Human Behaviour in Cyber Security

السلوك البشري في الأمن الالكتروني

by

ALYA ABDALLA ALJNIEBI

Dissertation submitted in fulfilment
of the requirements for the degree of
MSc PROJECT MANAGEMENT
at
The British University in Dubai

April 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that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.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 aim of this research is to identify the history of cyber threats and define the cyber security system. Moreover, highlight the human behavior and factor that influencing the security system supported by a qualitative research that are done by interviewing employees that work in the IT department. An interview was made by questions that highlight the importance of human and their role in improving a security system. The interview was done by emailing the targeted people who work in the related field. And after collecting the responses, the data were examined and studies to connect the human factor and the cyber security system.

نبذة مختصرة

الهدف من هذا البحث هو التعرف على تاريخ التهديدات في الامن الالكتروني وتعريف نظام الأمن الامن الالكتروني. بالاضافة ، تسليط الضوء على السلوك البشري والعامل المؤثر في نظام الآمن مدعومًا ببحث نوعي يتم إجراؤه من خلال مقابلة الموظفين الذين يعملون في قسم تكنولوجيا المعلومات. تم إجراء مقابلة من خلال أسئلة تسلط الضوء على أهمية الإنسان ودوره في تحسين النظام الأمني. تم إجراء المقابلة عن طريق إرسال بريد إلكتروني إلى الأشخاص المستهدفين الذين يعملون في المجال ذي الصلة. وبعد جمع الردود تم فحص البيانات ودراسات لربط العامل البشري بنظام الأمن الالكتروني

Table of Contents

1. Chapter 1: introduction

Many reports are missing the perspective of human factors and are side effects on the cyber security. And when it is mentioned or considered, the scope of human factor is often limited. As human factors considered being inflexible and static, moreover it can't be easily tackled, but can be influenced by increasing the awareness. Cyber security however is considered flexible; also the behavior of human can rarely be influenced as an outcome of the awareness alone. Moreover, to improve cyber security system one needs an appropriate intervention and purpose to tackle and change human behavior. The focuses of this dissertation is to explore the history of the first cyber threats around the world, and the types of threats that are influencing the cyber security from different approaches. The human behavior and factor in affecting the security system will be supported by statements from interviewees who are working in the IT Field.

1.1 The objective of research

The aim and purpose of research is to find answers to questions through the implementation of scientific process. Moreover, the main aim of research is to uncover the truth that is hidden and has not been discovered yet. Although each research study has a specific purpose, research objectives can fall into number of the broad grouping:

1. To add knowledge about a phenomenon or to attain new information and insight into it.
2. To reveal an accurate characteristic of a specific situation, individual, or a group. These types of studies of object in test are known as *“descriptive research studies.”*
3. Research also can help in determining the rate of frequency about something happened and if it is associated with something else. Studies like this are known as *“diagnostic research studies.”*

4. To examine a hypothesis of a regular relationship and connection between variables. This type of studies is known as *“hypothesis testing research studies.*

1.2 Background to the research

Information technology is valuable and critical to the modern society. It makes life much easier by enhancing efficiency of doing things. All over the world, impacts of information technology have been felt irrespective of the location in the world. However, as the world go through transformation towards becoming more technologically advanced, problems have emerged on the utilization of the existing technologies. It has become clear that technology can also be used wrongly and thus harming the very users that are supposed to benefit from it. The term cyber security to address all the needs related to this new challenge. Some people engage in unethical behavior to taking advantage of users’ vulnerability and expose them to various forms of danger including duplicating their identity, which can lead the users to grave economic and legal consequences. Unfortunately, the trend has been on the increase according to recent studies, which means that more people fall prey to the evil minds out there whose main focus is to cause problems to these people. It means that there is a great need to study these trends and establish ways of bringing the problem to the end.

1.3 Problem statement

The problem perceived in this paper increased danger of cyber security threats. The paper recognizes cyber insecurity as a major problem facing the contemporary society. The world recognizes the significance of information technology but also understand the dangers associated with its misuse by some sections. Today, there are many cases of cyber insecurity and thus having negative impacts on the society. The paper hopes to expose the dangers of cyber insecurity and highlight ways of dealing with the problem. It utilizes qualitative research methods to expound on the problem and enable the readers to see how grave the situation is currently all around the world.

1.4 Research significance

The study on cyber security would be a learning paradigm to enhance knowledge among the readers concerning the nature and impacts of cyber insecurity. It also looks at the cyber security systems and how human behavior influence the efforts put in place to ensure cyber security. It is believed that the study would help in enhancing positive behavior change to ensure cyber security in the contemporary society. The findings of this study would also make it possible to understand the current situation as far as cyber security and the systems put in place to protect users of technology from becoming victims of cyber insecurity.

2 Chapter 2: Literature review

2.1 Introduction

Cyber security is defined as the protection procedure that is taken in an organization to protect, avoid or lessen any risks or interruption that is caused by a cyber-attack. This security plan is meant to protect not only computer or devices that are connected to cyber world, but also any assets that are valuable to an organization. Assets such as computers, employees and buildings, are vital to any organization and must be considered when applying cyber security plan. Cyber security is defined by many researchers in many different aspects. One definition is by Merriam Webster dictionary “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”. More over the International Telecommunication Union (ITU) state Cyber Security as : “ Cyber security is the collection if tools, policies, security concepts, security safeguards, guidelines, risks management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications system, and totality of transmitted or stored information in the cyber environment” (Evans et al. 4669). One can agree that the definition of cyber security is an umbrella that not only protects the confidentiality and data privacy, but also the availability and integrity of that data. Moreover, it ensures the security of any valuable assets that is vital to an organization such as, devices, data, human, and building.

2.2 Cyber-attacks and first threats in history.

What threatens the cyber security is the evolving nature of cyber-attack and it nowadays around the world, moreover, becoming more and more complicated. Cyber-attacks come in different ways and types such as:

- *Phishing attacks:* This kind of attack happens by sending a mail or email to a user pretending to be from a trusted resource. The email contains a link and when the user clicks on the link it will ask him for a user name or password such sensitive information that the hacker can use later to in hacking the computer.

- *Unpatched software:* it happens when one runs a software with security weaknesses. When the software vendors find out the vulnerabilities they produce “patches” it is an additional code that help in fixing the security weaknesses. While running unpatched software hackers and criminals will be aware of the vulnerabilities and can use it for their gain.
- *Worm*: it’s a type of malware that comes from malicious attachment or software vulnerabilities, once the worm is installed it goes replicate itself in the computer causing the system slow down, moreover it can delete files, install software that can be a backdoor for the hackers.
- *Trojan*: Trojan is malware that comes hidden in legitimate software, even when it is installed on the computer the user will not know. It can be used by the criminals to gain access to the user’s system.
- *DOS Attack*: Denial of Service attack is used to slowdown a system by attacking the servers, causing troubles to the users to access the system.
- *Insider threat*: Insider threat is a term that means the behavior and act of any individual inside the organization. The insider threat can affect the security in a negative way and can be made intentionally or unintentionally that will cause a potential loss to the organization. The insider act and threat cannot be underestimated as to should be considered as a most dangerous threat for any organization.

The first threats that were started were:

- **First worm**

Bob Thomas in 1971 was the first man who created a program that is considered the first ever worm. The worm was spreading between computers devices which were a great issue at that time. Although it was not malicious, but it showed a message on the infected computer saying, “*I’m the creeper: catch me it you can”.*

- **First Denial of Service (DOS).**

Another incident was made by Robert Morris in 1989, which created a worm that affected the internet by slowing it down. This was the first DOS attack, although Morris did not create the worm to cause damage, he created it to point out the security weaknesses. Yet the he made started to replicate causing losses that are estimated around 100,000$ to 10,000,000$ and also caused in internet partition that lasted for day

Many malicious attacks started then to spread and become more complex to solve. The malicious attacks that are mentioned in the article are some of the attacks that were the first in history.

Day by day the cyber-attacks are getting more complicated and cause more damages that my lead to shut down to any organization. Many organizations and businesses nowadays are connected to the cyber environment, this connection lead to more risks and challenges of facing cyber-attacks. Moreover, attacker recently aim to cause more and great damage that will be costly to any organization, and those attacks are used for different interest such as political interest, personal interest (revenge) or competition

Although there are many kinds of threats around the world in the cyber environment. But the organizations most challenging threat is the insider threat, and that is affected by the behavior of the employees, whose their behavior can either affect the organization's security in positive of negative way.

2.3 Challenges and risks of cyber security

"I don't want to live in a society that does these sort of things ... I do not want to live in a world where everything I do and say is recorded. That is not something I am willing to support or live under." Edward Snowden.

Edward Joseph Snowden, he is an American technician and agent that worked as NSA (National Security Agency) Contractor that employed by the CIA (Central Intelligence Agency), and that before leaking information about the spy program to the press.

He is the former US state agent and a professional computer specialist and expert. And he published scandal about the people who he worked with and classifies them as unethical. He uncovered the National Security Agency's participation in some local surveillance practices, and that practices were thought of violating the people privacy. So he spent few years gathering evidence and information in order to uncover the truth to the press. After that, Snowden went to Hong Kong because of his concern for his safety, and there in Hong Kong he met know reporters to document the scandal and everything he had took and stolen. The evidence shocked the people around the world especially the United States. He revealed that people are being watched for every second of the day and everything is documented whether they are using social websites, emails and massages even the phone calls. The reason of why Snowden made that scandal is that, human right to live freely and the privacy of people who are being watched from different nations and religion.

This story shows that how cyber space is a critical. And how can it be used for different purpose, political reason, watching people, system breach and damaging any targeted entity. The cyber systems must be used wisely and be protected from the unethical use.

Years ago, Cyber threats were new risk few had experiment this risk. But today it is a risk that exists and clears that every organization should take in consideration. It is a risk that can cost more than $400 billion a year. Day by day the cyber attacks are spreading and becoming more persistent and complex. Cyber-attacks become a favorite tool for protestors and terrorist around the world, as they can threat any entity around the world and make a damage that can be physical or virtual assets. One of the recent incidents, cyber criminals have hacked 21.5 million records of American public service employees, manipulated with the network of German congress, and blocked 11 television channels in France for several hours. Moreover, at the click of a mouse hackers carried out an attack that affected on more than 1000 energy companies, hackers got the control over engines, wind turbines, power plants and gas pipelines, the incident took over 84 countries plus, United States, France, Spain, Germany, turkey and Poland. Although, people has gained benefits from information technology and cyber advances that held in the growth of the production industry such as energy, retail, transportation, technology, healthcare and banking. The world should not underestimate the other side of the technology, and that it is a doubled-edged sword the more you are dependent on it the more is the cyber threats and risk you will face in the future.

