The Preparedness of SMEs for cyber risk in the United Arab Emirates

أستعداد الشركات الصغيرة والمتوسطة لمخاطر الأمن السيبراني في دولة الامارات العربية المتحدة

by

KHALID MOHAMED ALSHEHHI

A dissertation submitted in fulfilment

of the requirements for the degree of

MSc PROJECT MANAGEMENT

Prof. Halim Boussabaine

October 2017

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that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.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

Alshehhi

_____

Signature of the student

COPYRIGHT AND INFORMATION TO USERS

Abstract

The cyber security preparedness has turned into a significant element of the business over the years. Due to globalization and the latest advancements, the internet has become a common thing now. However, internet and technology come along with many risks. These risks are referred to as cyber risks. These risks are higher for small and medium sized firms as compared to large enterprises. In light of this, the study aimed at analyzing ways to reduce cyber threats and investigate different methods by which companies can protect themselves against any kind of cyber-attack.

The study was specifically focused on the SMEs operating in UAE. A mixed approach was used for collecting and analyzing the data. This mixed approach comprised of both quantitative and qualitative techniques. The survey was conducted with 103 respondents, 100 of them were asked to fill in the questionnaires while three of the respondents were directly interviewed. The tests used for analyzing quantitative data were Regression analysis, Chi-square test, and correlation coefficient. These tests were run with the help of statistical software known as SPSS. The thesis ended with giving recommendations for improving the security of networks in offices and also a suggestion for future study.

Keywords: Cyber security, Cyber Attack, SME, Online Business, Cyber Threat, SMEs Project Management, UAE Cyber Attacks

ملخص

تحول تأهب الأمن السيبراني إلى عنصر هام من الأعمال التجارية على مر السنين بسبب العولمة وأحدث التطورات، أصبح الإنترنت شيئا شائعا الآن ومع ذلك، فأن الإنترنت والتكنولوجيا تأتي جنبا إلى جنب مع العديد من المخاطر.

ويشار إلى هذه المخاطر بالمخاطر السيبرانية ، وهذه المخاطر أعلى بالنسبة للشركات الصغيرة والمتوسطة بالمقارنة مع الشركات الكبيرة ، وفي ضوء ذلك، هدفت الدراسة إلى تحليل طرق الحد من التهديدات الإلكترونية والتحقيق في الأساليب المختلفة التي يمكن للشركات من خلالها حماية نفسها من أي نوع من الهجمات الإلكترونية .

ولقد ركزت الدراسة بشكل خاص على الشركات الصغيرة والمتوسطة العاملة في دولة الإمارات العربية المتحدة. وقد استخدم نهج مختلط لجمع وتحليل البيانات ، ويتألف هذا النهج المختلط من التقنيات الكمية والنوعية على السواء. وأجريت الدراسة الاستقصائية مع 103 مستطلعين، وطلب منهم 100 لملأ الاستبيانات في حين أجريت مقابلات مباشرة مع ثلاثة من أفراد العينة. وكانت الاختبارات المستخدمة لتحليل البيانات الكمية تحليل الانحدار، واختبار مربع تشي، ومعامل الارتباط. تم تشغيل هذه الاختبارات بمساعدة البرمجيات الإحصائية المعروفة باسم SPSS ، واختتمت الرسالة بتقديم توصيات لتحسين أمن الشبكات في المكاتب، وكذلك اقتراح للدراسة في المستقبل.

Acknowledgments

In the first place, I am grateful to have had the opportunity to study at The British university in Dubai . Secondly, I would like to show my respect and admiration to Professor Halim Boussabaine , who has been an exceptional mentor and advisor to me. Not only has he guided my scholarly efforts, but he has also inspired me to succeed. His advice has been invaluable, and it is one of the main reasons for my achievement.

List of Abbreviations

SME	Small Medium Enterprise
UAE	United Arab Emirates
IT	Information technology
CSD	Cyber Security Division
R&D	Research and Development
PC	Personal Computer
IoT	Internet of Things
BYOD	Bring Your Own Device
CSOs	Civil Society Organizations
CISO	Chief Information Security Officer

Table of Contents

List of Figure

List of Tables

CHAPTER 1 INTRODUCTION

1.1 Background to SMEs Cyber Security

Small Medium Enterprise (SMEs) is noted for ease in establishing in terms of funding and legality. Likewise, the growth of the internet for conducting the business has also been seen, not only in large corporations but more significantly in small and medium size enterprises. Increased used of the internet in SMEs have become more exposed to the risk of becoming the victims of cyber crime. However, IT (information technology) has offered numerous opportunities with respect to business operations and methods for communicating, both at a domestic level and globally.

The reliance of SMEs on information technology has additionally made them powerless against the risk associated with IT as they are newer than any other kind of traditional risks. According to (Madzima, Moyo & Abdullah 2014), Small Medium Enterprises can be among the most vulnerable internet and information technology users to be attached by cyber attackers. Consequently, ensuring the safety of these companies from digital security threats and cybercrime ought to be a noteworthy focus of every small and medium sized firm, as they are more vulnerable than the multinationals.

The attacking point layouts the exploitation of vulnerability by the cyber-criminal, and for the non-malignant events, it layouts the point of failure (Etzioni 2011; Sveen, Rich & Jager 2007). Notwithstanding the exploitation of vulnerabilities within an organization's assets of information technology, an individual himself might be the point of attack using different social building strategies, (for example, phishing) to gain access to the system. There is additionally reliance on outside systems, for example, infrastructures of public internet and cloud vendors, where a cyber-crime activity may bring about the same bad results as though the crime took place inside a company's own particular self-worked system.

Figure 0.1 Spear phishing attack model use to launch targeted attacks

(Sood & Enbody 2014, p. 58)

This exhibits the requirement for suitable due determination and confirmation procedures to apply to the inventory networks of information technology, as was highlighted by Global Security Report by Trustwave, based on the findings of the year 2014, according to which 46% of the organizations who had their security system's breached preferred outsourcing their IT functions, in order to avoid any further damage (Madzima, Moyo & Abdullah 2014).

The damage caused to an organization as a result of cyber-attack can be classified into eleven different kinds, demonstrating the degree to which the threat should be managed

depending on the importance of the data and the way the security was breached. The classification of damages likewise perceives that when there is a cyber-attack on a specific company, it not only impacts the organization, but any other entity associated with the company is also impacted by the damage, such as the customers of the company, suppliers, the company's shareholders and stakeholders, the employees of the company and its competitors as well (Etzioni 2011).

The organizations ought to consider the effect of such an attack on its stakeholders, especially the suppliers and customer as these two entities play the most important part in the success of a company. Kelly (2012) highlighted that online attacks of such nature are the representation of a risk, which is growing with each passing day and has caused trouble for companies of all sizes. According to the report of an Annual Global Breach, 60% SMEs and 81% of multinationals were affected by cyber security breaches (Choras et al. 2015).

Kaur & Mustafa (2013) added that numerous decision-makers and leaders in both kinds of SMEs, and public and private, have now understood that notwithstanding, being a driver for development, efficiency, and innovation, the advanced environment likewise presents instabilities that can damage the economic and social growth of a country. Advanced security breaches can have expansive financial outcomes for a company, for instance, disturbance of operations (e.g. through disavowal of administration or harm), direct loss of finances, claims, reputational harm, loss of aggressiveness (e.g. if there was a trade secret theft), and additionally loss of trust among shareholders and accomplices, clients, shareholders, employees and suppliers (Gendron 2013).

