CYBER-ATTACKS AND DATA INTEGRITY CONCERNS CRIPPLE LARGE PARTS OF THE INTERNET ON BANKING

الهجمات الإلكترونية والمخاوف المتعلقة بنزاهة البيانات من الإنترنت بشأن الأعمال المصرفية

by

MANAL AL BLOUSHI

Dissertation submitted in fulfilment

of the requirements for the degree of

MSc PROJECT MANAGEMENT

at

The British University in Dubai

February 2020

Declaration

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

ABSTRACT

The use of the internet in the banking sector is increased day by day. Most of the activities now are done with the help of the internet. However, with the advancement of technologies, the banking sector goes to the next level e-banking platform. They implement several technologies to gain a huge customer base and competitive advantage. However, with technological advancements, the cyber-crime is also boosted. The banking sector faces the most cyber-attack and confronts a huge financial loss as well. This research is conducted in the banking sector of the UAE. The topic of this research is to know about the impact on data integrity and the cyber-attack on the financial sector. Therefore, the researcher set some objectives and research aim before starting the work. However, this research will focus on the typology of the cyber-attack and its impact on the scope of the e-banking platform. Apart from that, customers' behavioral change for the e-banking platform is also focused.

It is recommended that the banking sector should implement several tools and methods to secure the platform for the customers. However, the Government should take some steps and implement some regulations to cope up with these difficult situations. However, the latest technologies like machine learning, DBMS, cloud-based technology and BlockChain can help in this matter.

Abstract in Arabic

يزداد استخدام الإنترنت والخدمات الإلكترونية في جميع القطاعات على مستوى جميع الخدمات وبالأخص في القطاع المصرفي يومًا بعد يوم. تتم معظم الأنشطة الآن بمساعدة الإنترنت. ومع ذلك ، مع تقدم التقنيات ، ينتقل القطاع المصرفي إلى المستوى التالي من منصة الخدمات المصرفية الإلكترونية. يقومون بتنفيذ العديد من التقنيات لاكتساب قاعدة عملاء ضخمة وميزة تنافسية. ومع ذلك ، وكلما زاد التقدم التكنولوجي والحلول الذكية يتم أيضًا تعزيز الجريمة الإلكترونية. يواجه القطاع المصرفي أكبر عدد من الهجمات الإلكترونية ويتعرض لخسارة مالية ضخمة أيضًا. ولقد تم إجراء هذا البحث خصيصاً في القطاع المصرفي في دولة الإمارات العربية المتحدة و موضوع هذا البحث هو للوصول إلى معرفة مدى تأثير الهجمات على سلامة البيانات وما العلاقة بين الهجوم الإلكتروني والمعلومات السرية ونزاهتها على القطاع المالي. لذلك قام الباحث بوضع بعض الأهداف وغايات البحث قبل الشروع في العمل. ومع ذلك ، سيركز هذا البحث على تصنيف الهجوم الإلكتروني وتأثيره على نطاق منصة الخدمات المصرفية الإلكترونية. بصرف النظر عن ذلك ، يتم التركيز أيضًا على تغيير سلوك العملاء في منصة الخدمات المصرفية الإلكترونية.

لذا ، يوصى بضرورة قيام القطاع المصرفي بتنفيذ عدة أدوات وطرق لتأمين المنصة للعملاء وشراء أفضل الحلول لحماية البيانات وكسب ثقة العملاء. ومع ذلك ، يجب على الحكومة اتخاذ بعض الخطوات وتنفيذ بعض اللوائح للتعامل مع هذه المواقف الصعبة. ومع ذلك ، يمكن أن تساعد أحدث التقنيات مثل التعلم الآلي ونظام إدارة قواعد البيانات والتكنولوجيا المستندة إلى مجموعة النظراء و Block Chain في هذا الأمر.

Acknowledgement

Investigating on this research content is viewed as among probably the best insight. It furnishes me with the possibility to improve my insightful abilities and information. I might want to grow my genuine appreciation to every person that remained close by directing me while playing out the whole assignment. From the outset, it might want to thank my administrator for the help also, direction that has assisted with leading top to bottom exploration and effectively complete my careful examination.

I might likewise want to thank the workers and government authorities for giving me interminable scholastic help, aptitude care information, and bearings while directing my review all through the exploration. I'm appreciative to my teachers too who consistently guided also, upheld me to experience difficulties and challenges all through my exploration, without their understanding and trust on me this undertaking probably won't have been feasible to finish.

Table of Contents

Chapter 1: Introduction

1.1 Introduction

In this 21st century, technology becomes a key part of every business, especially the banking sector. The dependence on technological advancements is increased day by day; even banking sectors can do think their activities without the help of technologies. However, technology provides some major threats to these sectors. These issues have to be dealt with as external threats in a systematic way. It makes a great impact on the unintentional and intentional acts of the internal stakeholders. Data integrity and cyber-attack become vital and serious issues in the last few years to several companies who mainly do their activities online. The e-banking sectors confront a major threat to these issues. Therefore, these sectors have to focus on these problems. The data should be authentic and reliable throughout its lifecycle. On the contrary, a cyber -attack is another major issue. To support the recent trends, the banking sectors focus on their online presence and depend on the digital money. The financial, personal and electronic data and information are stored. Due to the help of technological advancements, the theft tactics also updated day by day. However, this cyber-attack not only makes some financial loss, but it will also be the reason for leaking some important information. The massive malware attack is faced by these sectors. From the report of the experts of Group-IB, 99% of cyber-attacks are made for money theft(Maurer, Levite &Perkovich, 2017). Therefore, some new tactics and strategies are utilized to get some confidential advantages.

The banking sectors now are exposed by a huge number of cyber-attacks which becomes a major threat to information security and privacy. They confront the cyber-attacks in their several activities like ATM machines, online transactions, net banking, and electronic cards and so on. According to Web sense Security Labs, it is stated that the banking sector confronts these types of issues four times more than any other industry. Though, several banks implement several latest technologies to mitigate these issues. However, these cyber-crimes breach all the privacy and security and make a huge loss to these banks.

In this research, me as the researcher have proposed the best methodologies and sets some objectives to get a better outcome. The literature review is also drawn to support the research. Both secondary and primary data is found. I have also conducted questionnaires, surveys to collect the primary data. Apart from that, a mixed methodology is chosen to get the best result. The research

report, does the quantitative analysis for the primary data and thematic analysis for secondary data. The final result is also executed. In the end, a discussion and recommendation are also illustrated to support the result. The whole research is conducted in a systematic way so that the best possible outcomes tis achieved and also the banking sectors are prevented from future risks.

1.2 Research background

In the February 2019 Bangladesh bank confronted one of the biggest cyber-crimes. The cyber-hackers was managed to transfer $101 million from this bank with the help of hacking. It is not only an example. Many banks over the globe face this type of issue. As per the report of PWC's Global Economic survey, it is stated that cybercrime becomes the second most crime and in the last two years, 54% of organizations have confronted this issue. Tesco Bank of the UK also faces this same issue and the cybercriminals stole £2.5 million. For this reason, 9000 customers face a difficult situation. However, this cybercrime is increased day by day and it boosts to 12% compared to the last year.

Kaspersky Lab stated that UAE becomes the key and prime target of cybercriminals as the banks of UAE have faced most of the cyber-attacks in the last few years from 2016. Mainly UAE faces some malware attacks. In recent year, malware is detected by which hackers can control the ATMs of the banks. In 2016, cyber security was also breached named as "Operation Ghoul." Moreover, 68,000 customers suffered from the cyber-attack of Adwind Malware. Therefore, these banks need to look after data integrity. They should implement several latest technologies and methods to secure the online transactions made in the e-banking platform. It will help to get a profit, as well as the banks, will be able to build the trust of the customers. Therefore, this research will be helpful for these banks to know about the needed technologies to secure their e-banking platform.

According to a report published by (Alwan, 2018) there is bound to be 24 billion devices connected to the internet globally within mid of 2020. As this is good for digitization process, it also means that threat will be the strongest in case of cyber-attacks. According to a study (Hepinstall, 2019) UAE has experienced 1.1 million malware and phishing attempts between January and March 2019. Reports also indicate that the entire Middle Eastern region is already facing 3.16 million attacks in crypto currency and 5.83 million in phishing after March 2019, out

of which the banking sector is targeted the most. Security experts like (Guéraiche, 2019) say that cyber security in future would amount up to USD 66.5 million by the year 2025.

1.3 Problem Statement

Cybercrime becomes an emerging threat day by day as organizations now do most of their activities on the internet. The utilization of several latest technologies and the internet boosts the risk of these cyber-crimes and the banking sector losses data integrity. The topic is about the concern on cyber-crime data integrity to the e-banking. As the threats of cybercrimes like computer viruses, theft, hacking, phishing is raised, therefore, the research is needed to explore.

Cybercrime although an important issue, UAE specifically lacks in the knowledge and expertise when compared with the rest of the world. Cyber security in the UAE is still at its earliest stage and educational institutions must educate the youth and encourage to promote their cyber security skills. The problem currently that bank faces it the employees face difficulty in facing certain issues as they do not know how to handle them due to lack of skill and knowledge. As mentioned earlier in the research background, the amount of cyber threats that UAE is likely to face in crypto currency and e-banking cannot measure the existing security that UAE has and thus, it is pertinent that skill level is increased to a great extent to combat these threats. Reports say that Saudi Arabia has taken stricter measures than UAE, by imposing legislation on cyber security through government agencies. The nation also wishes to invest a good amount in cyber security in the future and increase awareness among its people.

However, with the help of technological advancements, the banking sectors can gain a huge number of customers. However, there is also a risk for the customers as well as the banking sectors to be in between of theft. Therefore, customers feel insecure to choose these e-banking services often. Therefore, it is very much needed to execute and demonstrate the core activities of these banking sectors. In this research, the researcher gives a focus on the impact of this cyber-crime and tools needed for data-integrity.

1.4 Aims and Objectives

Research aim: The aim of this research is to determine the impact of cyber-crime and data integrity on the e-banking platform and needed concern about these issues.

Research objectives: Now, the research report has set some objectives based on the aim as it will help to find the actual results and the major decisions that is to be taken from several aspects. The research objectives are as follows:

1. To identify the effects of data integrity and cyber-crime on the e-banking scope.

2. To reveal the impact of information technologies on the performance and activities of the financial sector.

3. To recommend the tools and methods that can be used for cyber-security and data integrity.

Research hypothesis

H0: Cyber-security and data integrity are not large parts of the internet on banking

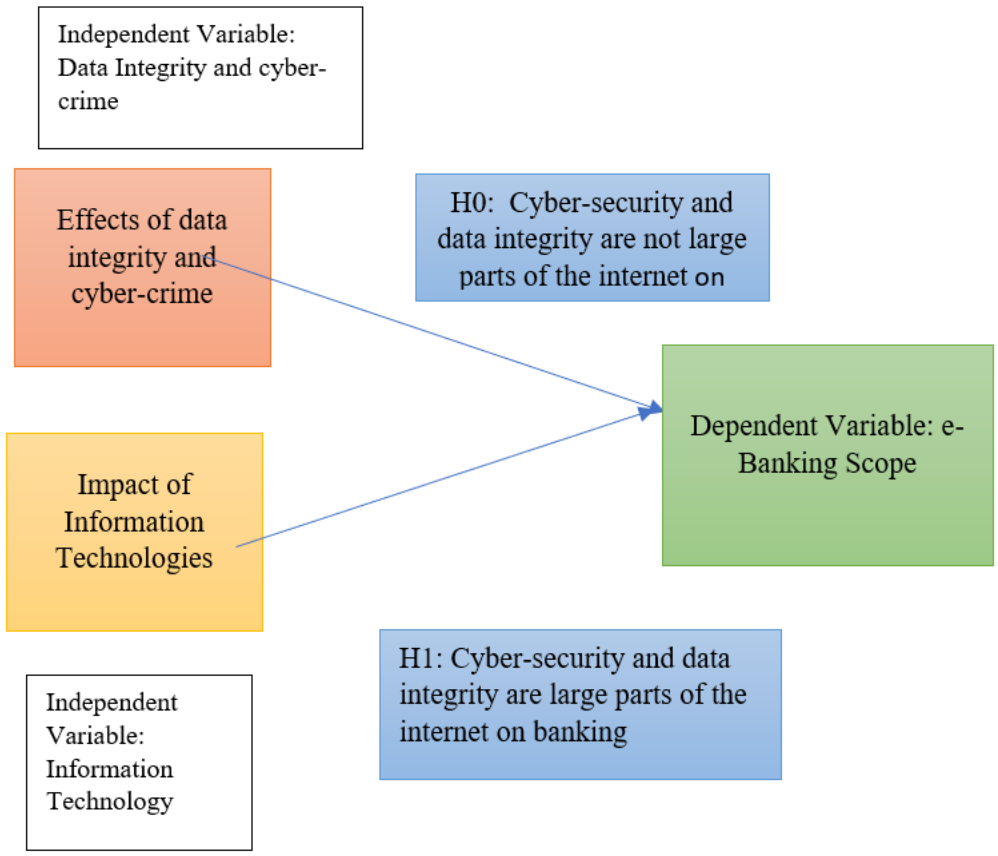
H1: Cyber-security and data integrity are large parts of the internet on banking

1.5 Limitation and future scope

In the meantime of the project, me as the researcher faces some issues and limitations. The first problem is finance. Due to the lack of a finance, the research may not be able to do several parts of the project at the right time. As a result, the project takes some extra time to complete. Apart from that, duringthe survey, many participants may not answer few questions and can leave the paper blank or give a confusing answer. Many of the participants also do not know the answers correctly. For this reason, the research report faces some issues at the time of data analysis. The actual results cannot be executed for this reason. These are the limitations of this project which makes some major barriers in front of the researcher to conduct the project smoothly.

