.377
3	I will not share my contact number with a person whom I newly know when asked	441	3.62	1.300
4	I will inform my parents when my online friends want to meet me up	441	3.61	1.384

#### 4.11. Discussion on cyberbully item students' awareness level

Cyberbully has become an eminent method of attacking young individuals as many are involved in social networking, the feedback obtained explains how the surveyed students are aware of cyberbully techniques and the methods to protect themselves. The overall results indicated that there is an average knowledge on cyberbully as the mean values are (M=3) with only Q2 having a higher mean of (M=4.28) as the question shows the majority of the students will not engage in giving harsh comments on social media. The rest of the questions indicates an average knowledge of the item, however, the SD shows not all the students are neutral. This result shows the students would not be involved in cyberbully, but there is a need for awareness to explain more on the item as the overall results are average as Table 5 has indicated that.

Table 5. Cyberbully item

S/No	item	N	Mean	SD
1	Although I felt unsatisfied with someone, I will never express it through social media	441	3.83	1.222
2	I think giving harsh comments to my friends on social media is not a good thing to do.	441	4.28	1.097
3	I think it is not acceptable to criticize someone when they uploaded their controversial photos.	441	3.84	1.204
4	I will never express my anger to someone through social media	441	3.69	1.295

#### 4.12. Discussion on internet addiction item students' awareness level

Internet access has become easier especially for students as many universities have internet access subscriptions for research purposes. Nevertheless, many students tend to spend more time on social media. The result from the feedback indicate overall results have an average mean of (M=3), this implies the students are less addicted to the internet. Q3 has the only less mean of (M=2.68), this indicates students can be engaged in other things even without the internet. The result of this item shows students' addiction is at an average level, however, the SD shows less concentration of the results from the mean, which implies the majority selected "Neutral". The neutral indicate student can be addicted to some certain aspect as Table 6. This result has shown also more cybersecurity campaign is needed to enlighten the students on the basic knowledge of cybersecurity.

Table 6. Internet addiction item

S/No	Item	N	Mean	SD
1	I will be extra excited when I use the internet	441	3.76	1.151
2	The time spent without surfing the internet is the most boring moment	441	3.30	1.356
3	Without the internet, there is nothing I can do	441	2.68	1.400
4	I would spend more time on social media than having outdoor activities	441	3.07	1.388

## 5. CONCLUSION

Cybersecurity knowledge is a must for all individuals irrespective of gender, education, organization, and age group as now many activities are performed via the internet. Many developed countries have implemented strategies on the cybersecurity awareness of their citizens. Also, much research was conducted to identify the level of cybersecurity awareness of an organization's staff, an educational. Cybersecurity awareness is essential for everyone, specifically young children (university students) as they have access to the internet using the university network and also on a mobile phone. There is a need to identify the current level of cybersecurity awareness of some important cybersecurity concepts (cyberbully, internet banking, internet addiction, and self-protection) to know what to do next in-term of designing and implementation the cybersecurity awareness program.

This study has indicated the surveyed students have shown a high level of cybersecurity awareness of some items, these items include internet banking, while other items like cyberbully, self-protection and, internet addiction are moderate. Elements that are moderately known there is an urgent need for a good plan implementation of cybersecurity awareness programs to address those item issues so as students might not be a victim of cyber-attacks especially the female's students. The study's contribution was identifying the items where the students have some basic knowledge of cybersecurity and which items require urgent intervention

for the awareness program. The results were explained above and also items were discussed and also items that need awareness were identified. The research would make it easier for cybersecurity experts when designing cybersecurity awareness programs as current issues and where students are lacking have been identified. The future work would focus on designing well-appropriate cybersecurity programs that will fill the missing knowledge identified from this research. These items include cyberbully, self-protection and, internet addiction.

## ACKNOWLEDGEMENTS

We would like to convey gratitude to Information Assurance and Security Research Group (IASRG), School of Computing UTM who contribute unanimously to this research. Apart from that, thank you to the Ministry of Higher Education, Malaysia and Universiti Teknologi Malaysia, that support this research under the UTM Research Grant Q.J130000.3551.05G73.