Most of the SMEs have a misinterpretation that they are immune to these breaches of digital security. Be that as it may, according to the previous studies, this is not the case. The vast majority of these criminal acts of digital nature on SMEs incorporate spyware, framework impedance, phishing, hacking, and malware. Moreover, SMEs does not accept the fact that these attacks are harmful to their company and are negatively impacting them in all ways. The individuals, who undergo such exercises, much of the time, are benefitted from the nonattendance of sufficient efforts to establish safety taken at SMEs and are therefore ready to get to the organization's private information.

According to (Kaur & Mustafa 2013) as indicated by the Information Security Breaches Survey of the year 2014, roughly 74% of the SMEs experience the ill effects of digital security

breaks identified with the leaking of the important information by the workforce of the organization itself. A standout amongst the most famous strategies utilized by these criminals is phishing, which is utilized to trap the web clients to uncover their own points of interest and other pertinent information. Programmers utilize a fake email id which appears like an email id of a company which is legally registered (Herath & Rao 2009).

Previous data framework security research has examined such malware programs as spyware, worms and Trojan horse from a plenty of experimental points of view, and important techniques and strategies have been proposed to lighten and destroy the dangers of such attacks. Future attacks would occur because of consolidating solid cryptography with malware to target the networks for a cyber-attack. According to academic scholars (Kozik & Choras 2013) recently, the development of another type of malware on the internet, known as cryptovirus or ransomware, draws consideration among data frameworks security professionals and analysts.

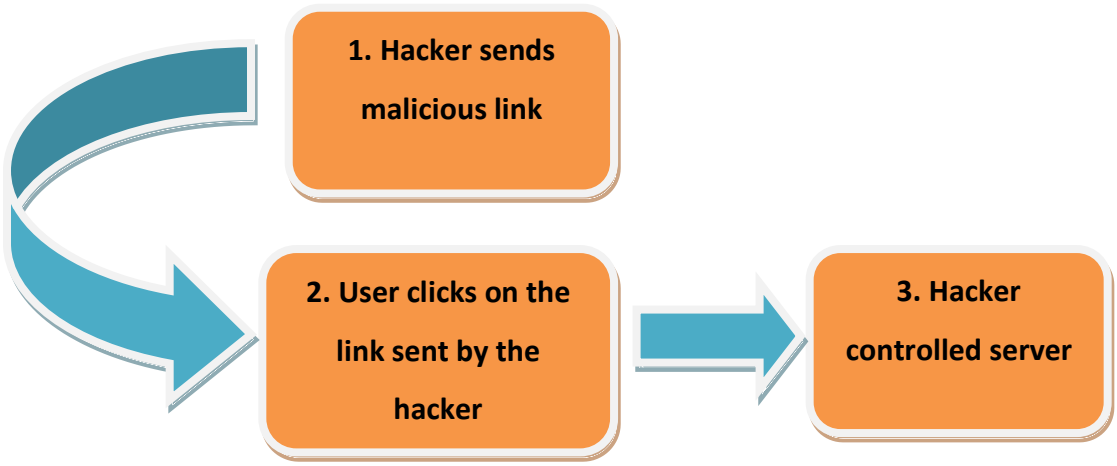

Figure 0.2 Cryptography with malware to target the networks for a cyber-attack

(Kozik & Choras 2013, p. 12)

Mallinder & Drabwell (2014) stated that as a serious danger to data resources, security, cryptovirus defrauds web clients by commandeering client documents, getting these documents encrypted and afterward requesting installment in return for the key to decrypt the documents. Looking for framework vulnerabilities, cryptovirus constantly tries to seize control over the computer or documents of the victim until the individual gives consent to the requests of the attacker, mostly by exchanging assets to the assigned online money accounts, for example,

Webmoney, eGold or by obtaining a specific measure of pharmaceutical medications from the assigned online drug stores of victims (Gupta & Hammond 2005).

An example of the most recent attack of cryptovirus is when the attackers hacked several email accounts in exchange for money from the victims. Therefore, to have an up to date, response plan for cyber-attacks and being fully prepared for a breach of cyber-security becomes a necessity and can benefit a small and medium sized companies in many ways. In case if there is a breach of system security to get to the information and finances of the company, the SME would then have the ability to respond quickly to contain a breach and minimize the monetary damages caused by a cyber-attack (Sveen, Rich & Jager, 2007). Therefore preparedness strategies are important for all business enterprises in order to counteract the impacts of malware and viruses, or hacks of any kind.

1.2 Research Problem Statement

The United Arab Emirates is considered to be one of the hubs for companies for starting their operations. This has increased the online activities of the organizations for conducting their business in the era of digitization, making them more prone to cyber-attacks. Hence, it is pivotal for SMEs to focus on safeguarding themselves from major cyber-attacks, which one a study by digital security firm Symantec reported 52.4% of the cyber-attacks on SMEs alone.

1.3 Research Questions

- What is the impact of cyber security breaches on SMEs?
- What is the current state of SMEs readiness for cybersecurity attacks?
- What steps can SMEs take for prevention of cyber security attacks?
- How can SMEs overcome information risks (inaccurate information, unauthorized people assessing wrong information and cyber-attacks)?
- Does cyber security allow SMEs to build trusted digital environment?

1.4 Hypotheses

H 1: The breaches of cyber security present negative effect on SMEs.

H 2: The organizational and operational activities are ready for the cyber security attacks.

H 3: The extra steps taken by SMEs will be useful for the prevention of cyber security attacks.

H 4: The activity of inaccurate information presents major overcoming in terms of SMEs

H 5: The activity of unauthorized people assessing wrong information present major overcoming in terms of SMEs.

H 6: The activities of cyber-attacks present major overcoming in terms of SMEs.

H 7: The trusted digital environment can be formed by allowing the protocols for cyber security.

1.5 Research Objectives

- To determine the impact of cyber security breaches on SMEs.
- To investigate the readiness state of cyber security attacks on SMEs.
- To benefits of being prepared for cyber security breaches.
- What steps can SMEs take for prevention of cyber security attacks?
- The benefits of cyber security that can allow the SMEs to build trusted digital environment.

1.6 Research Novelty

The content of this research is purely original, as the ethical and copyrighted aspects of the writing have been taken into consideration. Although there is extensive research done on the topic of cyber security breaches and its impacts, but not much literature is found on the preparedness of counteracting with these cyber threats specifically with respect to UAE. Therefore the research is original and authentic. The sources used in the paper have been properly cited with the names of the authors and the year the paper was published. The study holds great important in the field of IT and business especially for the companies that lack security measures to counteract cyber-attacks.

The following research would be helpful for SMEs that are looking for different ways and strategies to deal with the problem of cyber risks. Organizations can, therefore, take several actions to reduce the risks of cyber-attacks as would be specified in the following dissertation. For instance, SMEs can utilize secure passwords, for example, three irregular words, introducing malware programs and anti-viruses on all organization gadgets, affecting standard programming

that contain crucial security updates and instructing staff on digital dangers. Another method for enhancing security is to subscribe to the scheme of cyber essentials supported by the government itself.