However, there are several scopes of this research and it can be helpful in several aspects. Future researchers can take help from this research. Along with that, not only the e-banking sectors of the UAE but also the banking sectors all over the world can gain an in-depth knowledge of the threats of cyber-crime and tools required for data integrity. They can choose the best method to secure their online platform and customers' data from cyber-crime.Overall this project will identify the gaps that exist in the UAE market and will help future researchers with what they need to focus on.

Conceptual framework



Cybercrime is a significant issue, UAE explicitly needs the information and mastery when contrasted and the remainder of the world. Digital security in the UAE is still at its soonest stage and instructive foundations must teach the young and urge to advance their digital security aptitudes. The issue as of now that bank faces it the representatives face trouble in confronting certain issues as they don't have a clue how to deal with them because of absence of aptitude and information(Alwan, 2018). As referenced before in the exploration foundation, the measure of digital dangers that UAE is probably going to look in cryptographic money and e-banking can't quantify the current security that UAE has and subsequently, it is relevant that aptitude level is expanded generally to battle these dangers.They can identify the problems associated with these projects previously and take some important information regarding this topic(Guéraiche, 2019).

Chapter 2: Literature Review

2.1 Introduction

The literature review is one of the important parts in research by which the researcher can recognize the specific area of the research where he needs in-depth analysis. Analyzing this part, the researcher can know more about the topic and it supports the data collected by the analyst in the meantime of research.

Data integrity is a vital thing that should be maintained by all the banking sectors. Data integrity helps to store the electronic data of all financial transactions and information of the customers. Due to technological advancements, the e-banking becomes an emerging sector. However, the threats of the cyber-crime are also boosted. For this reason, to secure the information from the cyber-crime, the banking sectors should concern more about the data integrity. They have to utilize some latest tools by which they can ensure data integrity and mitigate the issues of cyber-attack.

In this chapter, first of all, several definitions associated with this topic are described. After that, some impact of this data integrity and cyber-attack on the banking industry are also illustrated. Apart from that, the effect of the adoption of several information technologies in the e-banking sector is also demonstrated. At last, the tools needed to be utilized by all banking sectors to ensure the security of the information and transactions.

2.2 Cyber-risks and types of cyber-risks

According to Healey et al. (2018), Cyber risk is termed as an operational risk which can be the reason for the loss of technology sets and information and affect the availability, confidentiality, and integrity of the electronic data. Cyber risk can make a huge impact on the part of a third party or direct third party. Cyber risk is dissimilar with the cyber-attacks. Natural disasters and software updates can be explained as cyber risks.

However, cyber-attacks can make a serious effect on the banking sectors in three ways: Integrity, confidentiality, and availability. Confidentiality is defined as data breaches by which the information of the customers and other important data is disclosed to the hackers or any other third parties(Ali et al., 2016). Integrity means the misuse of the technologies or defined as a fraud. On the contrary, availability problems can cause any business disruption. These three aspects can

make a direct impact on the e-banking sector. These issues make hinder the operational activities of online banking and as a result revenue loss will have occurred. These issues in a bank can lessen the brand image and boost the litigation cost. Therefore, the customers can not trust the e-banking.The security implication of cyber threat on the UAE is a serious one. The digital transformation step taken by the GCC members is to advance in technology and be the leading in the world, with respect to digital technology. But this has also encouraged phishing, malware, hacking leading to security threats of confidential information. According to a report by Erricson(El-Guindy, 2014), almost 20% of the organisations in the UAE regions are connected to an IoT device. By 2022, the report suggests that all household appliances too will be connected such as coffee machines, washing machines, and others. However, in times of cyber-attacks all these can use these devices to weaponise and attack the public and people in important positions.

As per researcher (Volodina, Zaluzhny, & Tarasova, 2019) camera and microphone enabled devices are more likely to be used as through them hackers can gain access to private lives of the individual, gain access to their bank accounts, insurance and others. On a political level, this is alarming, as it can lead to the using military codes and information for the wrong purpose. Various accounts can be hacked and the finance can be used for the wrong purpose. Serious threats have the power to boycott the entire political and financial structure.

2.3 Effect of cyber-attack and data integrity on the E-Banking scope

As per the study of Goel (2016), data integrity is termed as an assurance and maintenance of the consistency and accuracy of the data. This is an effective part of the information to sustain the interaction among storage, transfer, and usage. With the help of data integrity, the bank can make an interaction between the bank and the computer which can prevent any technical issues for modifying the data. Generally, the banking sector keeps all records in their databases and they also deliver them if the customers make any transactions. In that case, the bank utilizes several systems from the protection to the whole business process. When the customers' logs in their account on their website, they can check all data on their device(Arcuri, Brogi&Gandolfi, 2017). Therefore, it is very much important to maintain the accuracy of the data so the customers can easily access their accounts. In order to secure this data, the banking platforms have to utilize several technologies and tools to prevent their system from any type of threat. Due to these reasons, data integrity plays a significant role in the banking sector.

There are several statistical reports which provide some information about the effects of data integrity, security breaches and cyber-crime on the banking sector and its future scope. As per the report of Gartner Inc., it is stated that from 2004 to 2005, the customers face a financial loss of 929 million dollars for phishing. According toChevers (2019), the statistical report showed that 9 of the 10 cyber-crimes are associated with the E-banking sector. In the year of 2008, 7.5% of US adults lose their money for data breaches and financial fraud. This finance loss makes some adverse effects on the behaviors of the consumers. When the financial transaction will be secured and the personal data of the consumers are encrypted, the customers can trust the banking sectors. The TAN/PIN system can be used to secure online transactions. However, a report stated that this is not enough method to mitigate these issues. Bitcoin, the IT national association of Germany stated 4100 cases of the cyber-crime which was the result in a financial result of ten million. The loss amount for these cases is £3,700. Gartner Inc. conducted a survey in 2008 among 5,000 US adults to measure the effect of this theft and online fraud. It was seen that 36% of the interviewees claimed that they have faced Payment card fraud. Apart from that, they also faced New-account fraud by which the customers faced the loss of their personal information. The new account fraud was mainly associated with synthetic identities and as a result, most of the cases are unreported. Therefore, the people who faced such problems changed their e-banking and payment behavior.

According toTyagi(2019), the victims of 2008 changed their bank as well for security concerns. Many victims did not even do any bill payment and online money transfer through e-banking. Therefore, the banking sectors faced a huge loss for these cases of fraud and it is needed to utilize more secure technology to build the trust again to the customers.

(Figure: Geographical distribution of Spam URLs)

(Source: Orji, 2019**)**

From the report, it is known that Romania is the home of phishing web sites. 5% of the phishing web sites are from this country. However, 46% of phishing websites come from EMEA. Romania ranked tenth in Europe, the Middle East and Africa (EMEA) and this stat clearly showed that it is the origin of the phishing website. It is seen that in 2018, 12% of cyber-crime is increased than the past year which makes a huge negative impact on the banking sector.

According to the risk report of IBM X-Force, Romania got tenth ranking in generating spam URLs, seconds in generating phishing links and get the third position in the landing-page top. However, it is seen that China becomes first in generating the Spam URLs which makes a major threat to the banking sector worldwide.

2.4 Impacts of the adoption of information technology on the performance of the banking and financial industry

According toLawal, Lawal&Akanbi (2018), the adoption of information technology in the banking sector boosts the effectiveness of the performance and helps to gain more customers. The computer automation in the banking sector worldwide is developed in this 21st century and most of the banks start their e-banking platform with the help of information technology. From the study of Sabherwal&Jeyaraj(2015), it is seen that there are several variations in the technology and automate devices in the new banks compared to the old banks. It further demonstrated that information technology becomes the backbone of the financial sector in the context of an online presence. The customers can experience a hassle-free banking service and sophistication with the help of information technology. Therefore, to secure the transactions and attract more customers, these banks spend a huge budget on information technology. The on-line system helps in internet banking and facilitates the banks to launch their own websites. Apart from that, the customers can easily transfer their funds to another account from anywhere and they can get some flexibility to operate and control their account from any branch. Today, cashless transactions are only possible for this information technology.

The development of information technology provides some competitive advantage and mitigate the challenges come from the customers. The revolution and adaptation of information technology change the whole business model of the banking sectors and allows them to create value creation chains (Al-Azzam, 2015). They can offer their customers more reliable and authentic customer care services with the help of information technology. However, the utilization

of information technology lessens the operational cost and processing cost. The switching and search costs of the customers are also reduced. With the help of this IT, the bank can promote its products and services easily, even in the remote area. Therefore, it is concluded that, with the help of information technology, the performance and effectiveness of all financial sectors are evolved and enriched.

2.5 Tools and technology used for identifying cyber-attack and data integrity in the E-banking sector

As per the study of Avgerou&Walsham (2017), bank security plays a vital role in banking services as there is a high chance of cyber-attack. Without bank security, the consumers are not willing to utilize the internet for conducting financial transactions or checking their financial data and information online. Security threats consist of confidential information theft and invasion of individuals. To overcome these threats and cyber-attack, the banking sector provides various processes like identification, encryption and firewalls mechanism to give a better level of security. In the case of an online bank, the identification takes the term of Uniform Resource Locator (URL) or a known Internet address when the clients are identified by their password and ID for assuring the authorized users can get their accounts. Along with that, all messages between online banks and customers can be encrypted and therefore anyone cannot check those messages. Secure Socket Layer (SSL) is the most valuable encryption protocol. On the other hand, the firewall mechanism is also needed to secure all resources of the bank network from the users from another network. SSL acts as a set of devices to encrypt, deny and permit the computer traffic among several security domains. By differentiating filtering routers, digital certification, firewalls, encryption, the multi-layered security assures that the account information of a customer is secured from unauthorized access(Vaismoradi et al., 2016). This makes the banking services safe and secure by preventing any attack and maintain the data integrity by keeping the data consistent and accurate.

Sabherwal&Jeyaraj (2015)stated that, the best method of protecting online baking is chip card utilizing home Banking Computer Interface (HBCI). The method provides the assurance of high-security standards. However, the user must have their own software for the chip card reading device.Apart from that, many banking sectors try to improve their safety processes by replacing their TAN lists. TAN means Transaction Authentication Number for the E-Banking Services Consumers' Interests. This is defined as second layer security for single password authentication.

With the help of this method, the customers get a transaction related TAN via SMS on their mobile after signing up with that bank. As the cyber-criminal can unable to overhear the PC and mobile phone network of the customers, the TAN process helps to secure the banking service.According to the study of Sardina, Olkhovskii& Lowell (2018), another essential method of protecting banking service and prevent cybercrime is the TAN generator. This method is also called as Smart TAN and TAN is generated by this device for a short time period. This obstructs the misuse and interception of the user data. By implementing this method, the customers open their transaction data into a card reader which makes a TAN in connection with the bank card. After that, the bank computes that TAN and then enable their transaction if match. If it is not matched, then the transaction is not proceeding. Therefore, anyone can not track the customers' data. On the other hand, a new tool named electronic Identity (eID) card appears to help in the user authentication. The government and private-public partnership (PPP) only manage these cards(Ghernaouti-Helie, 2016). Another most useful process to protect E-banking services is Vulnerability Assessment and Penetration Testing. In this perspective, every bank has to assure the security information which is conducted via system vulnerabilities assessment and penetration testing strategy.This strategy has to be conducted by the well-developed security experts of the bank. Generally, penetration testing is termed as a security testing by which the real world attacks for identifying the methods of avoiding the security features of the network or system. Therefore, all banking services must take these penetration tests periodically by which they get all vulnerabilities in their network systems and equipment and many more.With the help of these technologies and tools, the banking sectors can keep their bank secrecy and protect the customer data from the cyber-attacks. In that way, they are able to gain a huge amount of customers and retain the existing customers which help in growing their business in a systematic way.

2.6 e-Banking platform security as well as protection of the consumer interests

According to Knowles et al. (2015), it is stated that high security of e-banking sectors acts as a protection of interest in financial institutions and protection of the electronic services. For this purpose, it is vital for the managers of banking services to implement the communication and information technologies to operate their services and secure the confidentiality of information. As per the consumer interest protection, the legal regulations by the assurance of security of banking services are assuring protection of consumer information, security against any unauthorized access and protection against any threats or cyber-attacks. Some laws are introduced

by the government and these are Law no. 455/2001, Law no. 677/2001, Law no. 365/2002 and so on. By using these laws, bank services can protect the data and make any transaction smoother. As per the study of Knowles et al. (2015), it has been concluded that authorization is obtained to mitigate any issue of payment method. The authorization has to focus on the banking services and prevent their data from any type of threat. They have to be aware of restoring the information managed by their system due to unforeseen events or natural disasters. In that way, their all functions and operations can be well-operated and they become able to keep safe and secure all the data and information of the customers which make their service more stable and effective.