As to respond to those threats many organizations are taking a step and cooperating in order to keep an eye on those threats. Concurrently, it's globally clear that people are becoming more independent on the internet and the cyber environment, reports are showing that the amount of data is expanding and there will be around 50 billion device that is connected to the cyber world by the year of 2020, moreover an estimate that everyone will have 6.5 device on this world. In addition, the cyber-attacks are not only affecting the companies directly, they also can cause a reputational loss, economic losses also can affect can flow down to the supply chain in the companies. As a result, of the evolving threats and the existence of cyber threats it is very important to assess and manage those challenges. Moreover, it is essential to keep in track and pace with the cyber criminals and apply a "near – term fixes" besides developing and applying a long term measures that will help in facing the risks and challenges in short and long term.

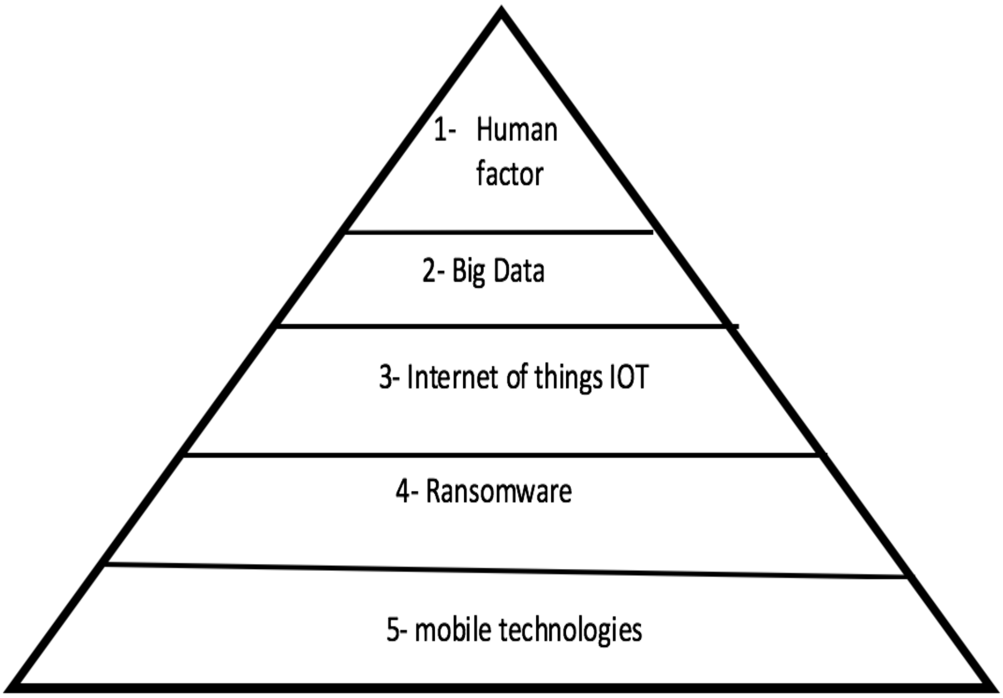
More than 30 countries including Germany, Japan, United States, Canada, Italy, France, and United Kingdom have started in implementing cyber security strategies and plans. In United Kingdom the Financial services regulators started working with other top banks in order to improve their cyber risk management. Germany asked the companies that are critical to the country infrastructure to report to the government if they face any cyber threats. Countries around the world started to take in consideration the risk of cyber security and how it can affect many sectors security, infrastructure and economic growth around the world.

2.4 The 5 Top Risk and challenges

Gene Spafford said that," *The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then, I have my doubts"*

All of us are living now in highly connected and digital world. That everything we use is now almost connected to the cyber environment. Furthermore, people cannot stop or be against the growth and the evolution of technology, since the growth of technology is helping more in country development in many ways. But it is very important to spread awareness among people about the cyber risks and explain way on how to mitigate cyber threats in cyber space.

Nowadays, every major organization and company whether it is small or big is facing or had been a victim of cyber-attack. Day by day new threats emerge that did not exist few years ago, such as, Ransom attack, smishing and hacktivism. Cyber threats are in growth and the more human are dependent to the technology the more those threats are becoming a big burden to everyone around the world. In TEDx conference Srini Sampalli talked about the five most challenges that people will face in cyber security.



5- Mobile technologies:

As noticed people are not only living in highly connected world but also a highly mobile, using cellular, WIFI, Bluetooth, RFID, and NFC. Those are only few technologies that people are using every day through their mobile. Companies are in race by adding new feature and technology in the mobile, there are number of sensors that the phone have. Those sensors can collect personal information such as, location sensor, accelerometer, and gyroscope for orientation, light sensor,

-

pressure sensor, and temperature sensor, barometer for attitude plus the phone's camera and the phone itself. By that collection of information, the phone can know and have more information than your closest member of family or friends.

All that information, have we ever wondered who is using that information that is used by the third-party application. Many are not aware of the rights that they are giving when downloading that third-party application. Many applications ask for access to your text massages, location and other things. Hackers and criminals can use those rights and hack the targeted device to build a virtual and digital profile by collecting that information from those sensors and from the third-party applications and use it against their targets.

4- Ransomware:

Comes in the 4th place in the pyramid. It is the latest type of viruses that also spreading around the world. Ransomware stands for ransom demanding malware. It gets to the targeted computer by either downloading an attachment containing a virus or when visiting a malicious website and clicks on a link or picture. Later, when it is on your computer it starts to encrypt all the files in the computer making them useless to use, and the only way to unlock them is to get the secret code to unlock the files is from the hacker itself. Moreover, to get the key from the hacker, he will ask to pay him in ransomware which usually through Bitcoin to keep himself anonymous. A report showed by the Professor Srini, there has been 600% increase in ransomware in just one year, many organizations have been a target to ransomware attack. Also, in just the first quarter of the year2016 there has been more than 200 million dollars paid in ransomware.

3- Internet of things (IOT):

IOT, every object that people will own will have or will be equipped with a capability that can, identify itself, communicate itself, locate itself, sense and compute itself. And in the very near future even the pen, watch, TV, car, microwave, fridge, baby monitor and even the cloth will be connected to the internet. Each one of them will have an IP address. Moreover, a report shows that there will be about 21 billion IOT devices by the year 2020 and will be communicating with each other, and that will be an easy cyber environment for the hackers. The use of IOT can lead to risk and threat of the country's infrastructure. Using IOT technology should be studied and analyzed before applying them in a sensitive organization.

2-Big Data:

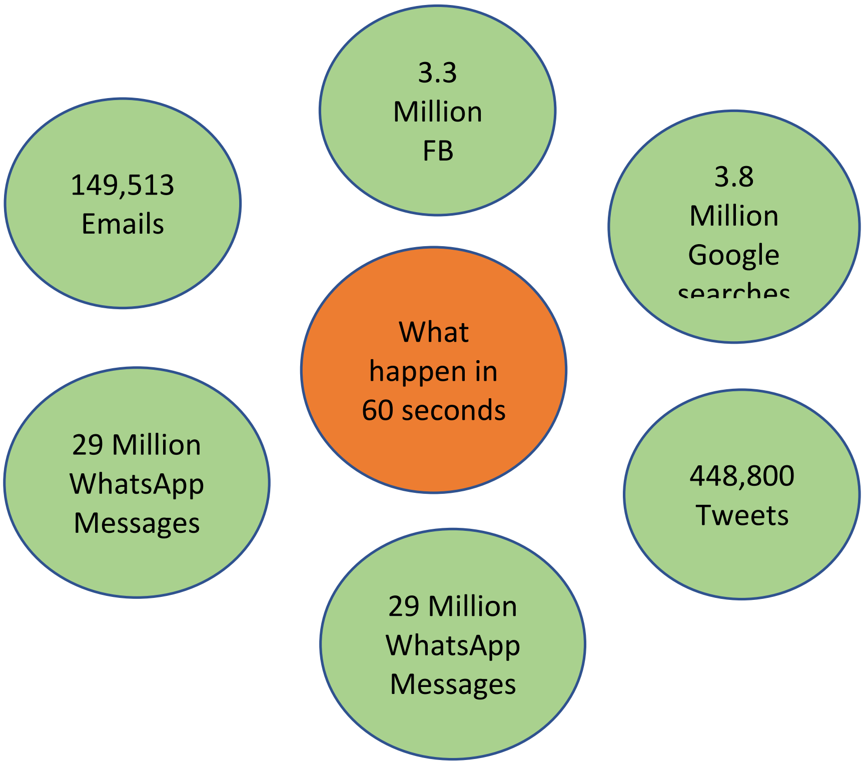

3.3 Million FB
149,513 Emails
3.8 Million Google searches
What happen in 60 seconds
29 Million WhatsApp Messages
448,800 Tweets
29 Million WhatsApp Messages

Figure (2) is from the video Top Five Emerging Cybersecurity Challenges | Srini Sampalli | TEDxDalhousieU

2- Big Data is a term that refers to the varied and heterogeneous mass of digital data that is produced by the organizations and individuals. And the characteristics of the big data are large volume, diverse forms and speed in processing. Big Dara require specific and more complex computer storage and tools for analysis.

In figure (2), it shows what happens online in 60 seconds. Srini mentioned that by the near future every individual will generate 1.7 million bytes if information every second which is incredibly a large digital footprint. Which attracts the hackers to cause a variety of different attacks.

1- The Human Factor:

The most important part and vital part of cyber security and a big challenge from any organization. Human factor can cause a weak link in the system of cyber security. It is said that “a mature sax system but professionals hack people”. It is easy to scam people using social engineering techniques to make them reveal sensitive information that the cyber criminals can use. For example, the last string in the weakest link is the personal password. Millions of bank accounts have been hacked, and an analysis shows that 32 million breached accounts shows that people are using simple insecure password that are easier for the hackers to hack. And that is because of the human nature of feeling troubled to memorize different password for different accounts and the hassle of changing from time to time.
In conclusion, the everyday evolving of the cyber threat can lead to many risks to any organization that depending on the use of the network and technology. In addition, the organizations around the world need to be updated about the new techniques and threats that are used by the hackers, in order to develop a good cyber defense. In the end to achieve a quality and strong security wall in the cyber space human and technology should work together.

2.5 Case Study about the Influence of Human Behaviour on Cyber Security Assurance

A study by Mark, Leandros, Ying and Helge on the aspect of human behavior in cyber security assurance was utilized in this project as a case study. The researchers begin their report by mentioning that there are numerous cyber security breaches reported all over the world despite the numerous security measures put in place by various organizations in different industries. The study was among the first ones to look into the cyber security assurance processes. The compilation of the research was based on the available research studies in the field of cyber security assurance and the influence of human element on the assurance process. The purpose of the study was identifying the cyber security elements that can be enhanced by further research and development focusing on the relevant and significant findings of literature review. The findings of the study showed the need to focus on areas that need further research such as assessment of human reliability as well as enhanced validation to ensure appropriate assurance.