1.7 Research Outline

The current section explains the research work, which is followed in a systematic and organized approach, presenting the chapters explaining make up the entire research study. In this relation, the research followed the following outline:

Chapter 1: The first chapter in this paper is the introduction to the topic of the study. The researcher has given a brief background of SMEs cyber security at the beginning of chapter 1, followed by research questions and research aim and objectives. The chapter also explains the novelty aspect of this study as the originality of any research work is the most crucial factor to consider.

Chapter 2: the Second chapter of this research study comprises of the in-depth literature review with will be shedding light on the research topic in hand, enabling to better understand the topic from different angles and facets. Additionally, research done by different scholars and researchers will be used as a source of prior research, establishing the understanding of the topic on the similar topic but from a different angle.

Chapter 3: It is followed by research methodology chapter. This chapter gives an in-depth analysis of how the research was actually conducted. Research methodology demonstrates the type of research approach used (mixed approach), the time horizon for the research which was cross sectional for this study. The chapter further explains the research philosophy used (positivism philosophy). The section of research methodology also gives the detail about the targeted population, the size of the sample used, who were the targeted respondents, and what sampling techniques were used to obtain data from these respondents. The chapter also discusses data collection methods and tools, the ethical aspect of the study and how the collected data were analyzed.

Chapter 4: Chapter 4 comprises of the findings generated from the collected data, based on the answers of the questionnaires filled by the respondents. This chapter gives the in-depth analysis and interpretations of these findings. The results were generated with the help of SPSS, a statistical tool used for analyzing collected data.

Chapter 5: The discussion chapter is aimed at developing a valid argument to understand the impact of cyber security reaches on SMEs and how well the companies are prepared against the cyber security threats. The benefits for SMEs on being prepared for cyber security breaches as well as the step that the SMEs can take to prevent cyber security attacks are also discussed. The primary motive of the chapter is to aim to discuss current state for readiness for cyber security attacks on SMEs. This chapter proposed valuable discussion for the research.

Chapter 6: The last chapter of this dissertation is the concluding chapter, which includes the conclusion, discussion, and recommendations based on the interpretations of the findings from the previous chapter. The outline of the thesis shows that this research has been formulated in a professional manner, keeping in mind all the important sections to cover. The dissertation follows a standard outline, provided by the supervisor.

CHAPTER 2 LITERATURE REVIEW

2.1 Impacts of Cyber Security Breaches on SMEs

According to (Han 2012) the impacts of cyber security breaches can be too much damaging for a company, especially if the company that the cyber criminals attack is a small or medium sized firm. The damage of such a huge caliber could be very devastating for the management of such an organization and might take years to recover from the losses caused by these damages. The breaches are very damaging for the long-term reputation of the company where any setback may result in serious threats to the company. These data and security breaches could provoke misuse of the information of an association, for instance, data that is of a sensitive nature or important details about the clients of a certain company. The breaches also create double standards of security which would ultimately give rise to malfunction of any appropriate system.

The SMEs However, (Hughes & Cybenko 2013) explained that it is usually be observed that the damages caused by a breach to a multinational corporation can be seen being highlighted by the media and news channels. However, damages caused by cyber theft and attacks to a smaller sized company is usually neglected by the media and is not reported anywhere. But in reality, as (Muegge & Craigen 2015) stated SMEs suffer greater damages, especially to the image and reputation of the company as compared to big organizations because of the impacts of a cyber-security breach. It is easier for big companies to cope up with the losses but for an SME, gaining back the old reputation would take extensive resources and effort.

2.1.1 Cyber Security

In spite of the advancements and developments in the field of IT (information and technology), and these developments can also increase the instances of various digital threats and dangers associated. According to (Payette, Anegbe, Caceres & Muegge 2015) the affirmation of structures, frameworks, and data over and through the web, security of networks and servers have turned into the principle concern for all business and firm, across all types of industries and markets, local or global. As the number of customers both current and potential have increased, along with propelled applications and data frameworks construct, so do the chances of more illegal cyber activities and threats for the companies.

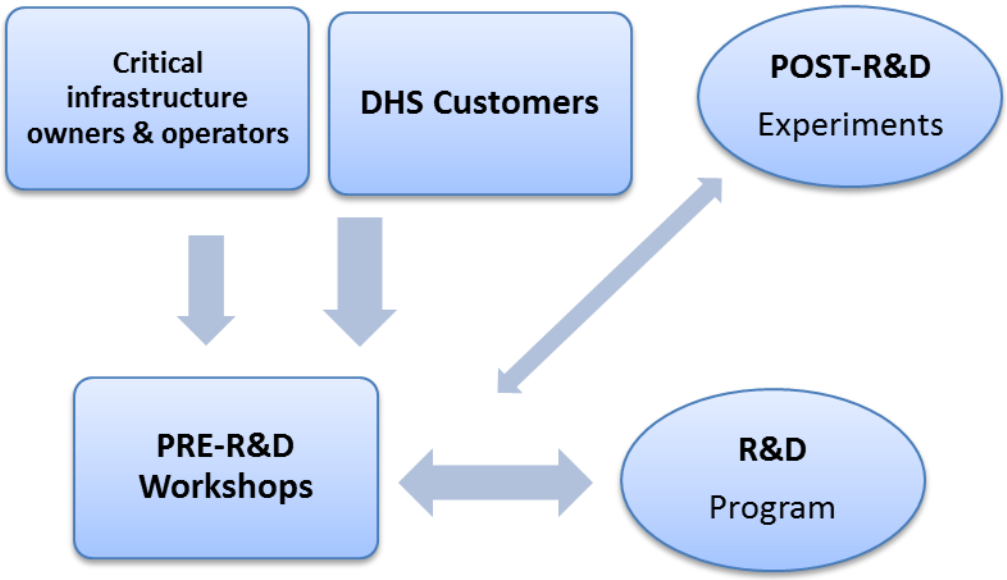

Figure 0.1 CSD's R&D Lifecycle Process

(Bailey, Miglio & Richter 2014, p 82)

Bailey, Miglio & Richter (2014) reported that the term can be characterized as the security of information advancement, which is centered on guaranteeing that the data of a firm (small or big), projects of these companies, systems, and PCs are sheltered from unapproved or unintended access, change or demolition. With the increase in volume and frequency of digital security break in, consistent efforts are required for the protection of individual and business related information and ensuring the overall national security of a country.

The risks posed by a breach in an organization's cyber security system can prove dire, especially where small and medium-sized businesses are concerned. This is because the Internet is the biggest, global 'market' available at present. Established businesses have, for the past two decades increasingly moved on to the Internet and set up their online systems. According to Seals (2015) a lot of present days SMEs were also initiated during this time period, and these were based, almost entirely and without exception on the Internet. Consequently, all their data

and daily business transactions are carried out online. A breach in data would, therefore, prove very harmful for them.