2.7 Summary

In this chapter, the researcher has demonstrated the key definitions of the terms associated with this topic. At first, the cyber-crimes have been defining and its types have been briefly explained. After that, the actual impacts of these cyber-crimes on the e-banking platform have been demonstrated. The researcher has conceded the role of information technology in boosting the effectiveness and performance of the banking sectors. Apart from that, the tools and methods for ensuring the data integrity and cyber-security have been illustrated. At last, the impact of these issues on the behavior of consumers has been discussed. Moreover, this chapter has facilitated the researcher to get a strong knowledge about this research and these data can be utilized as secondary data which helps him in further data analysis.

Chapter 3: Methodology

3.1 Introduction

The methodology can be termed as an effective and essential approach that is applied to accumulate proper data as well as information and analyze them in an effective way. In this part of the research project, the prime concern is to identify and discuss several research methods and their significance in gathering essential information regarding the research topic. Therefore, the methodology is an uttermost important factor for the success of this project. Along with that, this section is vital for the researcher to pick up the best accurate techniques and strategies in which all objectives of this research can be met in an efficient manner. In this section, the research chooses the proper and reliable methodology to know about the impact of cyber-attacks and data integrity on the Dubai E-banking scope. In that perspective, an appropriate research method is chosen and a reliable research design is conducted by the researcher. By taking the correct path, the researcher can be able to make any decision for conducting this research.

The methodology section begins with analyzing research philosophy and then continuing with the research methods and research approach which can be very helpful to gather accurate information. At the same time, research design, timeline, data collection, and analytical method and tool are also elaborated here. Furthermore, ethical consideration, limitation, and reflection of this research are also illustrated in the end part of the methodology section.

3.2 Research Philosophy

This research discusses implementing various methodological approaches and strategies in order to investigate several dimensions of cyber-attacks and data integrity. Saunders's research onion can be picked up to evaluate the stages which should be involved in the conduction of the project. While viewing this from the outside, every layer of this onion highlight more clear steps that must be required to make the project.

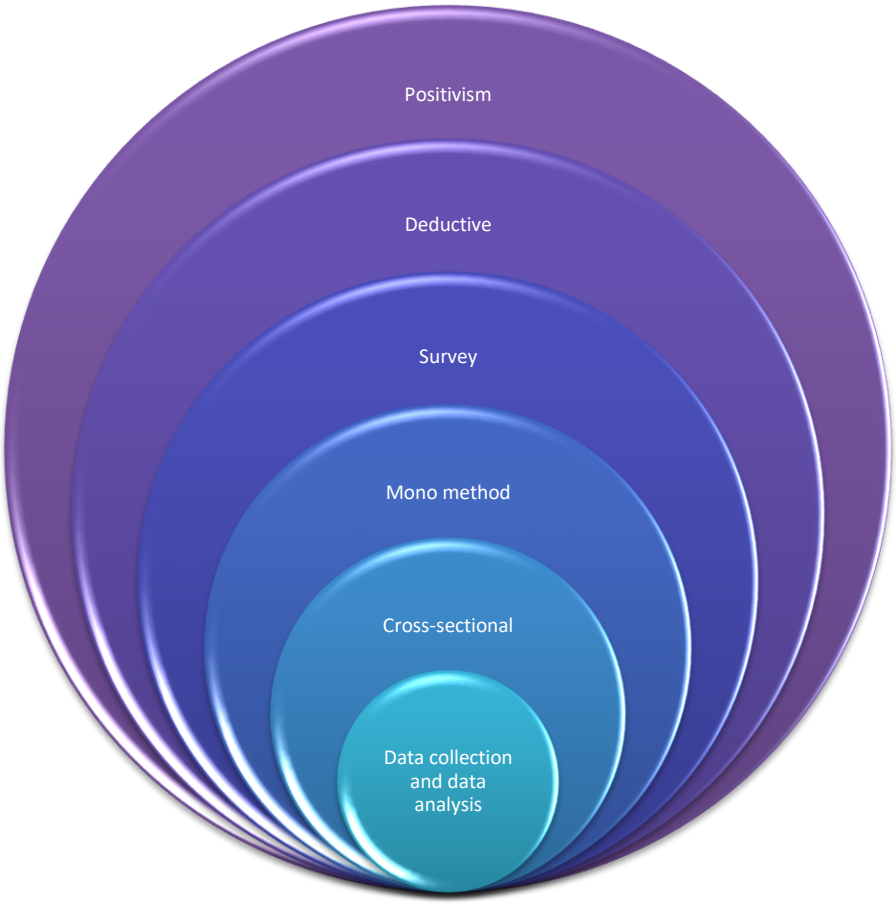


Figure: Research Onion Framework

(Source: Maximov, Sokolovsky&Gavrilov, 2017)

The research onion consists of six layers which are philosophical stances, strategies, choices, approaches, time horizons and procedures. A philosophical stance is the first layer which helps in determining the path of gathering as well as analyzing all information to prepare fine research. This layer involves several philosophical instances like objectivism, realism, interpret-ivism, constructivism, positivism, and pragmatism. In this project, positivism is chosen as a research philosophy by which the researcher gets the appropriate data measuring the proper knowledge of the cyber-attack and data integrity for the elimination of high risk of Dubaibanking sector. Apart from that, the research also designs the philosophy which strengthens the effectiveness of this project.

3.3 Research approach

This research approach must be selected based on the prime nature of the project as well as the project focus. The research approach mainly highlights a detailed image of data analysis and data collection methods. On the basis of facing problems in the end time of the project and during the conduction of the research analysis method, the report is chosen on the best and suitable research approach. The research approach is mainly separated into two parts and these are deductive and inductive. The deductive approach is concerned with the hypothesis from the main theories and the inductive approach derives the nature of the research. Along with that, the inductive approach begins with appropriate observation and then continuing with making a proper outcome. An inductive approach is very helpful to discuss the best direction of enriching the model and theories whereas a deductive approach helps to the validity of these models.

To conduct this project, the deductive approach is implemented which is to utilize and scan all the theories as well as the work of several researchers for identifying proper answer as per the research question and the aims and objectives of the report. This can be an effective approach because this allows the passing essential amount of data for getting an efficient conclusion. Moreover, the opinions of various experts in the field can also be taken into consideration.

3.4 Research design

Research design is considered as a plan of chosen methods and tools which is helpful for the researcher to meet all significant factors regarding this project in a systematic way. A proper research design helps in strengthening the efficiency of the project. In that respective, a fine research design with some questionnaires is adopted along with the opinions and reports conducted by various economists and researchers across the globe. This helps in the impact of cyber-attacks and data integrity on the E-banking scope.

3.5 Research method

The research method is also of utmost important in making a project. This approach terms as a process to accumulate appropriate information as per the research aim. The research method is categorized into two sections and these are qualitative research methods and quantitative research methods. With the help of a quantitative research method, this research will be able to investigate the research topic systematically(Sajid, Abbas &Saleem, 2016). After gathering

quantitative data, there will be a statistical, computational and mathematical process in order to analyze those collected data. This means that several information can be found outby making online surveys method, questionnaires among people or samples. After analyzing these data, this report has to give a proper result in the numerical forms. Along with that, the quantitative research method involves content analysis, focus groups. Apart from that, the qualitative research method is also helpful for the research report to determine the real behavior of people which is how they think, what they think and why they think in these terms.

In this project, the quantitative research method and qualitative research method are picked up as the measurement of this process is very easy and a proper result is obtained about the impacts of cyber-attack and data integrity in the banking sector. Moreover, the quantitativemethod consists of numerical analysis. Therefore, this method is suitable for the report to create a prediction regarding the future incidents.

3.6 Timeline

For this report the quarter 4 of the 2017 year to quarter 3 of the 2010 year is taken. After making a literature review, data collection, data analysis, risk identification, the project is written in quarter 2 and quarter 3 of the 2020 year and then submitted.

3.7 Data collecting tool and technique

Data collection is defined as a method of gathering all data and information from reliable sources. This approach helps in understanding the research objectives and mitigating any problem faced during the research and provides a proper conclusion as well. The data collection method is separated into two types and these are the primary data collection method and secondary data collection method. Primary data collection methods help the researcher to gather those data that are new as well as not been gathered by anyone before. The primary data collected by conducting an interview, survey, questionnaire. On the other hand, the secondary data collection method helps the researcher to those data that are already collected by various people and organisations. Secondary data is collected from books, journals, newspapers, magazines.

To conduct this project, both primary and secondary data collection methods are used for the collection of huge data regarding this project. In this research, the primary data is collected by making a survey method and questionnaire which helps to get proper data from the CEO and

managers of the Dubai banking sector. Besides that, the secondary data is collected through newspapers, journals, and the internet. In this case, primary data can be first-hand data of the research topic that is stored and primary data of someone is collected for gathering the secondary data. Primary data involves raw data whereas the secondary data are analyzed data(Gupta, Agrawal & Yamaguchi, 2016).

As per the questionnaires-survey method, some questionnaires that include many demographic and close-ended questions have been made. The questions which can be provided to the participants are the same. Each survey is made within 15 minutes. A survey paper is provided where the participants fill up all answers regarding the questions. In this concept, each question has some option which is needed to be chosen by the participants. The survey process conducted on the one-to-one system between the CEO or manager and the researcher.

As a result, the research report is able to gather all reliable data through primary data collection methods. Along with that, primary data also makes this project effective as these data are authentic and unique. Moreover, the secondary data is collected by the secondary data collection method which boosts the accuracy level of this project. Thus, the research report adopts both data collection methods and tools for the completion of this research.

3.8 Data analytical tool and technique

After choosing all reliable and consistent data by data collection tools, it is important to analyze those data and information in an effective and efficient way. In that case, the data analysis tool and technique is also the most essential phenomenon of this research study as this helps in making the research successful. This can be an effective procedure which utilizes several statistical tools for the explanation, interpretation as well as execution of the chosen data. In order to analyze these data, two different analytical methods are available and they are qualitative methods and quantitative methods. The whole analysis is finished by the qualitative method and qualitative in a descriptive way. On the other hand, the numerical information and data are analyzed using the quantitative method. Both methods support in finding the rationale of the project too. To make this research, the quantitative data analysis method is picked up because a proper result is obtained about the impacts of cyber-attack and data integrity in the banking sector. Along with that, a thematic analysis is also conducted to make a comparison between the discussion of the literature

review and findings. This can be effective to enhance the efficiency of the dissertation(Maglaras et al., 2018).

For the conduction of data analysis, content analysis is also selected. On the basis of the survey research method, content analysis can be termed as a research method that is used to the responses provided to the open-ended questions for coding their answer into some categories that communicate themselves for further quantitative statistical analysis. This method also helps to analyze the appropriate meaning of the information and data. Moreover, this process is very cheap and therefore the researcher selects this type of data analysis.

3.9. Research sampling

The sampling method is another important approach to making the research effective. The sampling method is termed as an item, team, objects or people who engaged in the survey process or those who help to provide the primary data. In this research project, one needs to measure all characteristics and perspectives for making an appropriate conclusion or outcome for this research. In order to build the survey method, the engaged population can be required to be questioned on the basis of the topic and objectives of this project. Therefore, conducting a survey with the CEO and managers of the banking sector in Dubai is important. Moreover, the report is always carefully implemented keeping in mind the targeted population. The size of the sample is 100. In this survey method, a survey paper is provided to the participants and all have to fill up this paper by selecting one option. A survey method is used where all CEO and managers are comfortable to express their opinion about the effects of data integrity and cyber-attacks on the banking industry. By implementing the survey method, this research can be well-structured. This is very much helpful in accomplishing this research work.

3.10 Ethical consideration

While making a project, ethical consideration becomes a significant aspect which is needed to be maintained at all cost. Without operating the ethic norms, the research cannot be submitted within proper time. As the quantitative study is the prime focus on the bonding between the researcher and manager and CEO of the Dubai banking sector, the ethical terms are not neglected during the project. The main principles of this project are un-biasness, consent, confidentially and fairness. With the term survey method, the data collection along with data analysis is interpreted. This project maintains an openness principle. From the survey method, the information is kept

confidential.During the survey research, their names and identities cannot be revealed and the sensitive objects can be removed if it is important. Moreover, the research does not provide importance to this biasness while preparing the project. Thefairness and rationality is always maintained at the end time of the survey(Fielder et al., 2016). By taking the moral principle, the report gathers all primary data from the participants of the survey method. Rationally means a relationship between the researcher and the participants and this also explains the relationship of the researcher with own findings.When a question is asked, the researcher has no right to ask further questions. At the same time, the researcher cannot force the participants in the survey method to give their answers. Additionally, any components are not injurious to the human while conducting this research project.