In the introduction, the authors recognize the increased growth of information security in the last two and a half decades. They also mention that information security is a common item within the public sector. With the topic of cyber security and hacking being common topics in the modern IT conversations, information security has more significance now more than ever. The authors also defined cyber security as the process or capability of protecting communication and information systems from unauthorized modification or use, exploitation or damage. However, there are still weaknesses and gaps within cyber security despite the increased interests and acceptance of the information security. The paper mentions that the evidence for this can be observed in the increased number of cyber security breaches observed all over the world.

The study shows a data on publicized data breach, which indicate that there have been an increase of 101% in the UK healthcare data breaches. It also shows that data aches resulting from human errors increased by 93% between 2013 and 2014. Data breaches as a result of cultural factors also increased by 95% during the period. The published scientific papers shows that researchers have placed more emphasis on the security controls though it does not show whether there is a correct application of these controls or not. In this sense, it demonstrates that there is a great need to focus on the people who are engaged in the operations.

The study also showed that human behavior is lacks consistency and can be influenced by the existing relationships. People are also likely to underestimate risky practices. The risky behaviors that are likely to result to cyber security. There are some people who would engage in risky behaviors despite knowing they could lead to cyber security threats to the organization. In this case, the paper also supports the need for organizations to pay closer attention to human factors in their efforts to enhance cyber security within their premises.

As a result of the increased publication of the security breaches, organizations continue to focus on finding ways improving cyber security as means of protecting reputation and brand as well as preventing or reducing the related financial impacts. The study also established that half of the cyber security incidents are caused by the people factor, which has remained the same since the start of information security management. The element is mainly people working with the IT systems and their unintentional errors and mistakes. The motivation of the study was to look beyond the current practices in the field of cyber security and tackle issues that are mostly left out untouched by other researchers. It highlights the insider threat spotlight report of 2015, which showed that organizations continuously invest ways of dealing with the insider threat. It also confirms the findings of this study that human factors play crucial role in cyber security in the various organizations. It established that staff-related breach make up a huge chunk of all the cyber security breaches. In this manner, it helps towards achieving the objectives of this study in demonstrating that human behavior is a crucial factor in cyber security.

The study supports this study by highlighting a survey that established that 72% of companies where security breaches were rampant had poorly understood security policy by staff members. It shows that companies need to ensure that their employees are well trained on issues concerning security. It supports the fact that companies that invest in training their staff on security issues are likely to avoid certain security breaches.

3 Chapter3: Influence of Human Behaviour

In this chapter the attention will be in the influence of human behavior. It will discuss the background of human factor that influence cyber security and the behavior and aspects of human.

3.1 Human factors background.

The Office of National Statics (ONS, 2016), published a report that estimated the cyber frauds which cost the companies an estimation of £193 billion. In addition, the report showed and highlighted that in the year of 2015-2016; 5.8 million of individual cases in of cybercrime had been reported and registered. Half of the cybercrime were fraudulent actions, such as, bank credit card account fraud, and the other half is the abuse and misuse of computer, such as, computer viruses and hacking or unauthorized access to computer. Other reports from the Business Crime Survey (BCS, 2015) showed that there is an increase of online fraud by 55% between 2015-2016. The same report is showing that the big problem and concern is the growing threats from human within the organization, or what is called "*insider threat*". The most important concern that the reports showed is that, the weakest link and element is the cyber security chain is human (Anwar et al., 2016; Nurse, Creese, Goldsmith, & Lamberts, 2011; Sasse, Brostoff, & Weirich, 2001; Sasse & Flechais, 2005).
Many organizations are focusing and devoted to improving their existing security system and infrastructure, and that because of the continuous fight to protect their businesses from the cyber threat (Pfleeger & Caputo, 2012).
Moreover. Many attempts to improve the cyber security by the technological solutions, such as, biometric devices, firewalls and other solutions that can provide legitimate defense against the variety kinds of cyber threats.
Yet, all these technological solutions are making an assumption that the security and cyber threats they are facing are coming from outside and external threats or attacker.
Early analysts in the area of cyber security highlighted that one of the biggest challenges of creating a strong and effective cyber security strategies is the human factor within the chain of the security system (Whitten & Tygar, 1998).

The researcher also noted that, the usability perspective that most of the security rules and systems are either too blurring or too problematic for the end users to absorb and follow effectively (Whitten & Tygar, 1998; Sasse & Flechais, 2005). They also highlighted that the condition is complicated in the characteristics of human factors including:

- Employees are lacking the understanding the importance and vitality of data, systems, software and protocols that are within the organization.
- Employees are unaware of the level of risks that are attached to the assets that they are responsible for.
- A lack of knowledge and influence of their behavior and how it can put the assets they are responsible for in risk (Sasse & Flechais, 2005).

3.2 The insider

Any system in the organization that contain an aspect of human activity, in addition, there is great possibility of the potential impact on the system as an insider threat. Recently the theory of insider threats has gained more attention around the world and, it presents a rising concern of the inside and internal security system in the organizations (Greitzer, Kangas, Noonan, & Dalton, 2010; Greitzer et al., 2016; Keeney, 2005; Probst, Hunker, Gollmann, & Bishop, 2010). The insider threat can lead to a weakness in the security system and breaches that can affect the company which can lead to a financial loss.

Researchers had described the insider threats as two types:

1. The Malicious Insider

Many researchers wrote about the insider threats, and they focused on the opinion of that those insiders or individual have a malicious intent and are running a hidden activity for their personal gain or financial gain. One example of the insider threat definition is presented by Cappelli, Moore, and Silowash (2012) is:

“A current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the

confidentiality, integrity, or availability of the organization's information or information systems."

The researchers explored the aspects of the insider from a psychology point of view. Researchers, like Shaw, Ruby, and Post (1998) had identified four main signs for a human that can become an insider threat, the aspects are:

1. "*Negative life experience*": an individual's past and experience affect their attitudes toward their colleagues, this past experience can cause frustration to the individual and can lead aggressive outburst.
2. "*Lack of Social Skills and Isolation*": Researchers also assumed that an insider can shows a symptom of social skills absence and tend to isolate themselves from the social activities. Moreover, the researchers suggested that a lack of social skills can lead the insider to other social interaction such as through social networking, it's not necessary that they will isolate himself, he or she might find another way of interaction with people. People who lack social skills and are using online social communication instead are unable to deal with workplace social and emotional issues or situations effectively. Shaw et al. (1988) suggested that a combination of aspects that can lead to an individual feel and have a mindset of frustration and dissatisfaction. And can be noticed when interacting with others in the workplace, what is also called "emotional leakage", which is where the individual acts are far outweigh comparing to the nature of the incident.

3. "*Sense of entitlement*": researchers think that some insiders are suffering from a sense of entitlement. This sense is usually provided by having the access rights and special privileges the insider has in his work. Those individuals may have a special skill that makes them have special treatment. Insiders may also have difficulty in adjusting to some specific rules and protocols in the organization.

4. "*Ethical Flexibility"*: the meaning of this concept is that insiders can suffer from an incapability of empathizing and understating other collogues that

would typically prevent an individual from committing an action of insider threat. Moreover, immaturity is an aspect that is linked to this habit.

CPNI (2013) added in their report some detailed aspects to the personality traits that is connected and associated to individuals who committed a threat inside a company. In CPNI report the insider threats was known as "*a person who exploits, or has the intention to exploit, their legitimate access to an organization's assets for unauthorized purposes*" (p.4). The study explored case studies on insider threats in UK and gathered those key information and elements that had a major impact on the insider's behavior as well as with others within the environment. Theses personality aspects are briefed as:

1. "*Immaturity*": researchers noticed that individuals is lacking in general life experience and categorized of being "high maintenance" in term of the supervision and attention they require, moreover suffering from having difficulties in making decisions in critical situations.
2. *"Low self-esteem":* it is noticed that is insiders lacking confidence socially, moreover they have a habit of the heavy need of praise and recognition from their colleague and others. Also, they find it hard to survive in adverse social environments, they life to stay in a comfort zone without getting criticized from others.
3. *"Superficial"*: most of the insiders are described as being "hard to know" by other people, and they are lacking a clear awareness of self-identity.
4. "*Lack of Conscientiousness"*: those insiders most them tend to neglect the rules and practices in the company. Plus, neglecting their responsibilities and duties. Moreover, they have a poor judgment, lack of attention to details, and poor focus.

5. *"Manipulative":* they have skills of persuading to get what they want, and garner relationships that will help them get what they want and ser their own interest. Insiders also aim to adopt social position that helps in serving their needs.
6. *"Emotionally unstable"*: showing a different of inflated mood swing and complains over the most minor problems and incidents.

Furthermore, The CPNI reports wrote about a number of predictors that are built on aspects of individual's living experience and mental and emotional factors. These key predictors are viewed as critically important in the evolution and development of potential insider threats:

1. Poor Work Attitude: a failure to cope and follow the works rules and protocols or being updated about new operating instructions and procedures.
2. Showing sign of stress: those signs include the exaggerating nervous habits, loss of temper, poor concentrations, confusion and difficulty in making decisions.
3. Vulnerable lifestyle: having a lifestyle that can let them to be manipulated by others and external forces such as financial stress, gambling, drug and alcohol addiction, these factors can lead to a desire for more financial gain.

4. Exploitable work profile is having a position that let them access to a sensitive asset in the company that are highly prized and could be sold for a profit.
5. A negative life event: an incident that could be a reason for a development of an insider threats, such as, work problems, a social status loss or work, and injury, and financial problems or loss.

   These are some aspects and indicators that are reported by the researchers, which will help in indicating the insider threats in a company. Other researchers argued about the term "insider threat" and move on to the term "insiderness".

   The other type of insider is:

2. <u>The Accidental or Insider</u>

(UIT; CERT, 2013) has defined an accidental threat as:

"*An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems*". (CERT, 2013, p. ix)

This type of threat happens because of the lack of knowledge of an employee, and the lack of intent to cause damage to a company. Moreover, it is unintentional damage that happens due to difficultly, lack of awareness and cognitive skills. For example; and accidental expose of sensitive information via website of email, or sharing a personal password and user name with someone, and improper disposal of physical information and records. These are some example of accidental and unintentional threat that most of the organizations face from an insider inside the company.

3.3 Human Factor and the Theory of planned behaviour

Many researchers realized how human behavior can affect the security of any organization. It either be affected if negative or positive way. Human's behavior can either strengthen or weakens the security in all types in any entity. And according to that a theory of planned behavior was suggested in order to help in predicting and controlling human behavior.

3.4 Aggregation principle

Since many researchers developed theories about predicting humans' behavior and put specific action according to that, those theories tend to fail because of the poor predictors in specific situations. Fishbein & Ajzen (1974) and Esptien (1983) proposed an answer for the poor predictivity and its validity of traits and attitudes, and it is aggregation of certain behaviors in different situations and form of actions. The idea of aggregation is that, the belief that any single behavior can reflect not only the influence of relevant disposition but also it is influencing other different factors that are unique to specific situation, occasion and action that are being observed. The other sources of influence tend to cancel each other when aggregating the various behaviors that are observed on different situations and various sit-actions, and that shows the result that aggregate gives a more valid measure of a specific behavioral disposition than any single behavior. Many reports and studies that are performed in recent years have verified the validation of aggregation principle by showing the overall attitudes and traits of personality that are in fact predict behavioral aggregates better than they predict significant behavior.