2.1.2 Role of Project Management in Cyber Security

Hughes & Cybenko (2013) indicated that organizations from all around the globe, from a wide range of commercial ventures and of all sizes are attempting to develop and implement the most appropriate methodologies for improvement, checking, and implementing a convincing anti-data break-in program and computerized security setting. Venture organization and administration theories can give the organizations structures that would act as rules keeping in mind the end goal to get the firms of all sizes through this method. Etzioni (2011) further stated that leaders are overwhelmed by most of the open "plans" that security providing firms are endeavoring to offer them, as often as possible ensuring that their thing will "100 percent" secure the establishment of an organization.

This declaration is purely misleading and incorrect; that is a stunning case. A study by Kroll in 2015 stated that there are various non-specific factors that are for the most part as major to an integrated and robust computerized security environment as the latest software of protecting computers against viruses such as Trojan horse or protecting the system with a firewall, for instance, insurances against data breaches, company policies and procedures to counteract with breaches and finally training the employees in such a way that the chances of these breaches from happening could be minimized.

Seals (2015) provided information that Intel's info security survey 2015, states that 68% of the data breaches occurring were serious enough to warrant disclosing details of the breach to the public, or were causing serious financial losses to the organization. That being the case, businesses needs to understand that each one of them is different, with their own set of risks and security threats. Therefore, there is no 'one size fits all' security solution that could deal with all businesses in general. Project management teams must assess the risks that an organization faces and then tailor a solution that would work best for the organization.

2.1.3 Types of Breaches in Cyber Security

According to Han (2012), there are numerous sorts of breaches of digital security that may truly affect the goodwill and reputation of a firm, both small and big. The types of breaches

that can be included in the list of data security breaches incorporate a staff member of a firm telling his corporate login username and password to someone who is not a part of the company that the employee is working in. Payette et al. (2015) elaborated that more types of breaches include someone trying to get unauthorized access to the information of a company, especially the data that is not for viewing of the general public. The list also includes an irresponsible employee, leaving his login username signed in before leaving the company for home.

Muegge & Craigen (2015) reported that this creates an opportunity for someone else, close by and observing the employee leaving, to come and use the company's computer to access important files and documents, especially the ones that are confidential. Hacking into a system or an organization's server is likewise a type of digital security break-in. Network security projects and systems that are highly effective and well-constructed can keep these attacks from happening. Hacking into the systems to steal information can seriously harm an organization's image.

Seals (2015) provided information that according to a survey conducted by InfoSecurity, internal threats account for nearly 43% of all data breaches. Not all threats are necessarily malicious in intent either. According to the same survey, nearly half the data breaches that were caused within an organization, by an insider, were not malicious. Such breaches would include carelessness on part of employees. The rest of these breaches could include a security leak caused by a disgruntled or fired employee; such breaches are in fact considered by most CSOs and CISOs as the sixth most frequent cause of major data leaks in an organization.

2.2 Readiness State of Cyber Security Attacks on SMEs

Miron & Muita (2014) explained that the main reason of SMEs for being less observant and prepared for any kind of cyber-attack is due to the fact that the managements of these small sized companies consider that their company is unlikely to be attacked by a cyber-criminal because of their size and lesser profits. It is usually observed that hackers mostly target bigger companies because of their size and financial performance. This fact is also known to the SMEs. This is why they pay less attention towards being ready for any kind of cyber-attack.

According to (Payette et al. 2015) organizations that are private do not have the same issues of security as do the publically-held organizations, and that they might also have pushed the issue excessively. Large companies usually have the latest technology and updated systems, therefore, they are more likely to have the best cyber security system installed within their

servers. The small and medium companies have a lack of investments and technology, lesser resources and therefore most of these SMEs do not have a proper cyber security system installed within the company's computers. Even if these companies do have some money in their accounts, they still won't invest in a cyber-security system.

2.2.1 Cyber Security Attacks on SMEs

Bailey, Miglio & Richter (2014) reported that most of the SMEs adhere to a misconception that they are safe to these digital security ruptures; however, it is the total opposite of what they believe. SMEs are usually the most vulnerable because of an absence of a proper cyber security system and are therefore have greater chances of being attacked by a cyber-criminal. The most normal sorts of events contain a greatest hits summary of computerized wrongdoing which fuses spyware, framework impedance, phishing, hacking, malware and the SMEs preventing the effects from claiming these assaults and their results. These culprits who digitally assault SMEs, as often as possible, take advantage of the lack of attention of a security staff member in order to access fragile information.

As indicated by (Choras et al. 2015) the survey of 2014 indicated that the data security breaches, including 22% of the SMEs, endured these security break-ins with respect to the mishandling of data that is sensitive and confidential, especially mishandled by the companies' own workforces. The most well-known technique utilized by these digital aggressors is phishing which is utilized to trap the web clients to uncover their own points of interest and other important information. These programmers utilize a fake email id which is made in a manner that it appears that it belongs to a renowned firm.

SMEs have been made a greater target for cyber criminals over the last two years, since 2015, than had ever been seen previously. According to a report published by cyber security firm, (Symantec 2016), stated that in December 2015 alone, almost 52.4% of all spear-phishing attacks were carried out against SMEs. November showed similarly high statistics. The reason why SMEs are becoming a target of so many attacks is because they are now being considered a 'soft target' by cyber criminals. SMEs in general, boast of a very weak cyber security system. A business that has just taken off will not have the sufficient resources, and will usually lack the relevant expertise to secure their systems against all kinds of cybercrimes.

Company Size	Aug ’16 (1 in)	Jul ’16 (1 in)
1-250	2806	2670
251-500	3982	2766
501-1000	4924	3619
1001-1500	7825	5782
1501-2500	3382	2190

Table 0.1 Email phishing by size of the organization

(Symantec 2016, p 1)

2.2.2 Impact of Cyber Security Attacks on SMEs Project Management

In the face of challenges of protection against digital attacks on company data, there is a need for project managers working for small and medium enterprises to include the stakeholder perspectives in the process of securing company’s information assets against these threats. According to (Payette et al. 2015) ventures of IT allow to securely "arrange-in" the security to the information systems especially to the components of essential basis; in this way, computerized security can and should be an essential consideration for the project management teams.

An advanced security perspective on undertaking organization improvement addresses open entryways in a structure that are known to the supervisors. According to (Muegge & Craigen 2015) notwithstanding the way that this work is shown here at an early stage and has not yet been exhibited in the field, one can genuinely assume that it begins a talk between venture administration, advanced security specialists, and suppliers of essential bases on the most capable technique to reasonably secure the systems that are fundamental for the working of SMEs. Hackers gaining access to the classified data of an undergoing project could be risky for any company especially smaller sized firms as they can sell this information to the rival company and get a substantial amount in return.

The security of the organizational data is directly connected with many sources of factors which majorly include customers and different stages of the production. The prospect or scope of the security system thus may vary from the level of customer flow in any business. The domains of protection also require extensive measure from many sources that would produce extra security for the cyber-crimes involved in the online organizational and business activities. The

role of project management has been considered as substantial in determining the extent of breaches that could occur to any business or organizational activities due to cyber-crime activities.

The strategic measures as in the case of project management are important for the effective results that are very basic for the case of a variety of approaches. The variety of approaches is important in the sense of providing security to the environment and to the overall organizational culture. The company policies and procedures are designed for treating the breaches in the most effective manner. The most common approaches are substantial for offering the company policies and regulations which guarantee the full flash training and guidance of the employees.