3.11 Reflection

For the accomplishment of the project, positivism as a research philosophy was picked up to understand the main concept of this assignment. After that, the deductive research approach was chosen here. Then, as a research method, the quantitative method was utilized which helped to store and execute the numerical data rather than the non-numerical data. After choosing the research method, both primary and secondary data collection method was chosen for making this research project effective by accumulating accurate data. After the collection of data, it is vital to analyze them in a proper way. Therefore, quantitative data analysis was selected. As a sampling method, the survey and questionnaire methods were conducted among 100 CEOs and managers of the Dubai baking industry. In that way, this project was completed at the required time.

3.12 Limitation

Certain limitations comes with this research while conducting the survey method. In that perspective, insufficient and inadequate data is a major problem which the research has confronted. While making this research, accurate data is needed. Flawed data and information can be probable to hamper the final results of this project. Due to this reason, extra effort was put while mitigating all risks and errors from this research work. At the same time, it was also noticed that some people were unwilling to answer the questions of the survey method. Therefore, this project suffered from inadequate data. Moreover, the survey method was also affected in this project because some were not focusing on the concept of this research topic and some did not fill the whole survey paper.Furthermore, there is a huge chance of biasness as some participants cannot answer. This

hampered the research work, especially in the data analysis. Besides that, the survey is very time-consuming which another limitation for this project is. In additionally, the time of each survey is around 15 minutes that is also a huge limitation.

3.13 Summary

This study analyzed the analysis of various research approaches and methodological techniques utilized to make this research project. Understanding of those data collection tools and methodologies supports in identifying the problems faced during the research. Along with that, this research provides the researcher to comprise between correct and wrong decisions.

This study also explained a proper sampling technique as well as procedures that help in finding the targeted audience for the data collection procedures. Apart from that, ethical consideration was also attached in this chapter for maintaining all rules and regulations and ethical norms during the research work.

Chapter 4: Primary and Secondary Data

4.1 Introduction

In the research paper, the non-technical and technical aspects have been stated until now. However, the researcher needs to collect some primary data by which he can analyze the real-world scenario. Therefore, for giving a rigid decision, the researcher has to collect some reliable and authentic data by which he can know the situation in the banking sectors of the UAE.

To get the research data, this researcher conducts a questionnaire survey among the CEO and managers of the banking sectors of the UAE. In this survey, the participants come from several banks like Bank of Baroda, Arab bank, FGB bank, Emirates Bank, Abu Dhabi Islamic Bank, etc. Apart from that, secondary data is collected from several journals, books, websites, and articles. This chapter will give a clear view of the questions which are asked, the pattern of the survey and the way to do the survey. This survey consists of 15 questions from which two are for the identifications of the participants and remaining are asked to accomplish the research objectives.

Apart from that, in this chapter, the quantitative analysis of this primary data is executed and thematic analysis is conducted for evaluating the secondary data. At the end of this chapter, a discussion is attached as it will draw a clear image of the finding's rand results. This discussion part will describe the decisions taken up after the successful completion of this research.

4.2 Survey questions

The questions were formed through researching articles, journals and talking to people on cyber-attacks. Several research was also done on the internet to come up with such questions. One of the main goals of survey question was to come up with insights on the banks and what they think about cyber security. It also gives us a reason, why some banks in the UAE is reluctant to move ahead with cyber security, when they know that the crisis is crucial. Questions also help an engagement and communication process between the interviewed and the interviewer. In this case, the CEOs of various banks may or may not answer a particular question, but it is important that they do. Some survey quality tools from Survey Monkey (Johnson, 2019) has also been used to come with the right questions which would benefit the research project.

4.3 Secondary Resources

As mentioned in earlier chapters, several journals and opinions of economists and experts were taken to form secondary data on the research. Various resources and reports from security groups around the world and IT security industries have been taken. They are all verified data which has been used to authenticate the results that were found.

Chapter 5: Data Analysis

5.1 Survey output

1. For which bank are you serving?

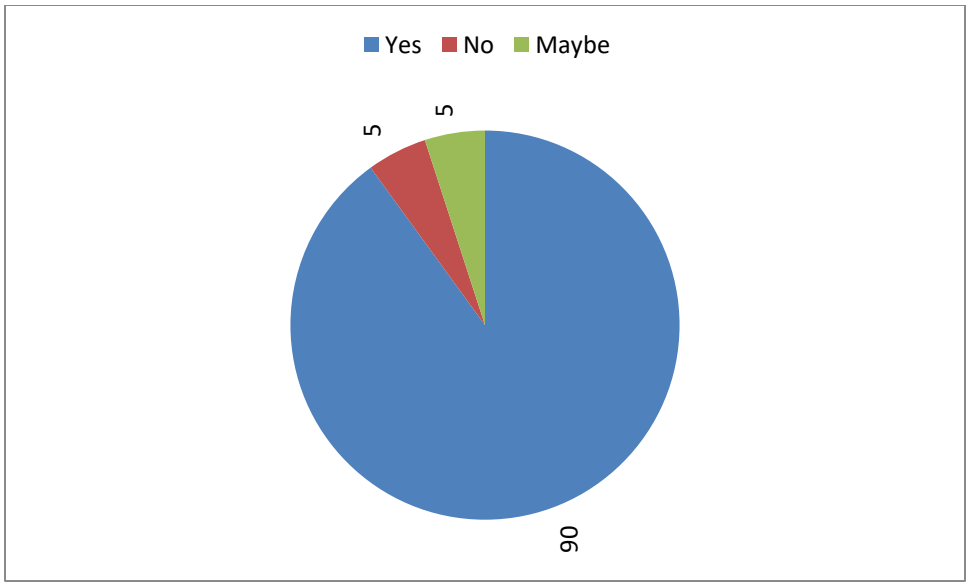
In order to conduct this dissertation and to understand the view of CEO and managers of the Dubai banking industry regarding the impact of data integrity and cyber-attack on their services, 100 CEOs and managers are selected for the survey method. They are working on several banks in Dubai such as Bank of Baroda, Commercial Bank of Dubai, Abu Dhabi Islamic Bank, Arab Bank, Emirates NBD, FGB Bank, and Others.

2. In which position do you work?

For conduction of the survey, 75 participants work at the position of Manager of those banks and 25 participants work at the position of CEO of those banks.

3. Do you think the internet is secure for conducting the financial transactions of the banking sector?

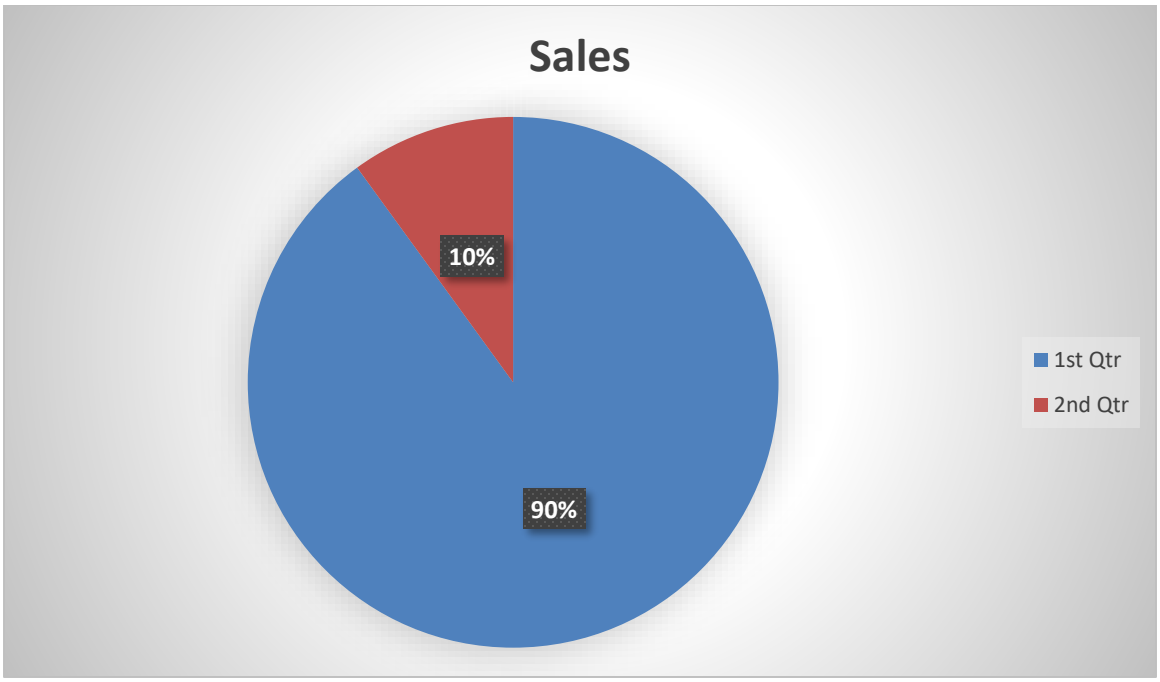
Variables	Percentage
Yes	5
No	85
Maybe	10



As per the above bar graph and chart, it has been seen that 90% of CEOs and managers go with the option Yes. Where 5% of CEO and managers told they don't think the internet is secure for conducting the financial transactions of the banking sector. Moreover, the rest of the 5% mentioned maybe their internet is secure for the transaction. This data was taken from several banks and the results are an average of all answers.

4. Does your bank face any cyber-attack?

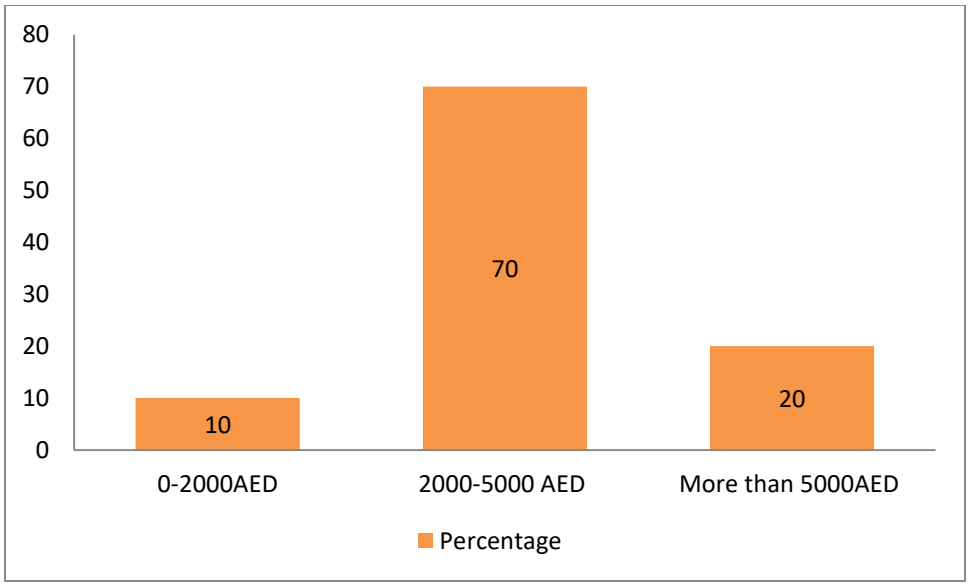
Variables	Percentage
Yes	10
No	90



In the present day, cyber-attack has been increased rapidly all over the world. During the survey, 90% of the managers and CEOs of the banking sectors said that they cannot confront any cyber-attack. On the other hand, 10% of them face a cyber-attack on their services.

5. How much financial loss did you face for the cyber-attack?

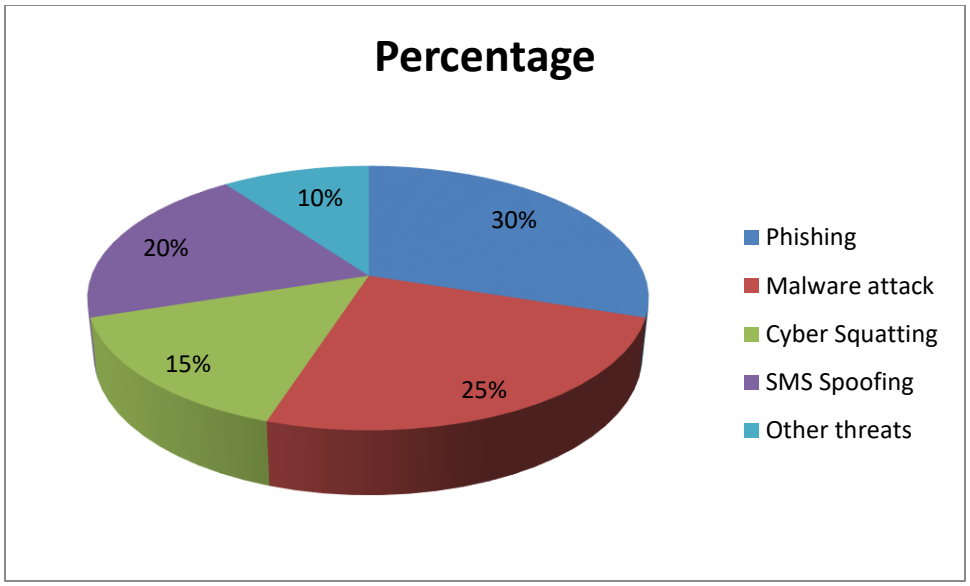
Variables	Percentage
0-2000AED	10
2000-5000 AED	70
More than 5000AED	20



Due to the cyber-attack, the bank service faces a huge financial loss just within 10% of the financial banks in the surveys that were taken. In that perspective, 10 of the managers and CEOs mentioned that they face 0-2000AED financial loss and 70% of them have confronted 2000-5000 AED. On the other hand, the rest of the 20 % face more than 5000AED.