However, the aggregation principle did not justify behavioral variability in different situations; moreover, it does not allow the prediction of a specific behavior in specific situation. The aggregation principle was meant to show the overall attitude and trait of personality in human behavior, and that their influence can be recognized by only looking at general, aggregated and valid sample of behavior. And their influence on certain actions in specific situations is weekened by the presence of other and more immediate factors. Many have argued that the general attitudes and personality aspects have an influence on specific behavior in an indirect way by influencing some factors that are linked to the targeted behavior.

This chapter will present the framework of the theory of planned behavior that deals with nature of behaviors and specific factors. The theory of planned behavior is designed to explain and foresee human behavior in specific situations and contexts.

3.5 The Theory of planned behaviour

In 1985, Theory of planned behavior suggested by Icek Ajzen, which was proposed in his article *"From intentions to actions: A theory of planned behavior."* In 1980, Martin Fishbein together with Icek Ajzen developed the theory of planned behavior from the theory of reasoned action. Plus, the theory of reasoned theory itself was developed depending on other attitude theories such as, "*expectancy-value theories, learning theories, consistency theories (such as Osgood and Tennenbaum's congruity theory, Heider's balance theory, and Festinger's dissonance theory) and attribution theory".* A reasoned action theory is that if ones assess a behavior as a positive attitude, moreover they think that their superior wants them to accomplish the behavior (subjective norms), this will lead to a higher objective (motivation) and the actor or the targeted person will likely to do so. Many studies have confirmed that relationship between attitudes and subjective norms to behavioral intention and the behavior itself.

- **Defining the key variables**

Normative beliefs vs. subjective beliefs

- Normative belief: it is an individual's awareness of social normative forces or other's belief that a behavior should or should not be performed.
- Subjective norm: it is an individual perception about a specific behavior that is affected by the judgment of other people that are important and related to that individual (e.g., parents, friends, and teachers).

Control beliefs vs. perceived behavioral control

- Control belief: a person believes that there are factors that can ease or hinder performance behavior. Moreover, the meaning of perceived behavioral control is theoretically related to self-efficacy
- Perceived behavioral control: a person perceiving and judging performing a specific behavior whether it is easy or difficult to perform. It is suggested that perceived behavioral control is decided by a whole set of available control beliefs.

Behavioral intentions and behavior

- Behavioral intention: it indicates that an individual is ready to perform a specific behavior. It is presumed to be an instant antecedent of behavior. And based on *“attitude toward the behavior, subjective norm, and perceived behavioral control”,* with each one weighted for its rank and importance with regard to the behavior and interest of population.
- Behavior: it is about a response of an individual in a specific situation with the respect to a given target. Ajzen mentioned that a behavior is function of a well-matched intentions and insights of a behavioral control, so perceived behavioral control is likely to moderate the influence of intention on behavior, so when behavioral control is strong a favorable intention produces the behavior.

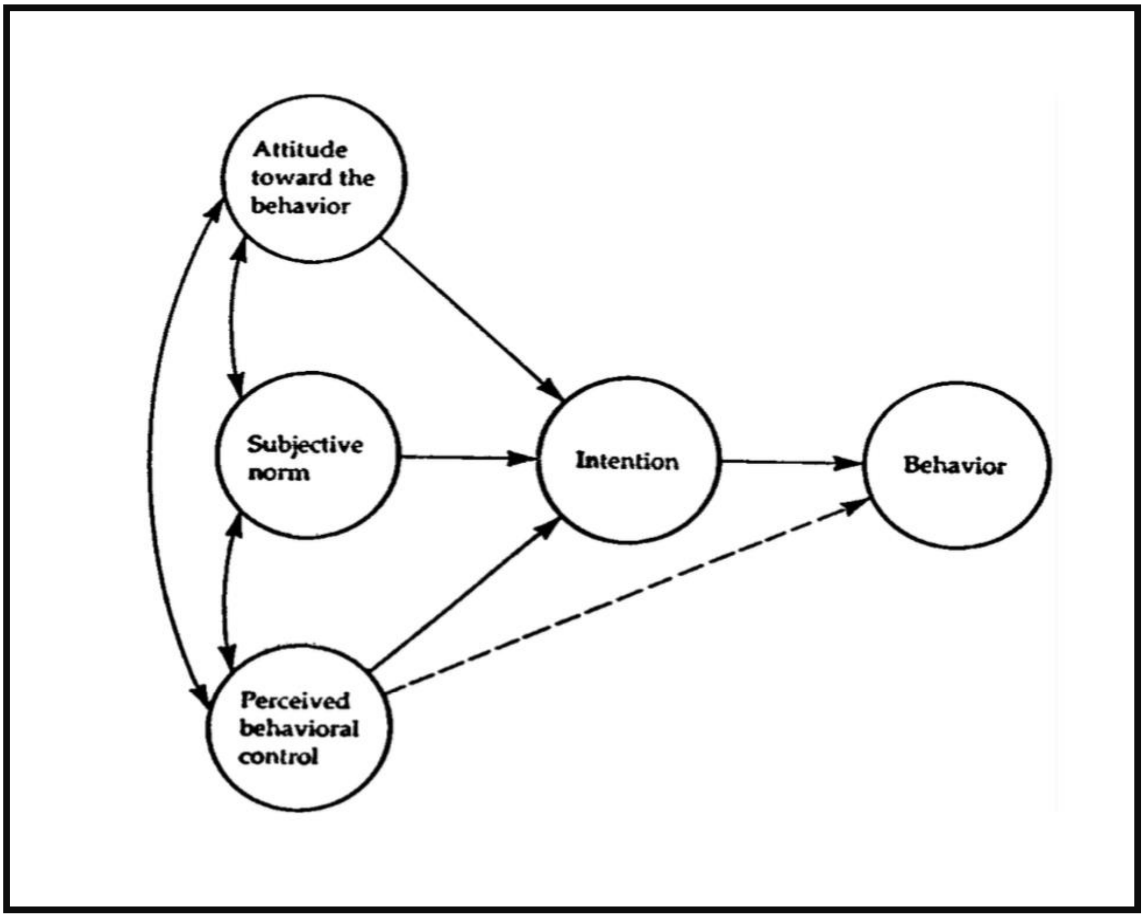
Conceptual / operational comparison

- **Perceived behavioral control vs. self-efficacy**

Ajzen (1991) mentioned in the theory of planned behavior, understanding the role of perceived behavior control derived from Bandura’s idea of self-efficacy. Recently, Fishbein and Cappella mentioned that self-efficacy is similar to perceived behavioral control in the integrative model that also is measured by objects of self-efficacy.

In the earlier research and studies, the composition and the number of object list of perceived behavioral control is depended on specific health topic. For example, a smoking topic is usually measured by object such as *“I don’t think I am addicted because I can really just not smoke and not crave for it,”* and *“It would be really easy for me to quit.”*

The theory of self-efficacy is embedded in Bandura’s social cognitive theory. Which refers to the opinion that an individual can perform a behavior that required producing the result successfully? Self-efficacy concept is employed as perceived behavioral control, and that means that the assumptions of the difficulty or ease of a behavior. Moreover, it is linked to belief control, and that means beliefs about the existence of reasons and factors that may ease or impede a behavior performance. It can usually be measured by factors that begin with the stem, such as, “I know I can exercise.” It mainly measures the assurance toward the chance or feasibility of performing a given behavior.



The figure (4) is taken from ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES.

Description of the theory of planned behaviour:

“Predicting Behavior: Intentions and Perceived Behavioral Control”

As mentioned in this chapter that the theory of planned behavior is an addition and extension of the theory of reasoned action that is made by the original model’s limitations by Ajzen & Fishbein, to deal with behaviors that people cannot control. The figure (4) demonstrates the theory in the shape of structural diagram. To help more in understanding and presenting the potential feedback outcomes of behavior on the existed variables that are not shown.

- **intentions**

As In the theory of reasoned action the vital factor in the theory of planned behavior is the intention of an individual to perform a specific behavior. Intentions are assumed to be affected by the motivational factors that can affect a behavior, intention can indicate of how hard individuals are willing to try, and how much effort they are willing to use in order to achieve a behavior. Moreover, as a known rule the studier the intention to engage in a behavior; the more should be its performance. Yet, it should be clear that the behavioral intention can uncover expression in behavior if only the specific behavior is under control.

For example, if an individual can choose the will to perform or not perform the behavior. While there are some behaviors can meet the requirement very well, the performance can be most depended at least to some degree on such non motivational influences like the availability of necessary chances and resources (such as money, skills, time, and support of others). Together, these factors show individual’s actual control over the behavior. A person should succeed in doing a performance to the extent that she or he has the needed opportunities and resources and will perform the behavior.

The achievement of specific behavior depends on the motivation (intention) and the ability (behavioral control); the idea of the behavioral achievement is by no means new. It creates and found the basis for theorizing on different issues as *“animal learning, level of aspiration, performance on psychomotor and cognitive tasks, and person perception and attribution”.* Some researchers recommended that some conception of behavioral control be used and included in more general models of human behavior, and in the form of *“Facilitating Factors”, “the context of opportunity”,* *"resources", or "action control".* It is usually assumed that motivation and the capability interact in their effects on behavioral achievement. Therefore, intentions are expected to impact performance to the level that the individual has behavioral control; moreover performance and behavioral control should increase to the level that motivates the person to try.

- **Perceived behavioral control**

Self-evident is important to behavioral control; the available opportunities and the resources available to an individual must to some level help the probability of behavioral achievement.

Perceived behavioral control has a vital role in the theory of planned behavior. Perceived behavioral control is the addition that made the differences between the theory of planned behavior and the theory of reasoned action.

In the prediction of intentions and actions before studying the place of behavioral control in predicting, it is more helpful to compare this concept to others control conception. Essentially, perceived behavioral control is different from concept that is made by Rotter's (1966) in the *"concept of perceived locus of control".* With emphasizing the factors that are connected to a specific behavior, perceived behavioral control is about people perception of performing a behavior whether it is easy or difficult to perform. While, *"locus of control"* is a general belief that remains constant across situations and actions' form, perceived behavioral control does usually vary thru situations and actions. So, an individual might believe that her or his outcomes are bent on by her or his own behavior (internal locus of control), however at the same time he or she might also think his or her chances of becoming an Engineer are very poor (low perceived behavioral control).