The impacts of Cyber Security Attacks on SMEs are extensive which specifically affect project management scope of the organization. The reason why this is such a very serious problem can be explained thus; when one considers that almost all data and business transactions for SMEs takes place online, the data is naturally stored there also. In the case of a very serious attack, sufficient data loss could occur to cause heavy financial losses to the business in question. It could compromise the personal data of clients and customers. In the case of businesses offering third-party services to other, bigger or related organizations, a breach in the first business could even compromise the security system of the client-business, leading to a potential, domino-style effect where the systems of many businesses could potentially be at risk from cyber threats.

2.2.2.1 Impact of Reputation of the Organization:

The impact of cyber security needs to be addressed in the most defined manner, where the companies are at major risks of damaging their reputation. The organizational damage is comparatively much more than the devastation of management. The management, therefore, must take important measures in controlling the outcomes and must formulate the respective strategies for the prevention of these threats. The broader the scope of prevention the easier it would be to recover from any unfortunate damage.

In May 2016, a hacker group, Anonymous conducted their operation Opicarus in which, along with banks in France, Tunisia, Philippine, Trinidad, and Tobago, the website of the Central Bank of United Arab Emirates was also compromised (Duncan 2016). Affected websites perforce stayed offline for many hours before they could be restored. That meant potential losses

of data for the banks and a loss of face in front of clients who would now consider the bank a 'weak' one. It also meant that the Central Bank's security breach affected the loyalty of customers who could potentially turn to other banks that would offer their data greater security.

2.2.2.2 Impact on Image and Long Term Stability:

The effect of the cyber-crime breach is more in small and medium sized enterprises as compared to large enterprises which have affected most of the reputation of SME businesses. It is also identified that the use of resources produces multiple effects that have increased the level of extensive protection and gain in the online business activities of the businesses. For the protection of image and long-term stability of SMEs, it is necessary to formulate and design appropriate system of security and protection that would give rise to many aspects of growth and development of the organizations.

2.2.2.3 Impact on Sense of Association and Collaboration in Other Business Entities:

The attack avoided as a means of cyber-crime protection present very long term benefits for the growth and development of any business. The introduction and the use of digital technology measures are considered to be extensive and create growing protection for the companies. The different influence on this basis may also set an exceptional influence on the business growth and development that develops a sense of association and collaboration in other business entities as well. Most of the researchers involved in the effectiveness of cyber-crime protection system have developed a basic concept about the implementation of strategic protection and security from cyber-crimes. These aspects are increasingly effective due to the prolong implementation of measures and is helping enough to the small and medium-sized entities.

2.2.2.4 Impact on Trust of Customers/Clients:

Usually, SMEs are involved in providing services directly to the end users, where they share their personal details with the organizations. Hence, in the case of the cyber-attack, the majority of the data of the customers is lost, which further leads to the financial theft to the customers. Other than just the financial losses caused, it also creates a lot of trust on the part of the customers whose data may have been stolen. This is especially true of that business which operates almost entirely on customer relations and services.

The Center for Strategic and International Studies (2013) stated that a customer whose bank account has been compromised would, upon trying to use their credit card, be informed that they cannot do so because the account has been compromised, or there has been suspicious activity from this account. In extreme cases, identity theft could also have taken place provided information that a UNODC report suggests that identity theft alone causes US $1 billion in losses globally. Such acts inconvenience customers, (unable to use their card for one thing), and leading to a lack of trust in both the organization as well as their weak security system which could so easily be breached.

Putting Malicious Cyber Activity in Context			
Criminal Action	Estimated Cost	Percent of GDP	Source
GLOBAL			
Piracy	$1 billion to $16 billion	0.008% to 0.02%	IMB
Drug Trafficking	$600 billion	5%	UNODC
Global cyber activity	$300 billion to $1 trillion	0.4% to 1.4%	Various
	US ONLY		
Car Crashes	$99 billion to $168 billion	0.7% to 1.2%	CDC, AAA
Pilferage	$70 billion to $280 billion	0.5% to 2%	NRF
US- cyber activity	$24 billion to $120 billion	0.2% to 0.8%	Various

Table 0.2 Putting Malicious Cyber Activity in Context

(Center for Strategic and International Studies 2013, p. 5)

2.2.2.5 Current Readiness of SMEs in UAE against Cyber Security Attacks

According to (Jhon 2015), the digital attacks as of late in the United Arab Emirates (UAE) have displayed a reasonable movement in the method for advanced wrongdoing, particularly for SMEs. Clearly, programmers are becoming better, more experienced and more dangerous in their activities. Digital security assaults have transformed into a tremendous, globe-crossing industry including a blend of exceedingly capable, complex software engineers and

criminal personalities that can strike any company of their choice sitting far away from the location of that company.

Kroll (2015) reports of cyber-attacks on the data of SMEs, specifically the data breach of smaller banks in the United Arab Emirates demonstrate the potentially destroying results of such arranged assaults. The proximity and advancement of threats infers that computerized security and administration of digital danger has now transformed into an imperative working issue for the companies situated in the United Arab Emirates especially the ones that are smaller in size as the risk is greater for them as compared to the risk faced by the bigger organizations (Choras et al. 2015). It is crucial that these small sized firms must broaden their perspective regarding the security of their data and information resources and start thinking beyond the average basic security measures.

2.3 Benefits of Being Prepared For Cyber Security Breaches

According to (Miron & Muita 2014) having a redesigned, digital attack counteract program and being completely ready for an attack on the digital security can benefit an organization which is smaller in size from multiple points of view. In light of the steps taken by a small or a medium sized company, if there ought to be an event of a cyber-attack on the framework security, the organization would have the ability to make snappy move to contain a break-in and minimize the damages associated with its financial data and money stored in the accounts of the company.

In addition, being prepared can save around 154 dirhams for every record that has been illegally accessed by an unauthorized source as claimed by (Kaur & Mustafa 2013). This in itself can minimize the unsettling influence of the business elements of an organization and upgrade its ability to stay centered and to prosper. A study by (Jhon 2015) explained that a company smaller in size will upgrade its chances of meeting the pertinent real requirements for making a helpful move in containing the cyber-attack and avoiding any kinds of damages associated with the attack that could turn out to be unreasonable for the company. The developments of an ability to consider a contingency plan, and improving it, can boost the capacity of a company to successfully manage a cyber-attack.

2.3.1 Initiatives for SMEs in UAE to be prepared for Cyber Security

Under the law of UAE called the Law of the Commercial Companies, team member for the management of a company subsequent to being brought to the nation for getting jobs in

UAE, are supposed to be presented towards an individual promise of not misusing the power that would be bestowed upon them by the company that they will be working for and by the government of UAE (Kaur & Mustafa 2013). As they are foreigners within the country, they would have to be extra careful with the rules and regulations of the company in order to guarantee the protection of company's information that is entrusted in their hands. There is a general rule relating to the commitments set out in the UAE Civil Code as well, giving that a man is at danger for 'damage bringing on acts' as stated by (Jhon 2015).

In case an association perseveres through damages as a result of a data or digital assault, and the assault is credited to blunder or a wrongful exhibition by an employee, then he could be held responsible for the damages. The key investigation would select the facts that would constitute a wrongful exhibit without clear principles in the law in regards to what level of data innovation and persistence or security certifications associations are required to stay aware of.