6. What type of cyber-attack does your bank face?

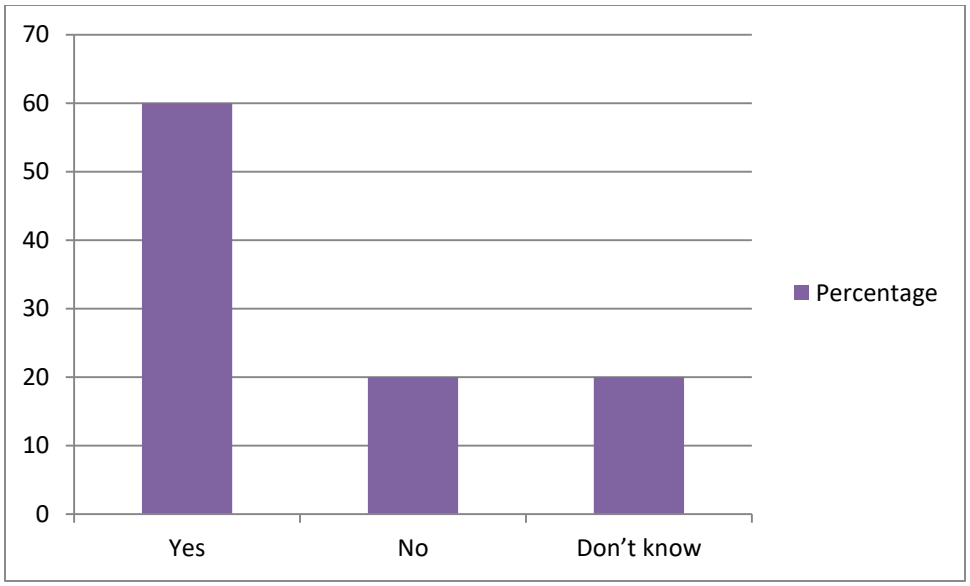
Variables	Percentage
Phishing	30
Malware attack	25
Cyber Squatting	15
SMS Spoofing	20
Other threats	10



Several kinds of cyber-attacks happened in the Dubai banking sector. Major Cybercrime threats are phishing, malware attack, cybersquatting, SMS spoofing, others. As per this question, CEOs and managers of Dubai told that 30% was of phishing that they faced and 25% of them were faced with the malware attacks. Along with that, 15% of them said that they faced cyber-squatting and 20% of them face SMS spoofing. On the other hand, the rest of the 10% faced other threats.

7. Do you think the customers change their online transaction behavior due to cyber-attack?

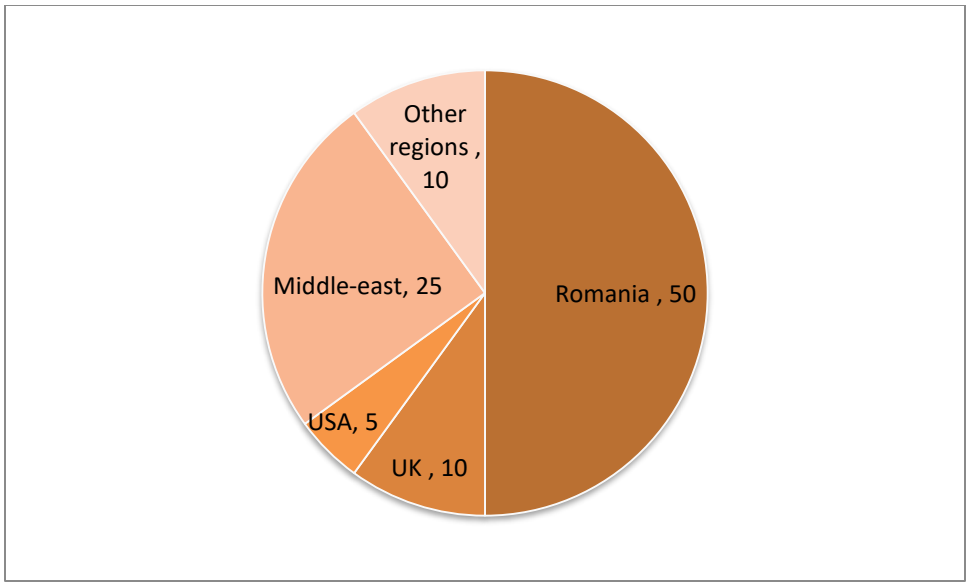
Variables	Percentage
No	60
Yes	20
Don't know	20



According to this question asked by the researcher, 60% of managers and CEOs of the banking industry said that the customers do not change their online transaction behavior for the cyber-attack. It is only that 20% of the customers were traditional in nature and preferred offline transactions. 20% of the consumers remained neutral.

8. What do you think that which region is responsible most for the cyber-attack?

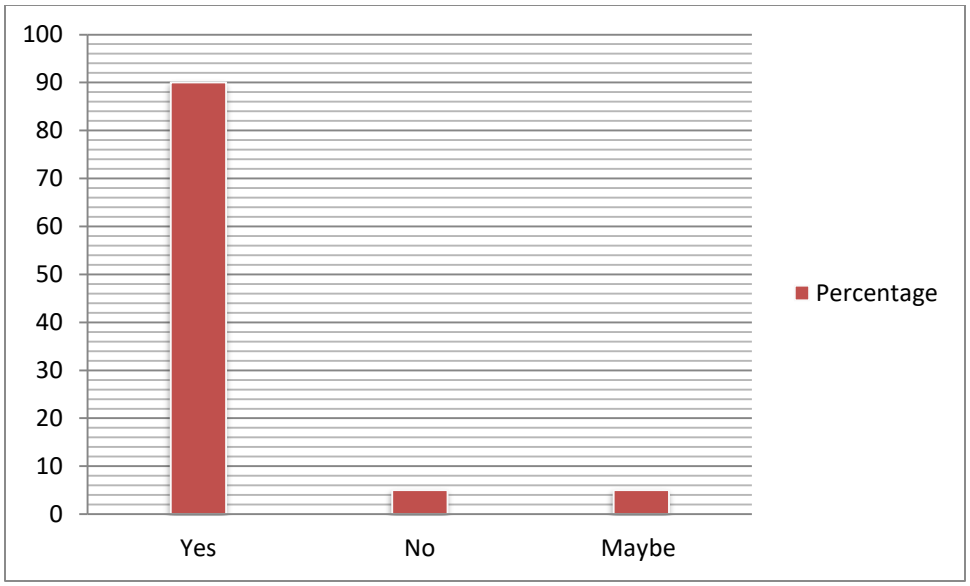
Variables	Percentage
Romania	50
UK	10
USA	5
Middle-east	25
Other regions	10



Due to the cyber-attack in the bank sector, several regions are responsible for this incident. Therefore, this question is asked to the manager and CEO of the Dubai banking industry to know their views regarding this occurrence. In that case, 50% of them go with the option 'Romania' and 10% of people think that the UK is responsible for the cyber-attack. On the other hand, 5% Of them said that the USA is responsible for cyber-attacks and 25% of people think that Middle-east is liable for this threat.

9. Do you think technological development is the main reason for increasing fraud-ness?

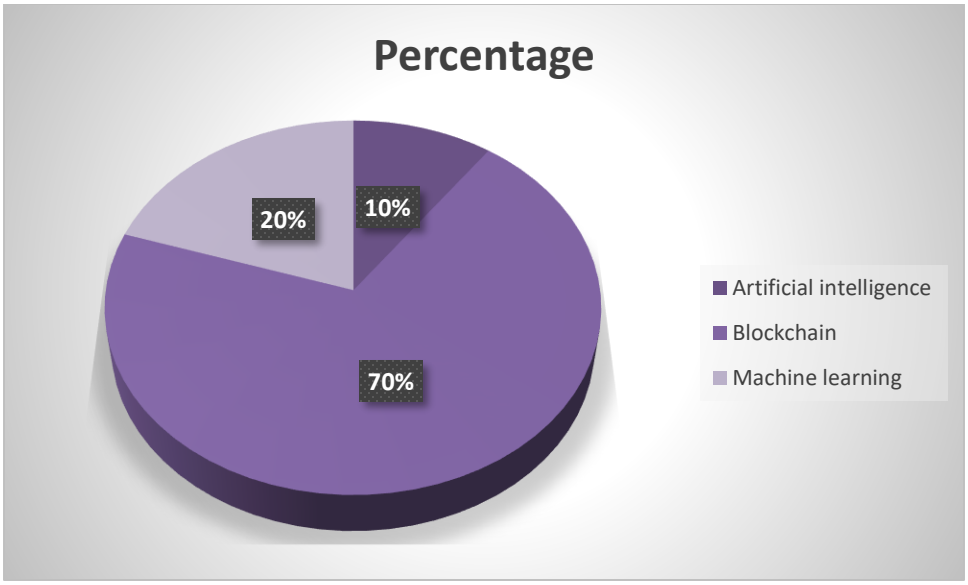
Variables	Percentage
Yes	90
No	5
Maybe	5



As per this question, 90% of managers and CEOs have been said that technological advancement is the main reason for the increment of fraud-ness. Whereas 5% of them don't think that technological growth causes the frauds.Along with that, the rest of the 5% of them has mentioned nothing in particular.

10. Which latest technology can make the online transaction safe and secure?

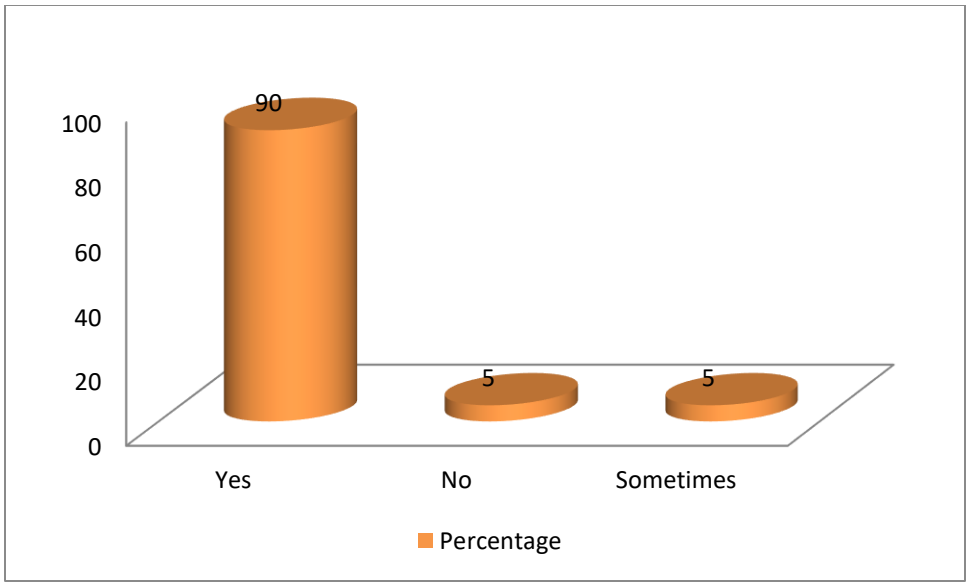
Variables	Percentage
Artificial intelligence	10
Block Chain	70
Machine learning	20



As per the above bar graph, it is concluded that 70% of CEOs and managers think that Block chain technology makes the online transaction safe. On the other hand, 10 of them said that artificial intelligence make a safe and secure transaction and the rest of 20% mentioned that machine learning is best for making a safe online transaction.

11. Do online customer service keeps proper records of the account transactions?

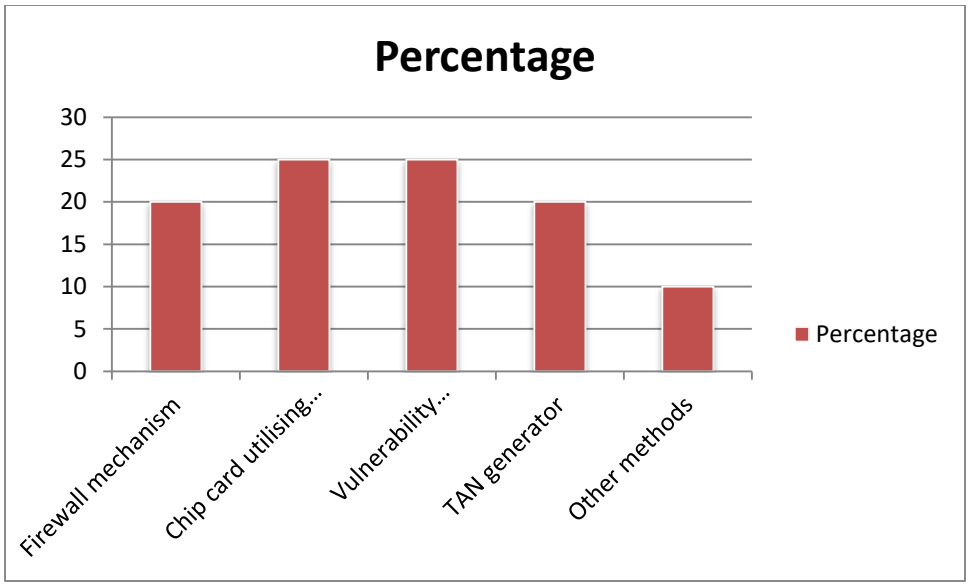
Variables	Percentage
Yes	90
No	5
Sometimes	5



According to this question, 90% of managers and CEOs of the banking industry said that their online customers' service keeps all records of the account transactions. Additionally, 5% of them never agree with this statement. At the same time, the rest of the 5% mentioned that their online services sometimes record all information on account statements.