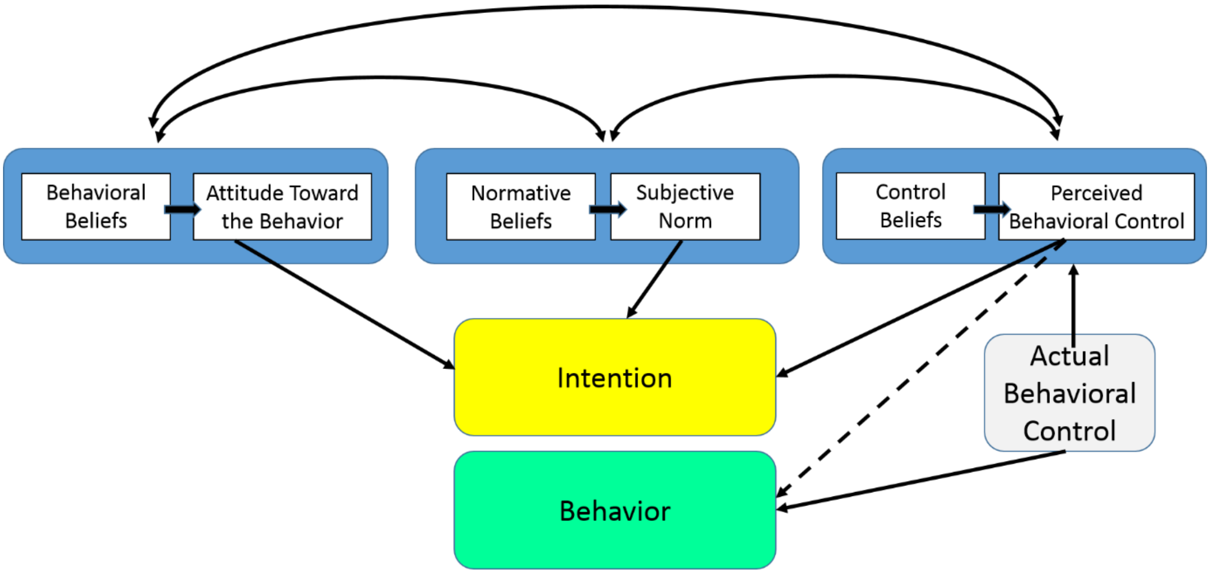
Studies found another approach of perceived control in Atkinson's (1964) concept of achievement motivation. There is an important factor in this theory that is the expectancy of success, and it is defined as *"perceived probability of succeeding"* in a specific task. Obviously, there are some similarities to perceived behavioral control in the view of referring to specific behavioral context and not generalizing the predisposition. In some way, the reason to achieve a success is not defined as a motive to success at a particular task but in expression of a general disposition

"Which the individual carries about him from one situation to another" (Arkinson, 1964). Moreover, this over all achievement motivation was expected to connect multiplicatively with *"situational expectancy of success as well as with another situation specific factor"*, *"the incentive values of success".*

Yet, the latest view of perceived behavioral control is the most well matched and suitable with Bandura's (1977, 1982) theory of perceived self- efficacy, and that is *"concerned with judgment of how well one can execute courses of action required to deal with prospective situation"* (Bandura, 1982). Most of the knowledge about the job of perceived behavioral control comes from the logical research program of Bandura and his colleagues. These studies have revealed that people's behavior is strongly affected by their belief of their ability to perform a behavior. Self-efficacy beliefs can affect choices of actions and activities, preparation an action, effort needed during the performance, in addition to emotional responses and pattern of thought. The concept of planned behavioral shows and places the concept of self-efficacy perceived or belief behavioral control within more over-all framework of the connection and the link among attitudes, belief, intentions and behavior.

Regarding to the theory of planned behavior, perceived behavioral control, along with behavioral intention can be used to foresee behavioral achievement. For this hypothesis at least two rational can be offered. First, holding intention constant, the struggle expanded to carry a course of behavior to a successful end is more likely to increase with perceived behavioral control. For example if two individuals have similar strong intentions to learn some skill like playing piano, and both of them to try to learn this skill, the one who is confident that he can learn and master this skill is more likely to continue that the one who have doubt in his ability. The second factor for assuming a direct link between perceived behavioral control and behavioral achievement is the perceived behavioral control can be used as a replacement for measure of actual control. Whether the measure of perceived behavioral control can replace for measure of actual control of course depends on the precision of the perceptions. Perceived behavioral control may not be realistic when someone has a little information about the behavior, like when the available resources and requirement have changed, or when a new element and unfamiliar factors have entered the situation. In those conditions, the measure of perceived behavioral control can add a little precision and accuracy of behavioral estimate and prediction.

But, to the level of realistic in perceived control, it can be used to foresee the chances of a successful behavioral act. (Ajzen, 1985).



This figure (5) is from (Sphweb.bumc.bu.edu, 2019).

“Predicting Intentions: Attitudes, Subjective Norms, and Perceived Behavioral Control”

The theory of planned behavior assumes three abstractly independent determinant of intention. The first one is attitude is the attitude. Attitude toward behavior and means that the degree to which one has a favorable or unfavorable assessment and evaluation of specific behavior. The second predictor is subjective norms which are known also as social factor, and it means the perceived social force, pressure and rules to perform or not perform the act and behavior. The third factor of predicting intention is the level and degree of perceived behavioral control which as mentioned earlier, states to the perceived difficulty or ease of accomplishing and performing the behavior, moreover, is expected to show and reflect past experience as well as predictable impediments and difficulties. As a general rule, the more the attitude is favorable and subjective norm with regards to behavior the greater the perceived behavioral control, the stronger the individual’s intention should be to perform the behavior. The prediction of intention can differ across behaviors and situations in the relative importance of attitude, subjective norm, and perceived behavioral control. Consequently, in some situations one may found that only attitudes have major impact on intention, and on others that perceived behavioral control and attitudes are enough and sufficient to account intentions, still in others all the three factors can make independent influences and contributions.

- **The limitation of the theory of planned behaviour**

Every concept of theory whether can have some limitation, and for this theory the limitations are:

- This theory assumes that the individual has obtained the resources and the opportunities that can help in performing the desired behavior successfully, regardless the intention.
- It does not consider other factors that can affect the intention and motivation such as, mood, past experience, fear and threats.
- Although the theory accounts normative influences, it still does not consider environmental or economic factors that can affect an individual's intention to perform a behavior.
- It assumes that behavior is an outcome of a systematic decision-making process and do not take in account that it can change with time.
- Although the researchers added a perceived behavioral control in the theory, it didn't mention the actual control over behavior.
- The factor of time frame is not addressed in the concept which is between intent and behavioral action.

3.6 Conclusion

This chapter shows how theory of planned behavior can provide a useful theoretical framework to deal with the humans' complexities and their social behavior. The concept of planned behavior combines some of the vital concepts in the science of behavior and social, moreover is defines these concepts in a method that allows foreseeing and understanding a specific behavior in particular situations. Attitudes regarding the behavior, subjective norms toward to the behavior, also perceived control on the behavior are normally found to foretell behavioral intentions with high level of accuracy. So, the intentions together with perceived behavioral control can account for a significant proportion of different behavior.

At the same time, there are many concerns that remain unsolved. The theory of planned behavior traces subjective norms, attitudes and perceived behavioral control to a basic foundation of behavior beliefs. While there are a lot of evidence for relations between behavioral beliefs and attitudes regarding the behavior, concerning normative belief and subjective norms, also between perception of behavioral control and control beliefs, the accurate form of the relations between them is still uncertain. The most accepted view that describes the nature of the relations and connections in term of expectancy value models, received some provision and support, yet there is need for more improvement. There is specific concern and are the associations of only reasonable magnitude that is regularly observed in efforts to relate belief-based measures of the concept constructs to other more wide and universal measure of these constructs. One can overcome the scaling limitation by optimally rescaling measures of belief strength, outcome evaluation, motivation to comply, and the perceived power of control factors, but the experimental gain in associations between global and belief-based measures is not enough and inadequate to deal with the issue.

However, from a general view, the application of the theory of planned behavior to a specific area of attention provides a mass of knowledge and information that are very useful in any effort to understand specific behavior, or implementing interference that will be useful in changing them (Van Ryn & Vinokur, 1990). Elements of the theory of planned behavior, Intention, perception of behavioral control, attitude toward behavior, and subjective norm each can uncover a different feature of the behavior, as well as each one of them can serve as a point of target to change it. The basic foundation of beliefs offers a detailed description that is needed to earn more information about the behavior’s factors. It depend on the level of the beliefs that one can learn about the specific factors that motivate one person to perform and engage in the behavior and be ready for another to follow diverse course of action.

4 Chapter 4 : research methodology

4.1 Introduction

This chapter about the methodology that is used for supporting this research. The methodology shows the result of the interviews that are done with the participants that works in the field that is related to the research.

4.2 Research

Research is referred to search of information and knowledge. And it also can be defined as a scientific and systematic exploration of information on particular topic. Actually, research is a skill of scientific investigation. The Advanced Learner's Dictionary defined research as *"a careful investigation of inquiry especially through search for new facts in any branch of knowledge."* According to Rendman and Mory, research is *"systematized effort to gain new knowledge."* Moreover, some people view research as a *"movement from the known to the unknown."* Also it is a journey of discovery.

4.3 Research methodology

Research methodology is a particular procedure and techniques that are used to recognize, choose and select, process and analyze information about a specific issue. In research report the methodology part allow people who reads the report to critically asses the validity and reliability of the report.

It is important to design a strategy in order to help in the research objective. Moreover, it is vital to use a research tool that is helpful in the research field. The data that are collected should be analysed to make sure that is validate and supporting the research field.

In this dissertation the information is gathered by focusing and defining the cyber security from different point of view, and then discusses it in the literature review. And according to that the dissertation aim, objectives, and related questions is defined. All the gathered information will be examined and discussed to recognize the results of the data. Then the following steps are conclusion and recommendation that will be built according to the result.

There are two types of research methodology that can help the researcher collect information and gain more knowledge about a particular issue. Researcher can either use quantitative or qualitative method to gather the needed information. Sometimes it depends in the topic or the issue the research is about.

Quantitative research it is used to quantify the issue by gathering numerical data, or information that can be used as statistics. This method is used to quantify opinion, behaviour and other variables. It also simplifies results from a large sample. Quantitative method depends on measurable data to formulate truth and evidence and reveal pattern in the research. The method of quantitative data is more structure that the qualitative data method. Moreover, the quantitative data method include different form of surveys, such as, online surveys, paper survey, mobile survey, telephone interviews, face to face interview, systematic observation and some others.

On the other hand, researchers can also use qualitative method to collect data. Qualitative method is an exploratory research. And it is used to help in more understanding of specific reasons, motivations, and different point of views. It helps in providing deep insight in targeted issue; moreover, helps develop and improve ideas and hypotheses for quantitative research. Qualitative Research is also used to discover trends in opinions, thoughts, and go deeper to understand the problem. Qualitative method of data collection can vary in suing either unstructured or semi-structured ways or techniques. There are some common methods that is used in this type of research method, like, focus group discussions, key information interview, in depth interviews also participation observation. In qualitative research method the sample size is quite small comparing to quantitative research method. Besides, the sample or the respondents are selected to fulfill a specific number of targeted sample quotas.