2.3.2 Common Cyber Security Breaches in UAE's SMEs

Quigley, Burns & Stallard (2015) explained that the computerized security and breaches into these systems is transforming into a growing problem for the SMEs of the United Arab Emirates, especially the ones in Dubai, with a review revealing that one-third of the firms inside the nation have been reporting advanced security cracks in the past one year. The giant addition in the use of online portion and e-organizations, despite the wide openness of unprotected mobile phones, has encouraged computerized guilty parties to target customers with phishing and malware assaults impacting an extensive variety of contraptions (Muegge & Craigen 2015).

Money is a prime factor, especially when the programmer is really taking cover behind the screen of the laptop and the odds of being arrested are negligible. The possibility of having access to the money of a company with almost no risk of being caught motivates various programmers to take creates fake identities and become inclined towards hacking into the systems of these companies to access financial data. According to (Thekkepat 2016) breach of the budgetary information of banks of smaller sizes has turned out to be exceptionally regular in UAE for as far back as 24 months.

2.3.2.1 Emerging Cyber Security Risks in UAE

Small and medium sized organizations are likewise thought to be a more serious danger of getting affected by the cyber-attack in a way which is not good for the company. Hughes &

Cybenko 2013) explained this mirrors the conviction that these small sized firms are more defenseless against such crimes and do not have a well-planned counteractive plan for dealing with this issue like other bigger companies, that are well established and have a proper security network. Then again, except for those dealing with inventive advancements, most smaller companies are viewed as less inclined to experience the ill effects of misfortunes associated with the theft of intellectual property and the damaged reputation, as they do not have much to lose. However, avoiding such events to take place is still essential, no matter what the size of the company is (Muegge & Craigen 2015). Cyber risks can be clustered in human risks, network risks, and physical risks.

Over two million people were made victims of cybercrime in 2015 in the UAE alone. This has been accredited as being a rise of nearly 23% from 2014. Duncan (2016) in his article highlighted that according to Norton by Symantec, nearly one-fifth of UAE residents became victims of cybercrimes in the previous year, and on average, lost up to 30 hours in efforts to try and fix an incident caused by cybercrime. They also lost an average amount of DH 2331. The three most common types of cybercrime activities taking place in the region are hack-activism, (when attacks are launched because attacker holds a different ideology), to destabilize an organization and for financial benefits.

2.3.2.1.1 Human risks:

These risks include the damages done to the workforce of the company because of the breach. For instance, if the company finds out that the breach was caused because of an employee's irresponsibility, he/she might have to face dire consequences, depending on the damage done. The breaches are very common as this may affect the entire performance of the workforce. The cyber breaches tend to create a network of illustrations for the personal actions that may further regulate the basis of damages and threats to the business activities and regulations. Most of the risks involved produce damaging consequences to the overall organizational performance of the company where the mainstream functions are affected the most.

2.3.2.1.2 Network risks:

The companies usually are inter-connected through networking, if in any case a cyber-attack is faced by the organization it can severely damage the functioning of a company's network by affecting it with a strong virus or malware. The network risks are substantial where

the collaboration among the employees and customers get affected the most. The risks at the individual level may produce alarming results but the network risks are very extensive and common in the online business or organizational activities that immensely affect the organizational effectiveness.

This is because most organizations have now moved on to the networking model of communication at the inter-departmental level within an organization. There are many benefits to networking. For instance, a file uploaded onto the organizational network will then easily be available to every user who is using a computer system shared on the same network. However, this also means that if a malware were, for instance, to affect a single PC, it could potentially, using that same route, also affect all the other computers on the network causing an immense loss of data for the organization.

2.3.2.1.3 Physical risks:

These risks are associated with the damages done to the physical assets and property of the company such as laptops and mobile phones. The damages in terms of physical prospect pose much damage that financially affects the overall performance of the company. The physical risks actually tend to crash the whole system and functional aspects of the company. The cyber-crime for this prospect is various where the damage to the software and hardware is considered to be very common in the businesses.

2.3.2.2 Insecure Passwords and Software Risks:

The online business activities must be secured with the help of protected password. The activities are majorly affected by stolen password or software configurations which result in overall devastation of the organizational system. The overall organizational dimension is strictly affected by means of this risk for which companies are required to set up a system of privacy and control in all the business activities.

The element of ‘too trusting’ in a business environment and especially if you have a networking system set up within an organization. Since nearly half of cyber-criminal activities turn out to be insider jobs, is it really essential to allow every employee within the organization to be able to access every single file and folder uploaded in the network? A better alternative would be to protect sensitive data by ensuring it is password protected. That way, even in the case of a breach in security, accessing a sensitive file without a password would be impossible hence making the organization’s data more secure.

2.3.3 Benefits of Cyber Security

Bailey, Miglio & Richter (2014) reported that there are numerous advantages of actualizing a digital security arrangement inside an organization. Advanced security guarantees the insurance of frameworks, PCs, and data from unapproved access. It involves improving information security and business intelligibility organization. Computerized security further improves accomplice trust in the information security game-plans made by the firms. It similarly enhances association accreditations with the right security controls set up (Choras et al. 2015).

In the event of a disturbance, recuperation time turns out to be quicker because of a legitimate digital security arrangement. Regardless, a couple of associations require a more hoisted measure of programming confirmation than others keeping in mind the end goal to accomplish these advantages, particularly the associations that are not so big in size as indicated by (Thekkepat 2016).

These small sized firms can consider including an application boycotting program as an approach to keep unapproved applications from running on corporate computers and servers. This kind of plan licenses the customers of cyber security providing companies to make a list of undertakings that are allowed to run on the computers of the company, and all others would be denied access automatically by the system. This would accordingly ensure the safety of confidential and classified files and documents of the company.

2.4 SMEs cyber risks mitigating strategies

The small and medium-sized companies must implement within their management strategies both business congruity arrangement and a mitigating arrangement for the cyber-attacks on their company's servers and computer systems. Furthermore, (Miron & Muita 2014) stated that a crisis management team must be set up to deal with a potential break-in with the digital security system of a company. In this connection, these measures incorporate a free IT quantifiable expert to make sense of it all and help the company to deal with all kinds of cyber threats and also help the company to deal with the damages caused when the attack actually happens.

The senior management of the SME can, in like manner, educate on the best course of action to take in order to diminish potential threats or any adversity concerning the sort of data and security breach. The plans should in like manner convey procedures in association with telling administrative forces and controllers what to do in such a circumstance, passing on

remotely to media, clients et cetera, recognizing all crucial honest to goodness necessities and managing any sorts of potential mischief that could cause damage to the positive image of an organization.

2.4.1 Cyber Security Prevention Measures

A very important aspect regarding the SMEs of UAE is concerned with minimizing their threat by preventive measures. Jhon (2015) emphasized that in order to keep the company away from operational loss and keeping the corporate data safe from the outside sources, progressive directors need to tail some vital standards that are to be followed within the company by all employees. To eliminate threats throughout the organization, security must reach past the IT office.