12. Which tools do you implement for identifying the cyber-attack?

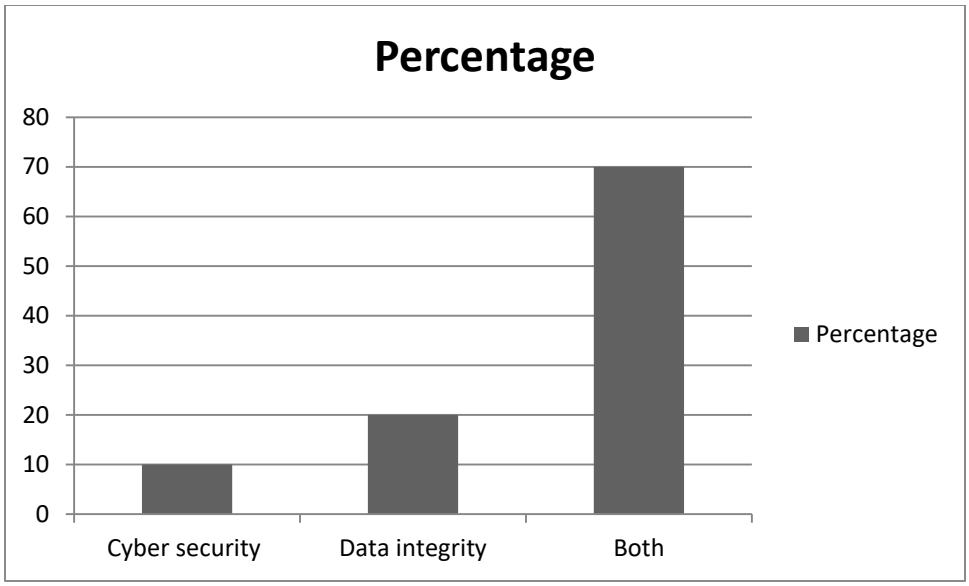
Variables	Percentage
Firewall mechanism	20
Chip card utilizing Home Banking Computer Interface (HBCI)	25
Vulnerability Assessment and Penetration Testing	25
TAN generator	20
Other methods	10



According to the above question, 20% of the participants have been said that the firewall mechanism is utilized for the identification of cyber-attacks. Apart from that, 25% of them have mentioned that they utilize chip cards utilizing Home Banking Computer Interface (HBCI) for identifying the cyber-attack and 25% of them said that they use Vulnerability assessment and penetration testing method. 20% of them utilize TAN generator and the rest of 10% use other methods and technologies to identify the cyber-attack.

13. How do you secure online customer service?

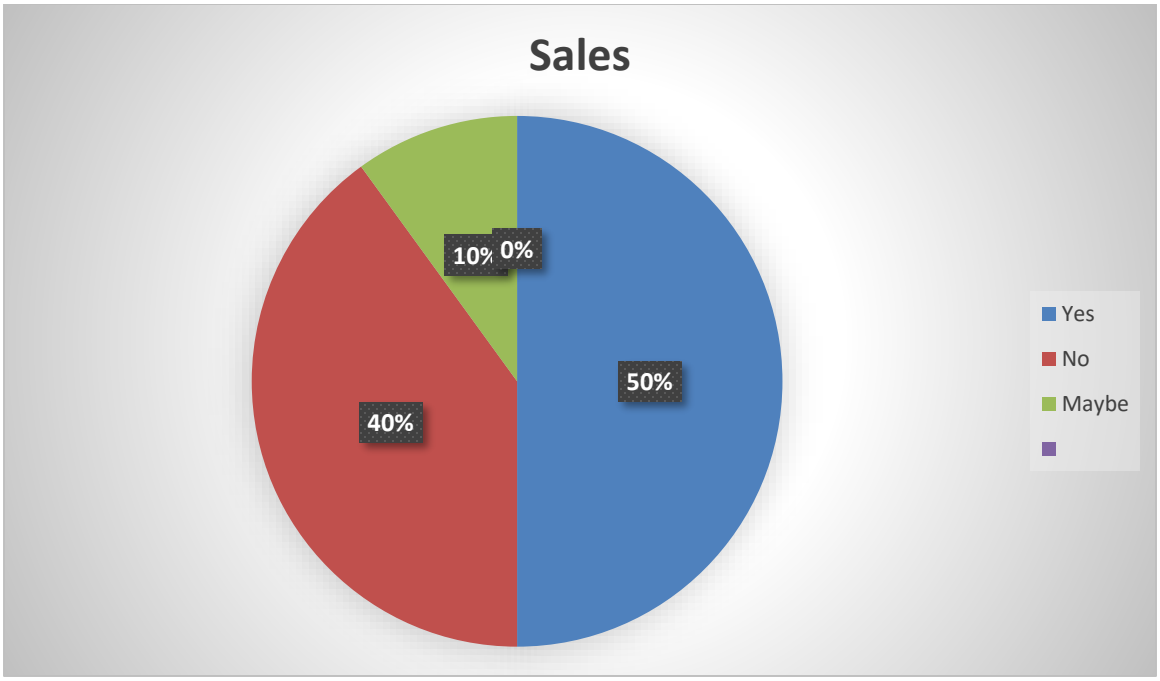
Variables	Percentage
Cyber security	10
Data integrity	20
Both	70



From the above bar graph and chart, it is seen that10% of CEOs and managers of the banking services think that cybersecurity helps to secure their online customer service. Where 20% of them mentioned that data integrity only helps in protecting their online customer service. On the other hand, the rest of the 70% said that both data integrity and cyber security are helpful for the protection of their services.

14. Do you think banking services should develop their business operations by securing the data?

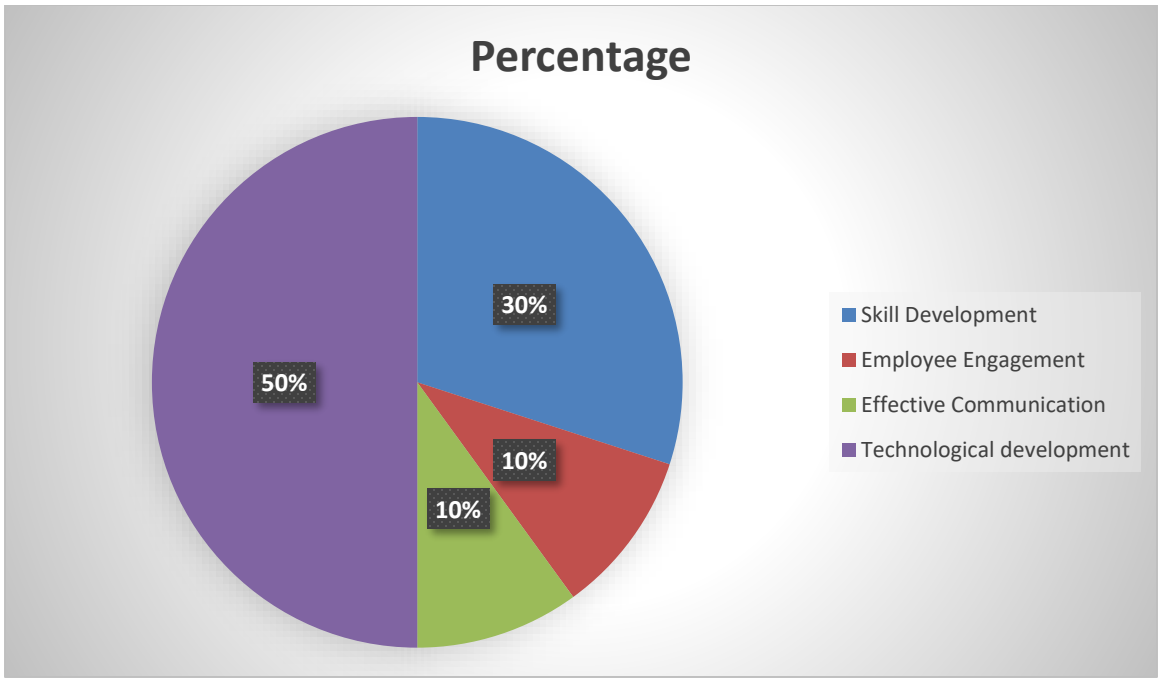
Variables	Percentage
Yes	50
No	40
Maybe	10



As per the above graph, a very interesting analysis was reached, it showed that 50% of participants think that banking service can develop their business operations by protecting all the data and 40% does not agree with this statement and 10% of them may be agreed with the above statement or may not.

15. What kind of progress do you notice while improving the protection of data in the Dubai banking sector?

Variables	Percentage
Skill development	30
Employee engagement	10
Effective communication	10
Technological advancements	50



After developing the secrecy of data, the banking sector can develop several factors that help in expanding their business in an effective way. According to this question, 30% of managers have told that skill development is possible by protecting the data and 10% believe that employees are motivated for the development of the protection of data. At the same time, 50% of them mentioned that the technology is developed and the rest of 10% said that communication can be improved due to the improvement of data protection.

Hypothesis Testing

H0: Cyber-security and data integrity are not large parts of the internet on banking

H1: Cyber-security and data integrity are large parts of the internet on banking

Question 16

16. Do you think data integrity concerns and is large part of Internet of Banking

Strongly Agree	Agree	Neutral	Agree	Strongly Agree
22	32	2	20	24

Question 17

Do you think that cyber-attacks are caused due to lack of security concerns in the Internet of Banking?

Strongly Agree	Agree	Neutral	Agree	Strongly Agree
27	33	2	20	18

From the research study, it can be identified that cyber security and data integrity are large parts of the internet on banking. This can be identified from the Regression test performed through SPSS analysis and gives the value of .944. This indicates that there is a direct relation in between the internet and advanced technology available to that of occurrence of cyber attacks. The attackers are taking advantage of the advanced technology and breaching the data integrity of the internet of banking. The adjusted R Square value is .891 along with the R Square Change value estimated to be .892. The Sigma value has been estimated to be .0001 which signifies that there is a positive relationship in between the independent and dependent variables. The mean square value has been estimated to be 209.861. The unstandardized coefficient value has been estimated to be .969.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	.313	.105		2.978	.004		
	Cyber_attacks_lack_of_security	.969	.034	.944	28.400	.000	1.000	1.000

a. Dependent Variable: Data_Integrity_large_part_internet_banking

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.944[a]	.892	.891	.510	.892	806.566	1	98	.000	.304

a. Predictors: (Constant), Cyber_attacks_lack_of_security

b. Dependent Variable: Data_Integrity_large_part_internet_banking

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	209.861	1	209.861	806.566	.000[b]
	Residual	25.499	98	.260		
	Total	235.360	99			

a. Dependent Variable: Data_Integrity_large_part_internet_banking

b. Predictors: (Constant), Cyber_attacks_lack_of_security

5.2 Thematic analysis

After collecting the secondary data, it is needed to analyze it. Therefore, it is needed to do a thematic analysis by which the researcher can make a comparison between all the collected secondary data. This analysis will focus on the journals, articles, and data of previous writers and researchers. In this report all the journals and researches conducted by other previous researchers are compared. The thematic analysis will help to make a decision based on the secondary data and limitations of the previous researches.

According to Warren, Kaivanto& Prince(2018), there are several cyber-attack can be occurred which can harm the financial and banking industry. As per these writers, the banking industry can confront some offensive activities as cyber-attacks as malicious insiders, malware, phishing website, hostile states, hack-tivists, and cyber criminals. These will create a systematic risk and loss of huge money. For these suspicious activities, the banking industry worldwide faces some serious issues. These cyber-attacks can become from several groups of attackers. According to these researchers, the activities of the cybercriminals stimulated by the black-market economy and in there, the knowledge tools are exchanged which will not define any kind of boundaries. In this research, the ransom wareWannaCry is mentioned. This ransom ware attacked several financial industries of the US and this ransom ware was monetized by some criminals of Russia and weaponized by the criminals of North Korea. They also mentioned data loss as a cyber-risk for e-banking services. Therefore, there is a need for proper data integrity. In May 2017, the breach of Equifax results in a loss of 15.2 million personal records. This cyber risk doesn't an immediate security risk but can create a major risk in the future. They stated that if the data loss has happened in a bank, then the consumers lose their confidence towards the bank and they change their behavior as well. However, this research described the triangle of trust by which the banks can reduce the cyber-risks. By the way, this research has some lacks as it will not discuss any latest technologies. However, this method will not sufficient to prevent these cyber-attacks. Therefore, they need to analyze some of the latest technologies by which the rate of cyber-attacks can be reduced.