In this research, the chosen method is qualitative data collection as it suites the research topic and objectives. Interview is the way to collect the needed data from the targeted and selected sample. As known interviews, by interviewing one can gain more knowledge and understand more about how the world is known by asking the targeted person to answer the structured but open-ended questions about their experience. Interviews can vary in the level to which informant or the targeted sample set the agenda. Yet in all cases informant define their own skills and experiences at length, as well as personal and life stories and histories. Moreover, in depth interviews are used to gather different view and perspectives on specific topic.

The questions that are asked in the interviews are covering the cyber security issue from different perspectives. And one can notice that it focuses on the insider threats and human factor in affecting the cyber security in different ways. Also, the targeted sample of the interviews was employees who are working in Information Technology and technical support.

The questions targeted different corners and individual's roles, of the issue that can cause the weaknesses in security of any organization, such as the role or top management, the individual's skills, the organizations role and the insider threats.

In summary, the study utilized qualitative research method whereby much focus was on content previews and interviews. Literature review was conducted both on online sources such as established and reliable sites. Interviews were also used as a primary source of information and provided more information about people understands about cyber security and how human factors affect the cyber security systems in place.

<u>Top management role:</u>

1. Do you think that top management has the responsibility to ensure the protection from cybercrimes in a company? Explain
2. Do top management should consider human behavior when designing cyber security

<u>Personal skills:</u>

3. Do every individual has the right skills to be able to protect the organization from cybercrimes? In addition, what are the skills they should obtain?

<u>Organization role:</u>

4. Are computer systems providing all the protection the company needs?
5. Is reporting cybercrimes important? And why.

Insider threat:

6. Are individuals from inside the company can be a threat to cyber security?

The questions that are mentioned above are helping in supporting the research objectives.

5 Chapter 5: data analysis and results

5.1 Introduction

In this section, a summary about the interviewed people will be presented with their job field and experience. In addition, the gained data will be analyzed and discussed from the different sights.

5.2 The profile of candidates

Candidate name	Job title	Years of experience
Participant 1	Network Security Administrator	11 years of experience in the field of information technology and technical support
Participant 2	System Administrator	7 years of experience in the field of system administration
Participant 3	Infrastructure and security network assistant	3 years of experience in network system.
Participant 4	System and technician assistant	5 years experience in system updates and servers of the organization
Participant 5	IT employee	5 years of experience in the field of information technology.

5.3 Data analysis and result

1. Do you think that top management has the responsibility to ensure the protection from cybercrimes in a company? Explain

Participant 1, who work as a network security administrator, and have 11 years of experience in the field of information technology, security and technical support, Eng. Participant 1 agreed on the first question and mentioned *"Cyber security is a critical business issue for every organization. The Framework and policy should be defined and enforced from top to bottom levels to ensure that the organization are protected. Every organization should have cyber security or information security framework,* *and policy and adherence to it to achieve. As this is information Era, Information is an important asset and information has to be protected by means of technology and tools. With cyber-attacks becoming more frequent and targeted, implementing a robust cyber security strategy is vital."* Participant 1, mentioned the three pillars,*"It can be achieved through three pillars of DATA security.*

1. People: Every employee needs to be aware of their role in preventing cyber threats. Cyber security staff need to stay up to date with the latest risks, solutions and qualifications.

2. Processes: Documented processes should clearly define roles, responsibilities and procedures. Cyber threats are constantly evolving, so processes need to be regularly reviewed.

3. Technology: by implementing right software tools, Firewalls, Security devices monitoring tool etc."

Moreover, participant 2, a system administrator, who worked for 7 years in the related field also agreed the above issue, and stated*, "That the top management have to take responsibility as they have to take the decision on how an individuals and top management need to design the policy that are related to cyber security. And allocate the budget for the same."*

Participant 3, she is an Infrastructure and security network assistant, and worked in the related field for 3 years. Also, she mentioned that "*most of the top management does not take responsibility to ensure cyber security protection, and they should be involved in this process."* In addition, she stated, *"we are now in 2020 and almost all the companies that are working depending on technology, and not considering about the disadvantages and what will happen if any data leak happened. In addition, employees do not have that much awareness on how they can be the reason on letting the attacker destroys the organization without the employee's notice."* Moreover, *"if top management does not have enough knowledge, they will not care about transferring the importance of cyber security protection to the employees and help them understand cyber security and how much a threat can cause damage an organization."*

Participant 4, a 5 years' experience in the organization, and worked as an assistant of system updating and servers. Stated that *"Yes, because cybercrimes hurt the* *company's reputation as well as result in many losses such as financial loss and confidential data loss."*

Participant 5, she in an employee in the IT department with 5 years of experience. She said *"Yes, Top management are responsible to make important decisions or delegating tasks within the organization, so when it comes to threats like cybercrimes, top management must come up with appropriate solutions to protect the organization from cybercrimes."*

Analysis

The results obtained from the response of various participants show that top management teams have a role to play in ensuring cyber security within their organizations. The first participant, who is an IT professional with over eleven year's experience, agrees that cyber security has significant impact on organizations. He acknowledges the significance of enforcing cyber security in the organizations. Information security or cyber security framework is crucial and the top management must strive to ensure that all the employees adhere to the established and outlined policies. People, processes and technology are the main pillars of cyber security. The same sentiments are shared among other participants who also agree that information security is critical to organizations and thus, organizations must go out of their way to enhance policies that sustain cyber security. In summary, the responses in this section show the significance of cyber security and the role of people in enhancing relevant policies by adopting the necessary behaviors and actions.

Summary

We can conclude from the first question and the participant's answers that the role of the top management can be divided in four areas and that:

- Defining the organization's framework in all or organization levels.
- Making decision when facing problems

- Must be updated and have knowledge in cyber security field.
- Must take the responsibility in order to protect the organization by all means.

2. Do every individual have the right skills to be able to protect the organization from cybercrimes? In addition, what are the skills they should obtain?

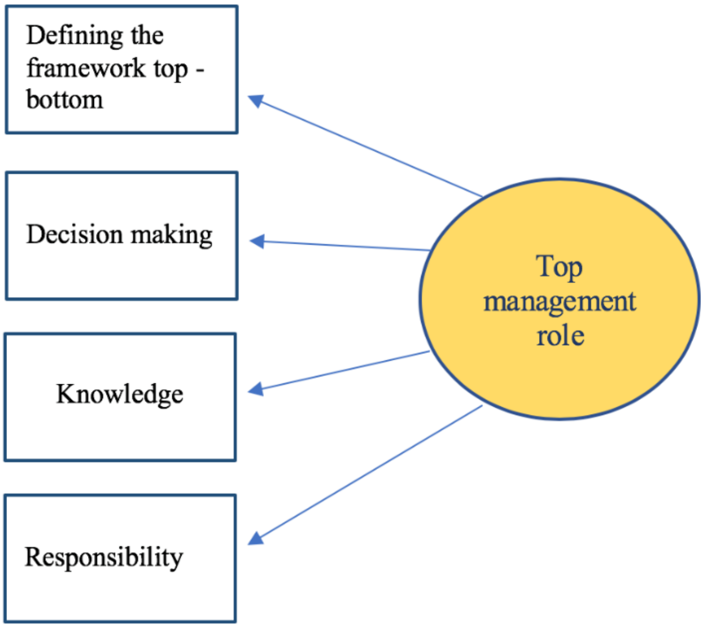


Figure (6)

Participant 1 Agrees that skills are important to protect an organization. And he added that *“Every employee has to play his role in protecting the network. Minimum awareness required that helps to understand the risk associated with unethical practices*.” Furthermore, he stated some important skills such as “*Basic information about web application, data networking and combination channels needed for the employees to aware of cyber security.”* Moreover, *“Basic knowledge of protecting mails, password policy management and keeping up to date to trends around the world of cyber environment. Employees should be made aware and get trained on cybercrimes and cyber security.”*

In addition, Participant 1, mentioned how humans can be a factor of threat, and stated, *“Human error may lead to data breaches, the employees need to protect the information they have and work on. They should be adhering to policy and standards followed in organization.”*

“1. Develop an Effective Security Strategy. Security should be built into the culture of your organization to ensure that every employee within the company understands the importance of cyber security and the far-reaching impact that a data breach can have.

2. Keep Defensive Practices up to date.

3. Security Awareness Training.”

Participant 2, said, "*Not all employees have the right skills in order to be able to protect the organization. Moreover, most of them are not updated about the latest trends of hacking systems, and, how to block those attacks."* Moreover, on term of the skill he thinks that *"it has to be someone who is specialized in that domain; they should have the Certification from the IT security."*

Participant 3, stated that *"sometimes yes but word of security needs to be updated and the people who are working in cyber security sometimes they should think as black hat not only white hat so in this way they can protect themselves from hackers."* And in term of the skills they should obtain, "*they should understand network and how it works, and they have to understand how the infrastructure works in the organization so the cyber security employee can know what are the strength and weaknesses and how they can protect themselves from the cyber threats."*

Participant 4, *"not all of them, and because individuals could be the reason behind these cyber-attacks. Some of the skills they need: taking instant actions and critical thinking."*

Participant 5, *"As an employee working in the IT department, not all individuals are able to protect the organization from cybercrimes, because the new technologies produce new threats and new cybercrimes. The skills an individual must obtain to protect an organization from cybercrime are as following:*

- *Able to detect cyber threats.*
- *Able to adapt and having the passion to learn, as the cyber threats are constantly changing. 0*
- *Problem solving and attention to details."*

Analysis

The results in this section show that there are specific set of skills that are crucial in protecting organizations against threats posed to cyber security. The participants also agree that there is a need to ensure that organizations have established cyber security strategy. Awareness campaigns and trainings are also of great significance in enhancing cyber security within an organization. The findings also show that organizations should invest in developing the right set of skills among their employees to make the significant assets towards improving cyber security and protecting the organizations from threats such as hackers and unauthorized data mining. The ability to detect threats, problem-solving skills and adaptability to changing technological environment are some of the skills mentioned as of great significance in mitigating cyber security threats.