## REFERENCES

- [1] J. Monrad. "Universities fall into the cross hairs of cyber attacks." Infosecurity-magazine.com. <https://www.infosecurity-magazine.com/opinions/universities-attackers/> (accessed Jan. 13, 2022).
- [2] F. A. Aloul, "The need for effective information security awareness," *International Journal of Advanced Information Technology (IJAIT)*, vol. 3, no. 3, 2012, doi: 10.4304/jait.3.3.176-183.
- [3] J. Clement, "Nigeria: number of internet users 2025," Statista.com. [www.statista.com/statistics/183849/internet-users-nigeria/](http://www.statista.com/statistics/183849/internet-users-nigeria/) (accessed Oct. 18, 2020).
- [4] Serianu, "Demystifying Africa's cyber security poverty line," Africa Cyber Security Report 2017, 2017. [Online]. Available: <https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf> (accessed Jan. 13, 2022)
- [5] T. V. Nguyen, "Cybercrime in Vietnam: An analysis based on routine activity theory," *International Journal of Cyber Criminology (IJCC)*, vol. 14, no. 1, pp. 156–173, 2020, doi: 10.5281/zenodo.3747516.
- [6] I. Monsurat, "African insurance (spiritualism) and the success rate of cybercriminals in Nigeria: a study of the yahoo boys in Ilorin, Nigeria," *International Journal of Cyber Criminology (IJCC)*, vol. 14, no. 1, pp. 300–315, 2020, doi: 10.5281/zenodo.3755848.
- [7] O. F. Nzeakor, B. N. Nwokeoma, and P. J. Ezech, "Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment," *International Journal of Cyber Criminology (IJCC)*, vol. 14, no. 1, pp. 283–299, 2020, doi: 10.5281/zenodo.3753223.
- [8] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Information Management & Computer Security*, vol. 18, no. 5, pp. 316–327, 2010, doi: 10.1108/09685221011095236.
- [9] M. Bada, A. M. Sasse, and J. R. C. Nuse, "Cyber security awareness campaigns: why they fail to change behavior," in *International Conference on Cyber Security for Sustainable Society*, arXiv:1901.02672, 2014.
- [10] N. Taha and L. Dahabiyeh, "College students information security awareness: a comparison between smartphones and computers," *Education Information Technology*, 2020, doi: 10.1007/s10639-020-10330-0.
- [11] K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, "Information security: management's effect on culture and policy," *Information Management & Computer Security*, vol. 14, no. 1, pp. 24–36, 2006, doi: 10.1108/09685220610648355.
- [12] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information security awareness at the knowledge-based institution: Its antecedents and measures," *Procedia Computer Science*, vol. 72, pp. 361–373, 2015, doi: 10.1016/j.procs.2015.12.151.
- [13] E. A. McDaniel, "Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness," *Issues in Informing Science and Information Technology (IISIT)*, vol. 10, no. 2012, pp. 313–324, 2013, doi: 10.28945/1813.
- [14] S. V. Ershkov, "Non-stationary creeping flows for incompressible 3D Navier–Stokes equations," *European Journal of Mechanics - B/Fluids*, vol. 61, no. 1, pp. 154–159, 2017, doi: 10.1016/j.euromechflu.2016.09.021.
- [15] A. A. Garba, S. H. Othman, and M. A. Musa, "A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach," *International Journal of Emerging Technologies*, vol. 11, no. 5, pp. 41–49, 2020.
- [16] A. A. Gabra, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: A case study," *J. Crit. Rev.*, vol. 7, no. 16, 2020, doi: 10.31838/jcr.07.16.108.
- [17] L. Slusky and P. Partow-Navid, "Students information security practices and awareness," *International Journal of Information Security*, vol. 8, no. 4, pp. 3–26, 2012, doi: 10.1080/15536548.2012.10845664.
- [18] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *Journal of Information & Knowledge Management*, vol. 15, no. 1, 2016, doi: 10.1142/S0219649216500076.
- [19] G. H. Kirwan, C. Fullwood, and B. Rooney, "Risk factors for social networking site scam victimization among Malaysian students," vol. 00, no. 00, pp. 1–6, 2017, doi: 10.1089/cyber.2016.0714.
- [20] D. Sarathchandra, K. Haltinner, and N. Lichtenberg, "College students' cybersecurity risk perceptions, awareness, and practices," in *Proceedings - 2016 Cybersecurity Symposium, CYBERSEC 2016*, 2016, pp. 68–73, doi: 10.1109/CYBERSEC.2016.018.
- [21] J. P. Gee, *What video games have to teach us about learning and literacy*, Pgrave Macmillan, 2003.
- [22] K. Squire, "Changing the game: what happens when video games enter the classroom?," *Innovate: Journal of Online Education*, vol. 1, no. 6, 2005. <https://nsuworks.nova.edu/innovate/vol1/iss6/5> (accessed Oct. 02, 2020)
- [23] Prenski, *Digital game-based learning*. New York: McGraw-Hill, 2001.
- [24] J. Gee, "What would a state of the art instructional video game look like?," *Innovate: Journal of Online Education*, vol. 1, no. 6, 2005. <https://nsuworks.nova.edu/innovate/vol1/iss6/1> (accessed Oct. 20, 2020).
- [25] Y. Yang *et al.*, "A survey on cyber security awareness among college students in Tamil Nadu a survey on cyber security awareness among college students in Tamil Nadu," *IOP Conference Series Materials Science and Engineering*, vol. 263, no. 4, 2017, Art. no. 042043, doi: 10.1088/1757-899X/263/4/042043.
- [26] A. Garba, M. B. Sirat, S. Hajar, and I. B. Dauda, "Cyber security awareness among university students: A case study," *Science Proceedings Series*, vol. 2, no. 1, pp. 82–86, Apr. 2020, doi: 10.31580/sps.v2i1.1320.
- [27] E. B. Kim, "Recommendations for information security awareness training for college students," *Information Management and Computer Security*, vol. 22, no. 1, pp. 115–126, 2014, doi: 10.1108/IMCS-01-2013-0005.