On the other hand, the study of Bamrara (2015) focused on the strategies taken to reduce cyber risks. When the banks are connected to some intranet or internet, then the intruders can harm the system anytime. In this research, techniques like authentication techniques, web password

hashing is evaluated. Authentication increases the security level on the endpoint and it facilitates to reduce the attacks on the private domain. The single-user environment is also helpful in this case. They can utilize one password for several applications. PwdHash is very important which an extension of the browser is. It makes the e-banking process domain-specific and it is an effective technique as well. Apart from that, this research mentioned Cryptography which is an ancient technique to secure the information from hackers. Additionally, the database management system (DBMS) is utilized to store the users' data and it is more secure than any other system as it is cloud-based. The database of a bank can store a huge amount of information and data. The users can a small part of this database and unrestricted and suspicious access will be blocked. Therefore, this DBMS can assure security in the context of access control. This study is very much focused on the strategies that can be taken by the banking industry to assure a secure service to their customers on the e-banking platform. This study is a recommendation for all the banks of UAE by which they can reduce the rate of cyber-crimes.

On the other hand, the study of Bouveret (2018) focuses on the cyber-attacks and cyber risks associated with the banking industry. In this research, it is stated that Romania is the origin of cybercrime and most of the phishing websites are generated from China and Romania. It is stated that the cyber-crime can be a threat to an e-banking platform in three ways and they are availability, confidentiality, and integrity. These researchers said that cybercrime can result in the loss of revenue and change of customer behaviors. Though the two articles focus on the cyber-attacks and the strategies to prevent these issues, the study of Bouvreet (2018) focuses on only cyber risks and its typology. There is no mention of its preventions and tools by which the banking sector can handle these difficult situations. Therefore, this study will give a perspective on the different types of threats that can be confronted by the e-banking platform but there is a lack as it is not mention any prevention.

Interview

1. Do you think banking services should develop their business operations by securing the data?

Manager: Based on the opinion of manager, banking services should develop their business operations by securing the data.

2. What kind of progress do you notice while improving the protection of data in the Dubai banking sector?

Manager: Based on the opinion of manager, technological development is the best progress of developing data in Dubai banking sector.

The SWIFT is of the opinion that two-factor authentication is the most secure way of transaction, therefore, the banking sector must develop a systematic plan to approach this problem. The main concern is that most banks are reluctant to install and develop such programs as they do not trust the risk prevention that it entails. Thus, banks cannot be fruitful from this research. However, this journal or study is needed for the researcher as he has to focus on the typology of the cyber risks by which he can take a decision on the risks confronted by the banking sector in recent days. Further research must be conducted to clear the discussion further.

5.3 Summary

This chapter is the main and vital part of this research as it explains the data and information regarding the topic. This chapter can be helpful for the researcher to accomplish the research aim and objectives. In this chapter, the researcher gave a deep insight into the collection of the data and analysis of the data. The structure of the survey was explained in this chapter. The survey is conducted on 100 participants who are managers and CEOs of some famous banks of UAE. The survey consists of 15 close-ended questions. After completing the survey, the researcher o a quantitative analysis to take further decisions about what the participants think about this topic. Apart from that, the researcher collected secondary data from several journals, books, articles, and websites. After that, he/she compared all the data and journals with the help of thematic analysis. The thematic analysis helps to give a brief explanation of these journals and the researcher can take the best part of these journals to analyze the research. Apart from that, a discussion part was also attached to this section. In this discussion, the researcher gave his decision after analyzing the whole information which he/she collected. Apart from that, this discussion will help the future researcher and banking sectors of the UAE to know about the data integrity and cyber security methods. As mentioned earlier research on education and awareness is also required which shall be covered through this research.

Chapter 6:Results and Discussion

The discussion of this dissertation reflects on the major key findings which are collected from the literature review, analysis as well as result chapters. The framework of this research work is made on the basis of the literature review section. This study has analyzed cyber risk and various types of cyber risks which have a major negative impact on the banking sector. However, online banking provides several kinds of benefits to the consumers and opens new opportunities for the banks, this also enhances the banking risk and threats especially security problems. This study involves a cyber-crime scenario and its impacts on bank finance. Among several types of cybercrime, ATM frauds, phishing, malware attack, credit card frauds are huge cybercrime that affect the banking industry badly. These issues foster the operational activities of online banking. Thus, their brand image becomes decreased and loses a large number of customers.

6.1 Observations

There has been quite some shortages when it comes to implementing cyber threat policies in the UAE region. According to a report by (Kesselring, 2018) it has been noticed that 74% of organisations are pressed for the threat of cyber-attacks and not only the banking sector. The Information Systems Security Association (ISSA) and the Enterprise Strategy Group (ESG) have joined hands to strengthen the industry and create more cyber security jobs throughout UAE.

Through our research it was also found out that there is a bug gap when it comes to cyber security laws in the Middle East. The main lack is the responsibility factor(Ibish, 2017). There is no dedicated departments that deal with the laws in various departments. More than one government like the Ministry of Trade, the Central Bank, Intelligence and Defense Department and others seemed to be involved in it. This causes immense problems when solution is to be found for such laws(AL-MOALLA, 2017). Moreover there are several other challenges in the UAE, which needs to be overcome for proper policies to be implemented. The implementation seemed to be a bigger problem for the UAE than formation.

According to the Bowden(financierworldwide.com, 2013), one of the largest obstacles that banks face in UAE is accepting the fact that threat exists. In the data analysis chapter, it is seen that 90%

of CEOs do not accept that banks face threats. It is only the 10% who accept that cyber-attacks are a major threat to security. However, the recent malware attack on the Saudi Aramco proves that the threat is real. Through the questionnaires, it was found out that there are various IT companies also admitted the fact that the higher authorities of the banks did not believe in allocating time and money to guard and increase their security level. The greatest threat here is admittance of the fact that cyber threats could be real.

The type of cyber-attacks in the questionnaires, also showed us that through ages cyber-crimes have also developed in nature. The criminals have also become more sophisticated and knowledgeable and the digitization process of the UAE government further facilitated matters for them. The sophistication and skill of criminals have reached to such a level that they can hack into multiple locations at the same time through organized criminal cells. This means that cyber security and risk management have become one of the crucial issues of our times. The threat should not be taken as just another IT risk, but a risk to the enterprise, where there should be dedicated risk managers. According to (Bestani, 2019) the entire C-level should be prepared to take an active role in risk prevention. He also mentioned that cyber criminals usually target companies which store huge amount of data and banks are a very lucrative targets with access to finances of the entire nation. This was further supported by the researches that was made.

6.2 Discussion

In the present day, online banking crime has been grown rapidly with well-developed e-banking platforms and therefore a proper investigation must be needed. In that perspective, it is vital to take steps to develop their using models and tools or bring new latest and advanced technology which helps to mitigate such secrecy issues in the banking sector. However, many banks in Dubai realized that new authentication techniques have some disadvantages by which they cannot obstruct online man from the attacks. Although a general protection have been taken by the banks in the market,they all are not perfect to catch all danger threatening in the e-banking services. Variousother solutions are available and these have a new layer of protection to secure the customer data and they must be adopted by the banks with changing times.

The results and findings discussed in the previous chapters also identifies the eradication of the cyber threat issues by advancement adaptation of several technologies and strategies. IT technology changes the whole business chain and model of banking services. This helps in making

a huge value in the market and exacerbates their competitive advantages by mitigating the challenges and risks come from the customers. In the literature review section, it is also concluded that the implementation of this technology does not only reduce the processing and operational cost of the banking sectors but also lessen the switching and search costs of the customers. People can also use a cashless transaction for the utilization of information technology in online banking services. Apart from that, data integrity is very helpful for maintaining all the data of any banking sector. Several technologies and tools are available and among them, the firewall mechanism is one of the major systems to identify the cyber-attack. Moreover, chip card utilizing Home Banking Computer Interface (HBCI), vulnerability assessment and penetration testing method, TAN generator is also a useful and effective method for providing proper safety and security of the customers' data. These can make their online transaction reliable. With the help of all these techniques, all security and safety issues can be resolved and their operational activities can be developed.

Meanwhile, through the secondary data, it was found out that Sheikh Mohammed bin Rashid Al Maktoum, the Vice President and Prime Minister of Dubai have launched a cyber-security strategy in 2017, which aims for a sustainable goal for the banking industry for the future(Progressive Recruitment UK, 2017). The new strategy have called on the experts to focus on five major areas; Cyber Smart Nation, Cyber Security, Innovation, Cyber Resilience and National and International Collaboration. Protection of data and integrity was taken as the highest priority by the Sheikh. For this very reason, the Dubai Electronic Security Centre (DESC) is working with all government agencies and the Central Bank to upgrade the level of electronic security. Effort is being made to make themselves at par with the international standards. A certain measure was also taken by the UAE Banks Federation (UBF); cheque chains were launched in order to authenticate user security. QR codes were added onto the cheques. MICR technology was improved and upgraded for the industry to ease the security on clearing cheques.

6.3 Summary

In this research work, the survey method (primary data) fostered this project because some were not focusing on the concept of this research topic and some did not fill the whole survey paper. At the same time, there is a huge chance of biasness as some participants cannot answer. Moreover, the fear of customer changing banks were also one of the reasons, why many didn't

choose to answer the survey questions properly.This has a negative impact on the research work, especially in data analysis. Besides that, the survey can be very time-consuming. Therefore, it is recommended taking only qualitative studies where face-to-face interviews will be conducted for depth analysis. The interview process helps to make a proper connection between the researcher and the participants by which the research gathers more information from them.But many positive results were obtained from the secondary data which came from authenticated sources like journals, news reports and more.

As per this study, it has been concluded that the banking sector has to implement an appropriate strategy and technology for the elimination of security issues. Along with that, if there have no security issues in the bank, they have to provide extra security in the online banking services which are provided to the customers. This helps in keeping all bank data safe and secure and retaining all customers as well. Thus, the banking service can get a huge competitive positioning in the market as well. This research paper is also helpful for the researchers to make further research work regarding this research topic.

Chapter 7: Conclusions and Recommendations

The main aim of the research report was to study the impact of cyber threat especially on bank integrity, analyze and asses the existing measures and give some further recommendations if any. This project is successfully completed and takes the decision from the outcomes. It is observed that there are some serious issues which should be mitigated.

Financial risks have never been more complicated than now with the advancement of technology. As cybercrimes continue to evolve, UAE has become the 5th nation in the world to be affected by cybercrimes. Citing Bowden(financierworldwide.com, 2013) again, there are hundreds of cyber-attacks which UAE faces daily and connectivity seems to be the main issue for it. Questionnaires did not provide this data, but when going through journals it was seen that 39% of financial institutions in the Arab region indicated that they suffered a decline in clients due to non-implementation of cyber security measures. This report was formulated by the IMF, the World Bank and the Arab Monetary Union. The government in 2018 had taken steps to cut the illicit flow of finances but threats are not completely eradicated by the laws.

7.1 Recommendations

It is noted that E-banking on the whole provides several opportunities to the banks and also provides a huge benefit to the customers. However, it is totally depended on the internet and therefore there are huge risks and security issues in this platform. However, the intelligence program can mitigate these issues to a great extent and give a competitive advantage to the banks. It is also seen that the banks of UAE have faced so much cyber-crime in the past few years which results in huge financial loss and change in customers' behaviors. They now think twice before taking advantage of e-banking. The main problem arises with connectivity but in the modern world that is something everyone should live with. Therefore, from the research, it is recommended that they should acquire some newest technologies which can assure better cyber security. Financial institutions should implement the next level e-banking services for the customers where the latest technologies like cloud, machine learning, BlockChain needs to be implemented to check all the endpoints and secure the electronic data.

Acquiring the newest technologies for data integrity is not easy. The bank should have enough resources and capabilities to acquire these technologies. They need to employ a higher

experienced IT professionals' team by which they can implement these technologies. However, it is seen that now the customers are always looking for the banks which give more security.

The number of cyber-attacks in the e-banking platform is boosted day by day and it is being a great challenge for the banking industry. From the survey, the researcher realizes that the authentication tools by most of the banks in the UAE have some cons and are not able to offer a reliable security performance. However, there are some methods and solutions for cyber-crime. They should introduce and implement some new layer which can ensure more security at the endpoints. In these technologies, the customers can confirm their physical identifications in the meantime of online transactions. Moreover, it is concluded that the bank should not bring only a single strategy to cover all the threats of the cyber-crime. They should acquire multi-layer protection to give their best and reliable services to the customers. Therefore, these banking industries should focus more on the data integrity as it will help to build the trust of the customers as well as they can gain more profit rate.

Another important finding from the result is that, there are some recommendations for the banking industry of Dubai to focus on data integrity and mitigate the cyber-attacks. It is recommended to the banks that they can go deeper into the cloud to cope up with cybercrime. They should migrate most of the activities in the cloud. The banks also need to work on their alert management system and various crime related methods like the Heartbleed, Shellshock bugs, DNS Tunnelling and the Domain system needs to be explored and ways must be found by the experts to combat attacks from them. Thus it is recommended that all banks come together to work on a common platform so that this threat can be managed in a cost effective way. This is further important because a study by Al Meshar(Kshetri, 2013) pointed that cyber security after 2021 can cost up to USD 6 trillion globally.