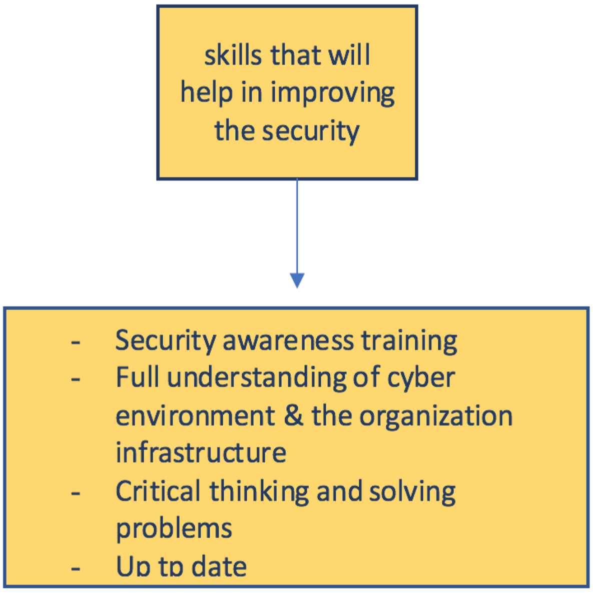

skills that will help in improving the security
- Security awareness training
- Full understanding of cyber environment & the organization infrastructure
- Critical thinking and solving problems
- Up to date

Figure (7)

Summary

One can notice and highlights the important skill that is mentioned by the participants. Some of the skills that are mentioned are vital and critically important. And should be obtained by any security employee:

- Training about the security awareness which will help in more understanding the importance of security in any organization.
- Provide knowledge and full understanding of the cyber environment and the organization infrastructure for the employees.
- Critical thinking and problem solving will help the employees to be quick-witted in facing any unexpected threat.
- Being updated about any new technology and threats risks around the world.

3. Are computer systems providing all the protection the company needs?

Participant 1, that computer systems do not provide the needed protection that the company needs. *“No, it involves as mentioned above their stages or phases involve protecting. Even if you implement the best technological measures and put processes in place to ensure they are properly deployed and kept up to date, poorly trained users, putting your organization at risk, can compromise their effectiveness.”*

Participant 2 also said *“no, the users who are using and applying the computer systems need to be educated in order for the right implementation of the system, otherwise, it will lead to system’s weakness because of the uneducated users.”*
Participant 3, *“depending on the type of the system and what are they using to protect the organization? Employees should put one thing in their mind that is nothing is secured 100%, since the organization is connected to the cyber world.”*
Participant 4, *“Not entirely because these systems need to be updated and checked to ensure that they are not breached. Also, individuals take a huge part in the protection matter. For example, some employees click on links that have malicious software.”*
Participant 5 mentioned that “*No, not all the time, the developing of new technologies created new cyber threats; e.g.; new viruses and so on. Therefore, organization must be able to develop new ways of cyber protections and integrate humans’ skills with technology.”*

Analysis

The response from participants shows that not all computers provide protection against cyber security threats. The computer processes and programs must be configured properly to enhance the capability of the computers to enhance cyber security. They also show the significance of appropriate training for the employees so that they understand how to apply relevant systems and keep them updated to avoid possible breaches. Integrating human skills with technology therefore, is the right approach towards improving cyber security.

4. Is reporting cybercrimes important? And why.

Participant1 agreed that reporting cybercrimes is important. *“Yes, always it has to be reported to avoid Rampant Damage to any organization.*
Cyber criminals usually aim to gain financially, extract data or cause disruption by (among other things):

- *Obtaining personal data to commit ID theft and financial fraud (cyber theft);*
- *Obtaining banking credentials to steal money, or intellectual property to sell to competitors;*

- *Installing ransomware to impair your operations and extort money from your organization (cyber extortion); or*
- *Installing malware to gain access to your systems in order to steal confidential or sensitive data.*
- *Denial of Service to legitimate user by DDOS attacks."*

Participant 2 said *"yes, reporting the cybercrime will keep the organization updated, and will help in improving the future protection and the future planning of the organization cyber security system."*

Participant 3, *"yes, because having the organization secured is the responsibility of each employee in the organization, not only people who work in the security field."* And added, *"When the organization hired you that means you are part of the organization, if anything happens to the organization the employees will be the first one that will be affected."*

Participant 4, "it is important to report cybercrimes, because it allows individuals to be ready for such events."

Participant 5, "Yes, it is highly important as it will help an organization to protect its data and private information."

Analysis

The section shows that employee involvement, such as in reporting any suspected case of cyber security threat is important to organizations. If they are aware of any cybercrime activity happening within their organizations, employees should report such incidents as soon as possible. The responses also confirm that open-door policy could help organizations fight cyber crime because they encourage participation from the employees on matters affecting the organization.

Summary

Reporting cybercrimes considered very important and agreed by the all participants. As it can help in avoiding the damage in the future and minimize the losses. Moreover, improving the system by improving the planning and protection level. And, protecting the vital assets of the organization and this is the data.

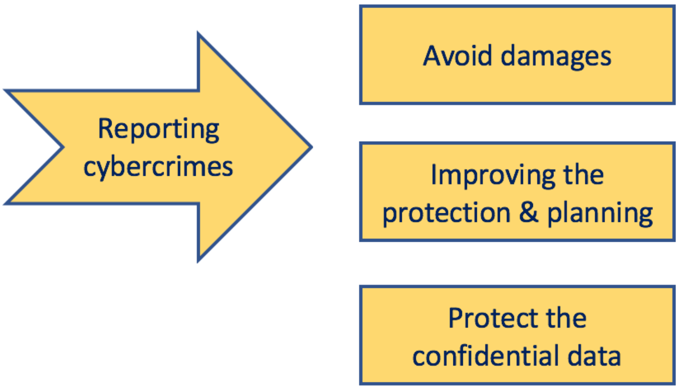
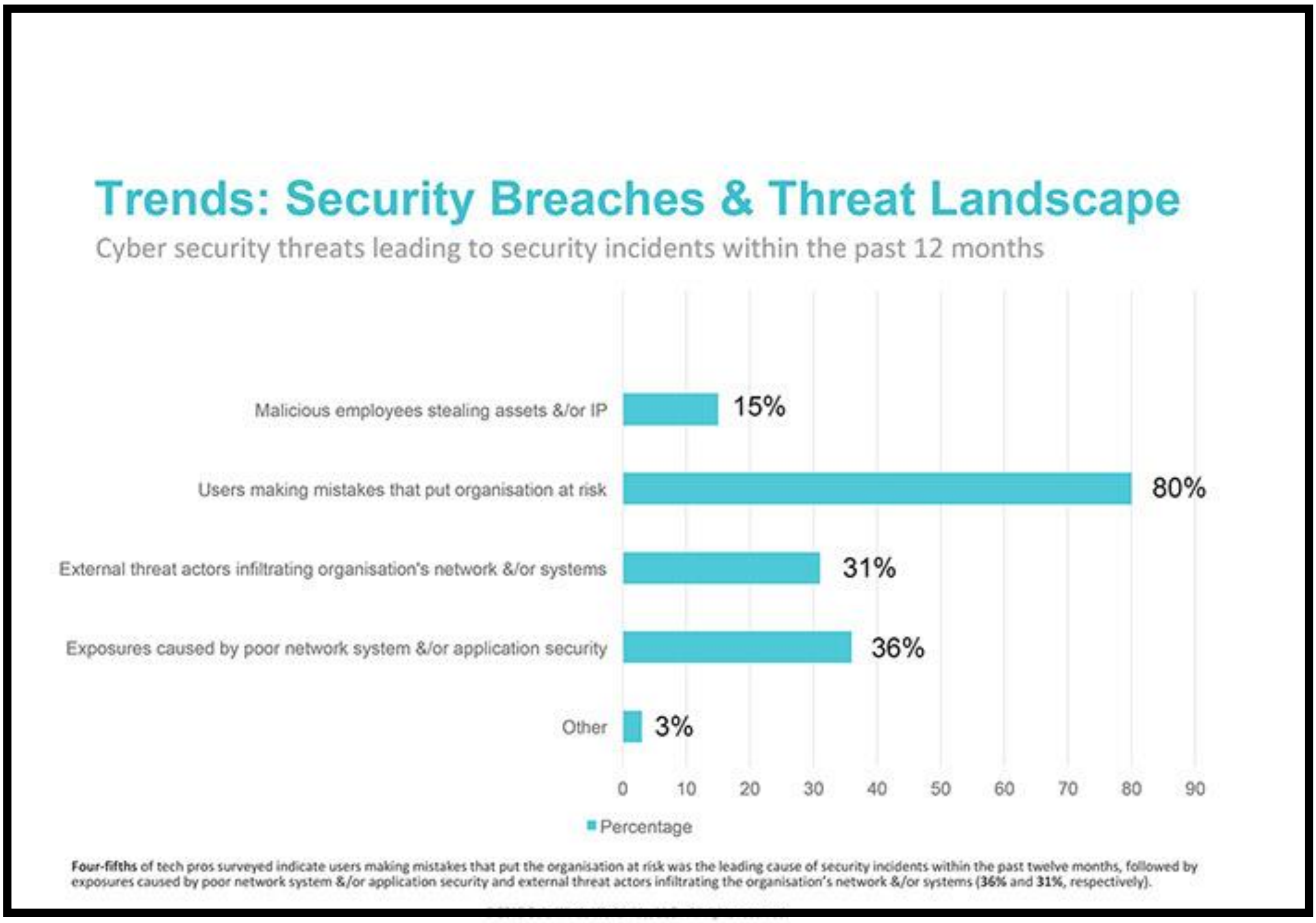

Reporting cybercrimes
Avoid damages
Improving the protection & planning
Protect the confidential data

Figure (8)

5. Are individuals from inside the company can be a threat to cyber security?

Participant 1, *“Yes there is saying: “The internal Threat is more dangerous than external.”” “We have to be protected from both external and internal. As Internal will strict policy adherence should be there. The internal user who is more vulnerable and risk to be monitored. Internal user mistakes created the largest percentage of cyber security incidents over the past twelve months (80%), followed by exposures caused by poor network system or application security (36%), and external threat actors infiltrating the organization’s network or systems (31%), Solar Winds research reveal.”*



Trends: Security Breaches & Threat Landscape

Cyber security threats leading to security incidents within the past 12 months

Four-fifths of tech pros surveyed indicate users making mistakes that put the organisation at risk was the leading cause of security incidents within the past twelve months, followed by exposures caused by poor network system &/or application security and external threat actors infiltrating the organisation's network &/or systems (**36%** and **31%**, respectively).

Figure (9) is provided by the participant 1

Participant 2, *“Yes, employees can be a reason of threats in the company. Many companies and organizations face threats or has been attacked and the reason was the inside threats. And some employees’ behavior can affect the company. Such as, if unwanted access is given to the user, weak password, unauthorized applications and others.”*

Participant 3, *“I agree that most of the attacks that an organizations face is because of human mistake or error. Whether it is intentional or unintentional humans can make mistakes the affect the security of the organization.”*

Participant 4, *“Yes, because some individual behavior can cause cyber-attacks whether it was intentionally or unintentionally.”*

Participant 5, *“Yes, but not intentionally. For example: a link was sent to some employees, so when you open the link it starts sending viruses to your entire email contact list. Another threat from individuals as using unauthorized websites.”*

Analysis

The findings in this section reaffirm the fact that individuals working within an organization can be major source of cyber security threat. Organizations must have do's and don'ts for the employees so that their actions to not expose the organizations to cyber security threats. They should understand that some sites or links when clicked could affect the whole system and make it vulnerable to external attacks.