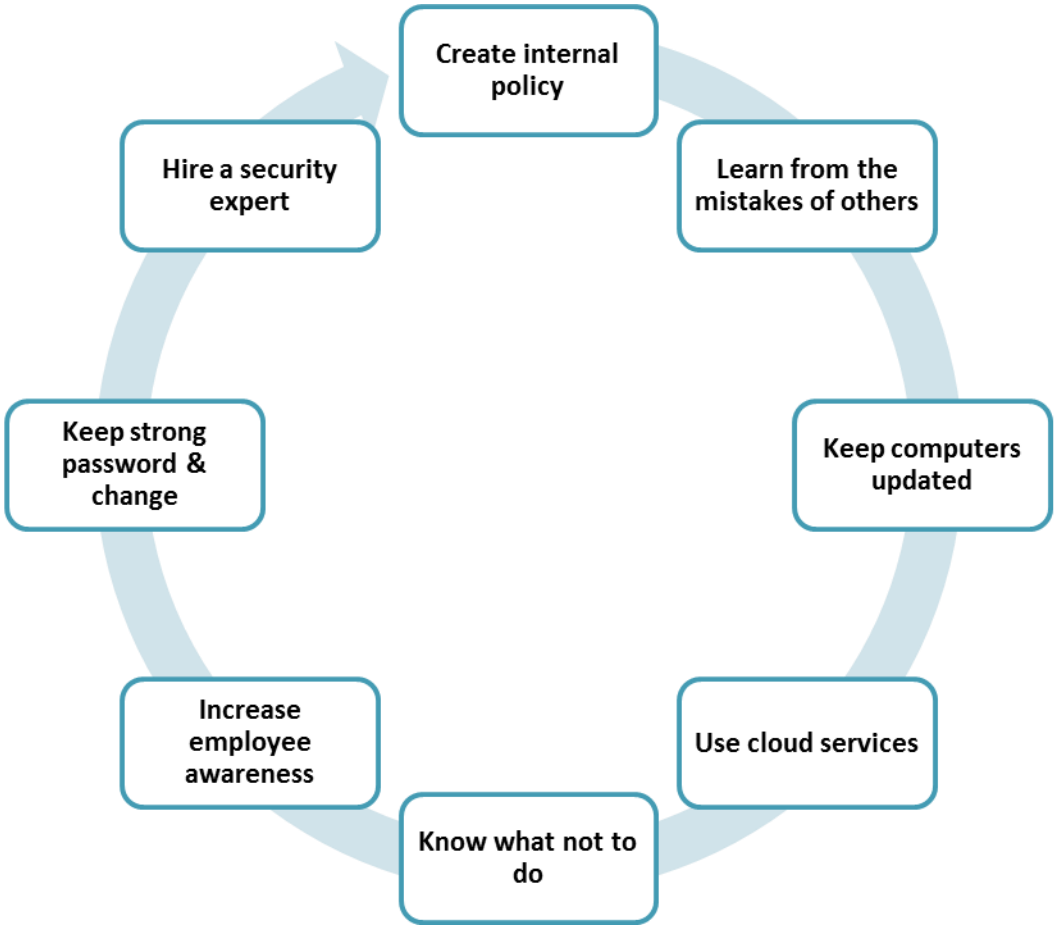

Figure 0.2 Preventive Measures for Cyber Security

(Sood & Enbody 2014, p. 15)

Thekkepat (2016) likewise suggested that an association must evaluate the way out systems of its workforce, remote undertaking tradition, on-and off-site data stockpiling homes and the sky is the point of confinement from that point onwards. The small and medium-sized companies of UAE should then develop and maintain new game plans and technique and physical shields fitting to the disclosures. The associations must ensure that the same models for data security are associated paying little regard to the department, by outfitting flexible masters with clear courses of action and strategy, ensuring security and confirmation writing computer programs is presented on phones and with the most recent overhaul, and giving adequate specialized backing and preparing particularly for the workforce that is dependably a mobile workforce.

2.4.2 Corrective Measure for Cyber Security

According to (Mallinder & Drabwell 2014), theft of essential online information of organizations includes the theft of electronic assets, credit and debit card information of customers and employees, authorized development, wholesale misrepresentation, and a huge gathering of other negative results. Stealing of data online or advanced digital misconduct greatly influences the individuals, organizations and government components. Break-ins into the servers and networks of a company are routinely executed by the poorly trained workforce, ex-staff members, sorted out programmers or cyber criminals, and remote gatherings of government bolstered mystery exercises. While government orders are driving organizations to address consistency exercises, the securities of various data assets has seen limited change and require restorative measures (Gendron 2013; Hughes & Cybenko 2013).

One of the most important steps that must be taken before any organization may put corrective measures in place is to recognize the threats that the said organization faces. According to Northcutt (2016) considering how this is the age of BYOD and IoT, it is essential for the complete security of its data that a business recognizes how these two trends could potentially put the entire organization as well as its cyber security at risk. Appropriate measures, such as making an inventory of the devices that are coming to the workplace, the software even that could be accessed while there, securing configurations for the various software and hardware, setting up malware defenses and constantly assessing and correcting risks would help make the organization’s cyberspace more secure.

Preventative	Detective	Corrective	Compensatory
Security awareness training	System monitoring	OS upgrade	Backup generator
Firewall	IDS	Backup data restoral	Hot site
Anti-virus	Anti-virus	Anti-virus	Server isolation
Security; y guard	Motion detector	Vulnerability mitigation	
IPS	IPS		

Table 0.3 Preventative, Detective, Corrective, and Compensatory

(Northcutt 2016, p. 1)

Various organizations, both small sized and bigger ones, are doing combating subtly having been deceived by information robbery and are attempting to understand the potential results and systems towards recovering from the damages caused by cyber-attacks. The security provided to the systems and servers help these organizations to recognize risks to authorized and sensitive data assets through the development of the fundamental measures to neutralize these threats or respond to computerized wrongdoing and the stealing of important information of the company.

2.4.3 Steps for SMEs in UAE

Thekkepat (2016) reported that companies that are small or medium in size, situated in UAE, must take a perfect chance to set up the profiles and records of the workforce of the company including the upper management, which would offer unmistakable levels of access dependent upon the parts that they play with the firm. For instance, lower level employees should be denied access to the data which is only for the upper management to be accessed and can, therefore, be logged in by a manager or any other executive from the upper management. Some people may require a more broad extent of access.

However, others ought not to need to interface with certain sensitive data (Kaur & Mustafa 2013). This practice can promise that only the people who are concerned with certain types of information are able to access it instead of allowing the information to run wild all

through the system. SMEs should similarly look into the matter of developing security measures for the internet organizing locales and web indexes, for example, Bing, Yahoo or Google. A few associations follow the strategy in which specialists are allowed only a particular measure of time to utilize corporate framework resource for unwinding practices like delight purposes or looking at their profiles on Facebook or Twitter.

2.4.4 List of Risk Strategies

With the help of a comprehensive analysis and finding from previous researchers, the following four risk strategies can be considered important to avoid cyber-attacks and coping up with its after effects.