The research aims and objectives is to find out how cyber-attacks impact bank integrity and for this the IT team of these banks should be strong and these banks should take advantage of the cloud computing power. Microsoft Azure, one of the best cloud service providers can facilitate the banking industry by providing the advantage of machine teaching(Rodriguez et al., 2015). It is also cost-effective and the bank should not be invested too much money for such infrastructure. However, the cloud is the best way for the bank in the case of cyber-security. The big cloud providers offer strict security to its datacenters. The utilization of biometrics can reduce the

percentage of cyber risk. These types of cloud rapidly check all the endpoints and block all of the threats before their impact on other consumers. Apart from that, IT professionals should be expertise in several latest technologies by which they can implement several security and take a step on an emergency basis.

7.2 Summary of the study

This research project is conducted in a systematic way by choosing the best methodologies. At first, the timeline was made as it will help the researcher to manage all the activities on time. In the first chapter, the aim and objectives were set. Apart from that, the need for this research was described. The limitation of this research was also explained. The future scope and the background of this research were demonstrated. In the second chapter, the literature review was done to support the collected data according to the research objectives. The third chapter provided a clear view of the best-suited methodologies for this research. In this research, the researcher collected both primary and secondary data as well as he followed mixed methodologies. In the fourth chapter, the information about the surveys was explained. Along with that, the results of the survey and data analysis were done in this chapter. At last, a small discussion was given in this chapter. The last chapter illustrated some suggestions for future researchers as well as the banking industries of the UAE. At last, the conclusions were drawn.The questions were important in drawing up conclusions and showed effective ways where recommendations could be targeted to improve bank integrity.

Chapter 8:Recommendations for Future Research

There are few further recommendations have been observed which will help the future researchers to get the best result by eradicating these serious issues. Firstly, it is seen that the sample size is limited which limits the possibility for conducting further interview session. To get a better outcome, the research report should increase the sample size. However, the interview has helped in qualitative analysis and now we can know about the particular behavior and feelings about this topic by the interviewees. However, it is seen that many participants left some questions unanswered and some gave some confusing answers. From this situation, some difficulties were faced and therefore it is necessary to find a better outcome. As mentioned earlier higher authority in banks are also fearful of the fact that answering questions truthfully might affect their customer base and hence this made the possibility of getting proper answers very difficult. However, if banks could conduct internal audits and examinations, they could have come up with much better results as to what is lacking in their system of cyber security. The data analysis chapter clearly showed that many of them were not aware that the threat is real. Thus, acceptance of cyber threat must also be taken into consideration, especially by the authorities of the banks.

Secondly, it is recommended that the pattern of the survey should be more systematic and the future researchers should take care of this situation that everyone can clearly understand all the questions and give their best possible answer. The questions should not only be targeted to the higher authority of the banks but also to customers as well. A study (National Security Council, 2019) pointed out that only when customers become aware of the rules and regulations and the risks of e-banking, only then the banks can be pressured to further improve their system. Thirdly, it is also recommended that the questionnaire be improved to include important questions to lessen the time period as we can see that it will take more than one year to complete the whole research. Therefore, there was a delay in finding the result and take a decision. However, if the timeline can be short, then the banking industries can take major decisions very fast according to the result of the research; this is possible by asking pertinent questions only and also targeted the customers with the awareness of the issues.

Lastly, it can be said that although questionnaires are good for getting qualitative results, the inefficiency faced in the interviews makes us think that secondary data were able to give much better results and much more accurate data. The research method thus, needs to further explored by the future researchers so that authenticate results can be obtained.

8.1 Conclusion

Overall to conclude it can be said that the future is difficult to predict and can only be hopeful; this is because the future greatly depend on the capacity of the banks to take up cyber security strategies and how much they are willing to spend on them. But a minor step can be taken by the government by introducing education of cyber-crimes and also implementing cyber laws throughout the country. A report (Jacobson & Levitt, 2009) confirms this theory stating that education and awareness is what is necessary for fighting a transnational threat like this.

References

AL-MOALLA, S. M. (2017). *ANALYSIS OF THE UNITED ARAB EMIRATES' NATIONAL SECURITY.* Durham: Durham University.

Alwan, H. B. (2018). Policy Development and Frameworks for Cyber Security in Corporates and Law Firms. *International Journal OF Legal Information*, 137-162.

Bestani, S. (2019). *Banks cannot drop their guard against cyber threats in the region.* Retrieved April 19, 2020, from https://gulfnews.com/business/banking/banks-cannot-drop-their-guard-against-cyber-threats-in-the-region-1.64703167

El-Guindy, M. N. (2014). Cyber Crime Challenges in the Middle East. *3rd Annual Cyber Security for Energy and Utilities.* Abu Dhabi: NCBI Publications.

financierworldwide.com. (2013). *Cyber security and data protection in the Middle East.* Retrieved April 19, 2020, from https://www.financierworldwide.com/cyber-security-and-data-protection-in-the-middle-east#.XpvuXsgzbIU

Guéraiche, W. (2019). *The UAE and the Arab Spring: Rethinking Foreign Policy.* Cham: Palgrave Macmillan.

Hepinstall, W. M. (2019). *UAE loosens Saudi alliance to push peacemaker image.* Reuters.

Ibish, H. (2017). *The UAE's Evolving National Security Strategy.* Washington: Arab Gulf States Institute.

Jacobson, M., & Levitt, M. (2009). *Combating the Financing of Transnational Threat.* Dubai: Emirates Center for Strategic Studies and Research.

Johnson, H. (2019). *Total Quality Management Survey Tools.* Retrieved April 18, 2020, from https://www.surveymonkey.com/curiosity/10-online-survey-tips/

Kesselring, L. (2018). *Cyber Security Skills in Crisis: 3rd Annual Global Survey by ISSA and ESG Open Today.* Vienna: Information Systems Security Association.

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Middle East and North African Economies.* Springer.

National Security Council. (2019). *Transnational Organized Crime: A Growing Threat to National and International Security.* National Security Council.

Progressive Recruitment UK. (2017). *How is Dubai strengthening its efforts on cyber security?* London: Progressive Recruitment UK.

Volodina, N. V., Zaluzhny, A. G., & Tarasova, D. M. (2019). The systematic approach to modern political and legal systems of states on countering international (transnational) extremism. *The Revista Amazonia Investiga*, 98-103.

Al-Azzam, A. F. M. (2015). The impact of service quality dimensions on customer satisfaction: A field study of Arab bank in Irbid city, Jordan. *European Journal of Business and Management, 7*(15), 45-53.

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2016).The effects of cyber threats on customer's behaviour in e-banking services. *International Journal of e-education, e-business, e-management and e-learning*, *7*(1), 70-78.

Arcuri, M. C., Brogi, M., &Gandolfi, G. (2017). How Does Cyber Crime Affect Firms? The Effect of Information Security Breaches on Stock Returns.In *ITASEC* (pp. 175-193).

Avgerou, C., &Walsham, G. (Eds.). (2017). *Information technology in context: Studies from the perspective of developing countries: Studies from the perspective of developing countries*. Routledge.

Bamrara, A. (2015). Evaluating database security and cyber attacks: A relational approach. *The Journal of Internet Banking and Commerce, 20*(2).

Bouveret, A. (2018). Cyber risk for the financial sector: a framework for quantitative assessment. International Monetary Fund.

Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., &Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13-23.

Ghernaouti-Helie, S. (2016). *Cyber Power: Crime, Conflict and Security in Cyberspace*. EPFL Press.

Goel, S. (2016). Cyber Crime: A Growing threat to Indian Banking Sector. *International Journal of Science Technology and Management*, *5*(12), 552-559.

Gupta, B., Agrawal, D. P., & Yamaguchi, S. (Eds.). (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*.IGI global.

Healey, J., Mosser, P., Rosen, K., &Tache, A. (2018).The Future of Financial Stability and Cyber Risk. *The Brookings Institution Cybersecurity Project, October*.

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015).A survey of cyber security management in industrial control systems. *International journal of critical infrastructure protection*, *9*, 52-80.

Lawal, T. T., Lawal, N. A., &Akanbi, A. A. (2018).An Evaluation of the Legal and Regulatory Challenges of Electronic Banking System in Nigeria.

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., ...& Cruz, T. J. (2018). Cyber security of critical infrastructures. *Ict Express*, *4*(1), 42-45.

Maurer, T., Levite, A., &Perkovich, G. (2017).Toward a global norm against manipulating the integrity of financial data. Economics Discussion Papers, No 2017-38. *Kiel Institute for the World Economy. http://www. economics-ejournal. org/economics/discussionpapers/2017-38 Page*, *2*.

Maximov, R. V., Sokolovsky, S. P., &Gavrilov, A. L. (2017). Hiding computer network proactive security tools unmasking features. In *CEUR Workshop Proceedings* (Vol. 2081, pp. 88-92).

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review*, *24*(1).

Rodriguez, L., Curtis, D., Choudhury, S., Oler, K., Nordquist, P., Chen, P. Y., & Ray, I. (2015, October).Action Recommendation for Cyber Resilience.In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 1620-1622).ACM.

Sabherwal, R., &Jeyaraj, A. (2015). Information Technology Impacts on Firm Performance: An Extension of Kohli and Devaraj (2003). *MIS quarterly*, *39*(4), 809-836.

Sajid, A., Abbas, H., &Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384.

Sardina, J., Olkhovskii, A., & Lowell, R. P. (2018). *U.S. Patent No. 10,025,710*. Washington, DC: U.S. Patent and Trademark Office.

Tyagi, S. (2019). Cybercrime overwhelming online banking: A Project Management approach's alternative1, 2.

Vaismoradi, M., Jones, J., Turunen, H., &Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis.

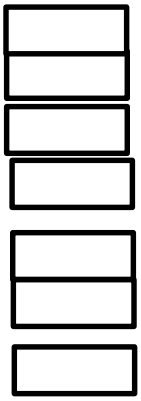
Warren, P., Kaivanto, K., & Prince, D. (2018). Could a cyber attack cause a systemic impact in the financial sector?. *Bank of England Quarterly Bulletin*, Q4.

Appendices

Appendix 1 (Survey questions)

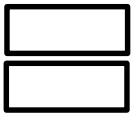
1. For which bank are you serving?

- Bank of Baroda
- Commercial Bank of Dubai
- Abu Dhabi Islamic Bank
- Arab Bank
- Emirates NBD
- FGB Bank
- Other Banks



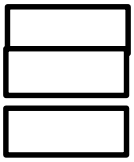
2. In which position do you work?

- CEO
- Manager



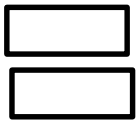
3. Do you think the internet is secure for conducting the financial transactions of the banking sector?

- Yes
- No
- Maybe



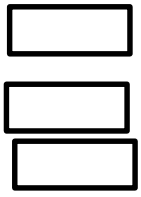
4. Does your bank face any cyber-attack?

- Yes
- No



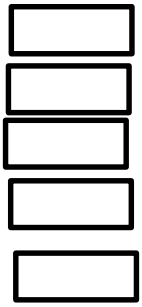
5. How much financial loss you faced for the cyber-attack?

- 0-2000AED
- 2000-5000 AED
- More than 5000AED



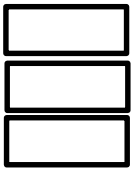
6. What type of cyber-attack does your bank face?

- Phishing
- Malware attack
- Cyber Squatting
- SMS Spoofing
- Other threats



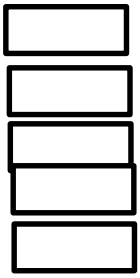
7. Do you think the customers change their online transaction behaviour due to cyber-attack?

- Yes
- No
- Don’t know



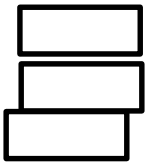
8. What do you think that which region is responsible most for the cyber-attack?

- Romania
- UK
- USA
- Middle-east
- Other regions



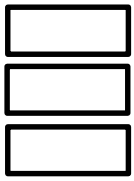
9. Do you think technological development is the main reason for increasing fraud-ness?

- Yes
- No
- Maybe



10. Which latest technology can make the online transaction safe and secure?

- Artificial intelligence
- Blockchain
- Machine learning



11. Do online customers service keeps proper records of the account transactions?

- Yes
- No
- Sometimes

12. Which tools do you implement for identifying the cyber-attack?

- Firewall mechanism
- Chip card utilising Home Banking Computer Interface (HBCI)
- Vulnerability Assessment and Penetration Testing
- TAN generator
- Other methods

13. How do you secure online customer service?

- Cyber security
- Data integrity
- Both

14. Do you think banking service should develop their business operations by securing the data?

- Yes
- No
- Maybe

15. What kind of progress do you notice while improving the protection of data in the Dubai banking sector?

- Skill development
- Employee engagement
- Effective communication
- Technological advancements

Appendix 2: Gantt chart

Research activities	2017	2018				2019				2020		
	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Formulate research proposal												
Formulate research proposal												
Research methodology												
Identify Relevant Literature												
Implementation of the Research project												
Questionnaire Design												
Data Collection and Report												

Evaluation of Research outcomes												
Data analysis of results												
Present Findings and Discussion												
Presentation												