- [28] F. Khalid, Y. Daud, M. Jasmy, A. Rahman, M. Khalid, and M. Nasir, "An investigation of university students' awareness on cyber security," *International Journal of Engineering and Technology*, vol. 7, pp. 11-14, 2018, doi: 10.4236/ce.2016.711158.
- [29] J. Son, D. Kim, R. Hussain and H. Oh, "Conditional proxy re-encryption for secure big data group sharing in cloud environment," *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs)*, 2014, pp. 541-546, doi: 10.1109/INFOCOMW.2014.6849289.
- [30] L. Conradie, M. Pitchford, E. Myers, T. Barnes, and E. Short, "Cyberharassment awareness course (cybac): Influences from domestic abuse perpetrator programmes for its design and function," *International Journal of Cyber Criminology*, vol. 14, no. 1, pp. 220–235, 2020, doi: 10.5281/zenodo.3750140.

## BIOGRAPHIES OF AUTHORS







**Adamu Abdullahi Garba**     is a Ph.D. Student at Universiti Teknologi Malaysia, and a lecturer II at Yobe State University Damaturu Nigeria on leave of study, he got his first degree at the University of East London in Software Engineering in 2013 and Master in Computer Science at Universiti Teknologi Malaysia in 2015. His current research interest is information security, cybersecurity, and database management, and software engineering. He is a member of Information Assurance and Security Research Group (IASRG), Department of Computing Faculty of Engineering Universiti Teknologi Malaysia (UTM). He can be contacted at email: adamugaidam@gmail.com.



**Maheyzah Muhamad Siraj**     received the B.Eng. degree in Computer Engineering from Universiti Teknologi Malaysia (UTM), Malaysia in 2000 and the MEngSc degree in Computer and communication engineering from Queensland University of Technology (QUT), Australia, in 2003 and Ph.D. in Computer Science from Universiti Teknologi Malaysia (UTM), Malaysia in 2012. She is an active member of the Information Assurance and Security Research Group (IASRG), IEEE, and IACSIT. Currently, she is the Coordinator for the M.Sc. of Information Security program. Her major research interests revolve around Information Security and Assurance including Intrusion Detection, Alert Correlation, and Analysis, Intrusion Response and Prevention, Network/Digital Forensic. She can be contacted at email: maheyzah@utm.my.



**Siti Hajar Othman**     is a senior lecturer at the school of computing, faculty of engineering, university Teknologi Malaysia (UTM). She has been working in UTM since the year 2000 until now, she received her Ph.D. at the University of Wollongong, Australia in 2012, master of science computer science - real-time software engineering at universiti teknologi Malaysia, Malaysia in 2002 and bachelor of science computer science - majoring in computer system at universiti teknologi Malaysia, Malaysia in 2000. Her research interests are in Security Management–IT Security Audit, IT Disaster Recovery, Information Security, Cryptocurrency, Cybersecurity, Disaster Management, Computer Forensic, Knowledge Retrieval, and Conceptual Modelling. She can be contacted at email: hajar@utm.my.