6. Does top management should consider human behavior when designing cyber security system?

Participant 1, "Yes**,** as organizations become increasingly dependent on information technology and intellectual capital assets, the key areas of IT risk are usually seen as:

- IT infrastructure and network security (arising from concerns about hackers, terrorists, cyber-criminals, insiders, outsiders, viruses, and so on).
- Data integrity, confidentiality and privacy (arising from regulatory and market pressure around protecting personal (e.g. data protection legislation), and corporate data (e.g. fair disclosure regulations), as well as financial and operational data (e.g. Sarbanes Oxley).
- business continuity (arising from concerns about the capability to continue in business after a natural or man-made disaster);
- IT management (arising from concerns about project failure, poor IT operational performance, inadequate IT infrastructure, etc.)."

Participant 2, "yes, as since human behavior can affect the security system. Those behavior need to be considered when designing a system, moreover, top management to find ways to deal with behaviors that affects negatively on the system."

Participant 3, *"As I worked in the IT related field, I saw many errors that happened in the cyber system were from the employees, that causes gabs and weaknesses in the system. And because of that when top management should look into human's* *behavior when designing a system as they considered a vital factor of any system weaknesses or strength."*

Participant 4, *"Yes, human behavior must be their priority followed by the IT infrastructure because humans are the ones who deal with these attacks as well as the attackers."*

Participant 5, "Yes, as the human behavior can either increase or decrease cyber threats. For instance; increasing individual's awareness on cyber threats and improve human behavior on security to prevent/ reduce cyber threats. Therefore, it is really important for top management to consider human behavior when designing cyber security system as most of the cost of cyber-attacks are actually results of human error/ behavior."

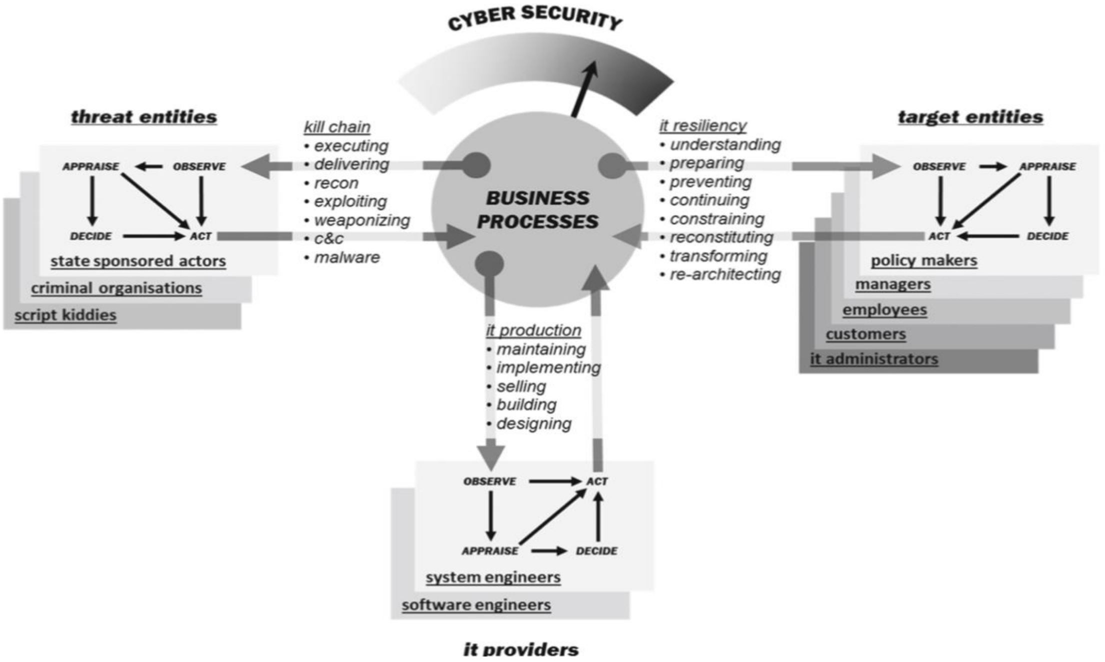
Analysis

Human behavior is crucial in designing of cyber security systems. These behave could enhance or hinder cyber threats to organizations. Human are responsible for handling the system and other related components and thus, they need to be trained and equipped with the right skills and knowledge. Every effort should be made to minimize human errors that could increase threats to cyber security as much as possible.

6 Chapter 6: discussion

The findings of this study confirm that humans play crucial role in enhancing cyber security systems. Previous studies have established that human factors can contribute either positively or negatively to an organization's cyber security. These studies all indicate that prioritizing people solutions is the best way of enhancing cyber resiliency in the contemporary society. Addressing and securing information infrastructure is no longer enough, and organizations must focus on addressing the human factors that could affect cyber security. The findings of the study also highlight the significance of investing and planning for the human components in addressing cyber security. It has also established that instilling a culture of cyber awareness and interest in an organization is crucial because of the changing nature of cyber threats. By doing so, an organization would in a better position of handling the ever-changing cyber security environment. The mindset that cyber security is only the responsibility of the IT department should not be encouraged in an organization since it is likely to expose an organization to serious threats.

A case study utilized in this paper titled 'Human behavior as an aspect of cyber security assurance' also supports the findings of this study. In this study Mark and colleagues looked at ways of reducing the rampart cyber security breaches by focusing on and addressing the human aspect of cyber security. The study



The figure (10) is from Understanding Human Factors in Cyber Security as a Dynamic System established that humans play a crucial role in ensuring cyber security within organizations. In this regard, the case study contributes positively in this study by reafirming the findings of this study and also giving it more relevance because the findings are aligned and contribute towards improving cyber security. Therefore, in summary, human beings working within an organization are important assets that organizations can utilize in enhancing their cyber security capacity. The findings herein establish and encourage the investments towards improving people skills and developing cultures that enhance cyber security. The people factor could be the weakest link as far as cyber security is concerned and thus, an organization would only be strong by having skilled and knowledgeable workforce on issues of cyber security.

7 Chapter 7: recommendation

In the end, the organization must take into consideration the human behavior and how can human acts affect the cyber security. So in order to build a healthy and strong cyber security these are some recommendation in order to help in improving and developing a strong security.

- Organization must define the term insider cyber threats and how it can influence the cyber security.
- Provide training for the employees, an orientation programs must be provided for the employees by the organizations. And Highlight what is allowed and not allowed while working in the organization. Provide them with safety tips in using different software and applications in their computers.
- The top management must discuss with them the factors that lead to cyber crimes and what actions that are required from them to handle those threats.
- Rewarding the employees who go beyond their call of duty and dedicated to their work and are trying their best in order to fight the gaps and threats that are affecting the security.
- The top management should look into framework that helps in changing and affecting the behavior of an individual, and that framework should suite the cyber security application in the organization.
- Top management should have more knowledge about the human factor framework and in how to apply it and pass it down to the employees.
- Moreover, a good working environment is a reason that could affect the insider intention and lead him to positive attitudes.

In conclusion, looking at the human factor framework one can realized that there are many organization that lack many information in how to influence human behavior and categorize them. And the lack of these knowledge lead to fault solution of human behavior. That’s why one can recommend that different framework in cyber security protection must be present and taught in the organization in all levels .

8 References

- Ajzen, I. (2012). The theory of planned behavior. *Handbook of Theories of Social Psychology: Volume 1*, vol. 211, pp. 438–459.
- Climer, S. (2019). *History of Cyber Attacks From The Morris Worm To Exactis | Mindsight*. [online] Mindsight. Available at: https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/ [Accessed 8 Dec. 2019].
- En.wikipedia.org. (2019). *Theory of planned behavior*. [online] Available at: https://en.wikipedia.org/wiki/Theory_of_planned_behavior [Accessed 8 Dec. 2019].
- Evans, Mark, et al. "Human behaviour as an aspect of cybersecurity assurance." *Security and Communication Networks* 9.17 (2016): 4667-4679.
- Fischer, E. A. (2015). Cybersecurity issues and challenges: In Brief. *Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities*, pp. 45–54.
- Houston, N. (2015). The Impact of Human Behavior on Cyber Security, pp. 403–422.
- ICAEW. (2019). Top five cyber risks, p. 2 [online].Available at: https://www.icaew.com/-/media/corporate/files/technical/business-and-financial-management/smes/bas-files/top-five-cyber-risks.ashx.
- Macmillanihe.com. (2019). *Choosing appropriate research methodologies*. [online] Available at: https://www.macmillanihe.com/studentstudyskills/page/choosing-appropriate-research-methodologies/ [Accessed 8 Dec. 2019].
- Marsh & McLennan. (2015). Cyber Risk Handbook 2015.
- National Cyber Security Centre (NCSC). (2013). Cyber Security And Risk Management - An Executive Level Responsibility, p. 8 [online].Available at: https://www.connectsmart.govt.nz/assets/NCSC-Cyber-security-risk-management-Executive.pdf.
- Qualitative research method-paper 1.pdf. (n.d.).
- Reddy, M. L. & Bhargavi, V. (2018). Cyber security attacks in banking sector: Emerging security challenges and threats. *American International Journal of Research in Humanities, Arts and Social Sciences*, vol. 21(1), pp. 65–71.
- Rosenblum, A. (2019). *What is Unpatched Software and How it Affects Businesses in 2018*. [online] NinjaRMM. Available at: https://www.ninjarmm.com/blog/it-horror-stories-why-unpatched-software-hurts-business/ [Accessed 8 Dec. 2019].
- Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A Human-Computer Interaction Approach for Usable and Effective Security. BT Technology Journal, 19(3), 122–131. doi:10.1023/A:1011902718709.
- SentinelOne. (2019). *The History of Cyber Security — Everything You Ever Wanted to Know | SentinelOne | Autonomous AI Platform*. [online] Available at: https://www.sentinelone.com/blog/history-of-cyber-security/ [Accessed 8 Dec. 2019].
- Soltanmohammadi, S., Asadi, S., Ithnin, N. & Science, C. (2013). I j c r b, pp. 329–354.
- Sphweb.bumc.bu.edu. (2019). *The Theory of Planned Behavior*. [online] Available at: http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html [Accessed 8 Dec. 2019].
- *Top Five Emerging Cybersecurity Challenges | Srini Sampalli | TEDxDalhousieU*. (n.d.).

- United States Cybersecurity Magazine. (2019). *A Brief and Incomplete History of Cybersecurity | United States Cybersecurity Magazine*. [online] Available at: https://www.uscybersecurity.net/history/ [Accessed 8 Dec. 2019].
- Vaseashta, A., Susmann, P. & Braman, E. (2014). Cyber Security – Threat Scenarios , Policy Framework and Cyber Wargames. *Cyber Security and Resilency Policy Framework*, pp. 1–10.
- Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*. Elsevier Ltd, vol. 38, pp. 97–102.
- Yue, O. C. (2003). Cyber security. *Technology in Society*, vol. 25(4), pp. 565–569.
  أراجيك