2.4.4.1 Administrative rights restrictions:

The company must restrict the administrative rights of an employee for using applications and the database of the company. The use of databases must be limited to few persons who will ultimately secure the flow or identification of different measures taken by the company in restrict of cyber-crime activities. According to (Mallinder & Drabwell 2014), the restriction on access is considered to be one of the most substantial and legitimate measure in avoiding the prospect of cyber-crime activities. The measure is highly effective and regulating in the proper functioning of businesses and provides a long-term stability and growth to the company.

It limits the need for an organization's employees to know more about sensitive data to a more need-to-know basis. As a result of this, the risks involved with disgruntled employees leaking, or mishandling sensitive data is minimized. Another related option is allowing only the relevant employees access to only those parts of a file or data that is relevant to their sphere of work. Doing so allows data to be more secure because this means that even a breach in one part of a file or data will not mean a loss of all the data as a whole.

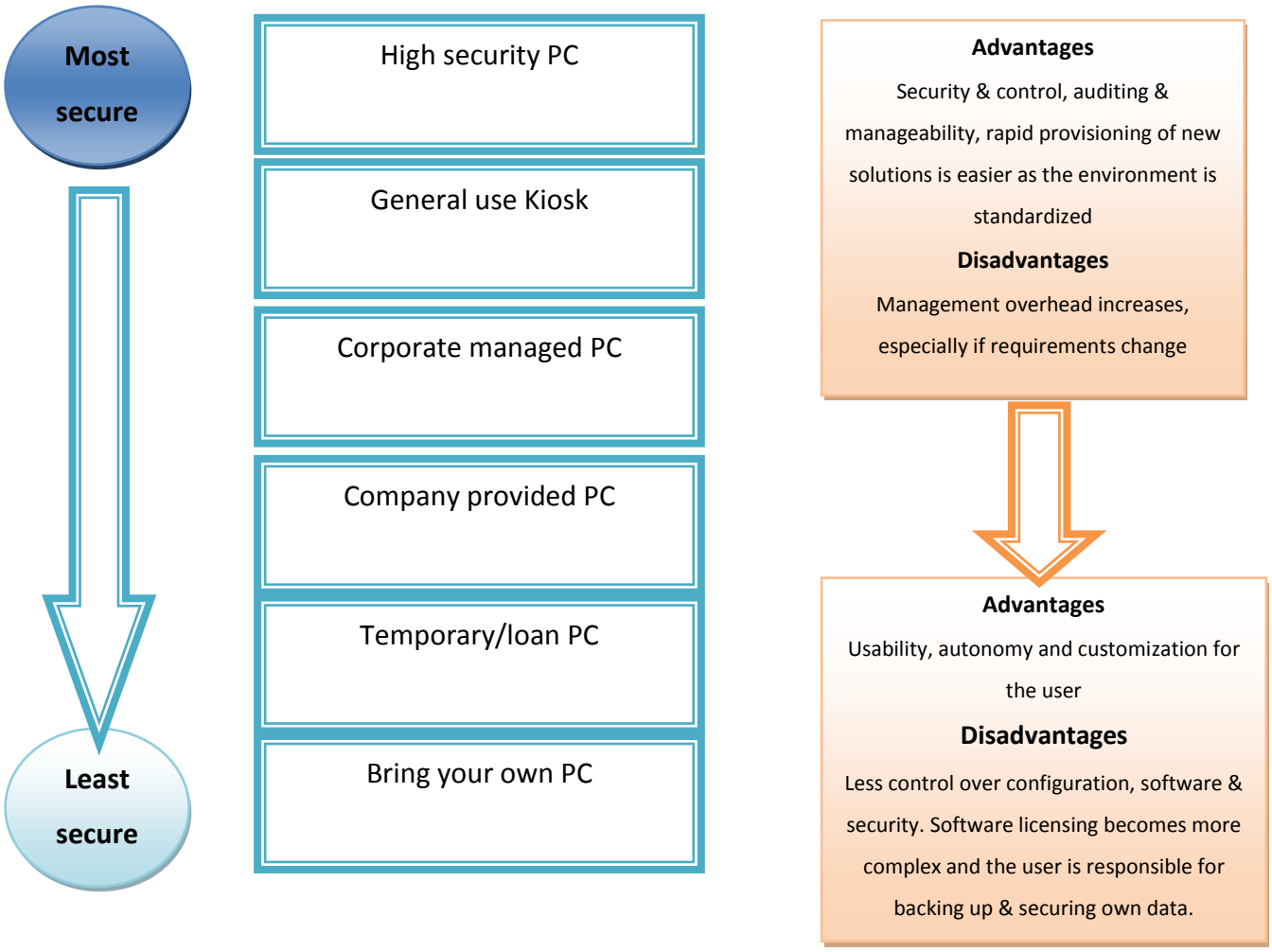

Figure 0.3 Mitigating the use of Local Admin

(Mallinder & Drabwell 2014, p.18)

2.4.4.2 Patching Applications:

Patching of applications like Microsoft office, web browsers, flash PDF viewer and Java. The software is prone to be affected by these cyber-crime activities that ultimately result in a decline of overall organizational performance. For this reason, the effective measures are important in setting the organizational effectiveness by securing the software applications that are extensively used in the overall organizational activities.

2.4.4.3 Patching operating system vulnerabilities:

The operation systems are exclusive that turn out to present many threats for the business activities. Jhon (2015) emphasized that the secured layouts must be formulated in order to diagnose the problems in the first place. The operational activities are particularly considered to be very important and functional in terms of providing stability to the day to day functions. All this require a great deal of consistency and control over presenting guidelines and protocols that are suitable for the organizational performance.

2.4.4.4 Whitelisting:

To prevent unapproved programs and malicious software from running, the company must use application whitelisting (Thekkepat 2016). The whitelisting is a very common procedure used nowadays for preventing the company from any suspicious activities. The activities are therefore recorded to be based on the level of unapproved programs that generate some defined measures or actions for function. The functional prospect of any activity is then recorded and measured for devising the appropriate action plan in general.

2.4.4.5 Cloud Computing:

There are three basic clouds computing, where each involved different types of assets, IaaS, PaaS, and SaaS. However, each type possesses different risks and benefits, it is essential for the SME to identify its need and then select the cloud computing type. Moreover, this gives SMEs liberty to choose the users. Additionally, these are considered to be “pay as you go”, making it cost effective for they are able to avoid upfront investments in hardware, IT experts, and software.

The risks involved with cloud computing, however, continue to exist. No matter which cloud computing option an organization may choose to buy, this will be a third party organization that will be providing the cloud services. An organization may theoretically speak, set up own cloud platform which would naturally be very secure. However, for any SME it would also be a very costly initiative which would, therefore, make it unfeasible.

Hiring cloud services means that an organization other than the host organization (SME) will be allowed access to sensitive company data. This could include employee records and personal details, and details of business deals, transactions, and strategies. Such information if

leaked could have different impacts depending on which sector an SME, whose data has been compromised, belongs to.

However, financial, data and maybe even loss of business, as details of one's business strategies become public surface are unavoidable. Research suggests that most CSOs, CISOs, and Project Management teams are more worried about utilizing cloud services than the actual risks involved; warrant they should be (Thekkepat, 2016). However, this does not detract from the fact that cloud computing means putting the most sensitive of an organization's data in the hands of a complete stranger. The best way to reduce risks involved is to research how and where data will be stored by the service provider before buying a cloud-based service.

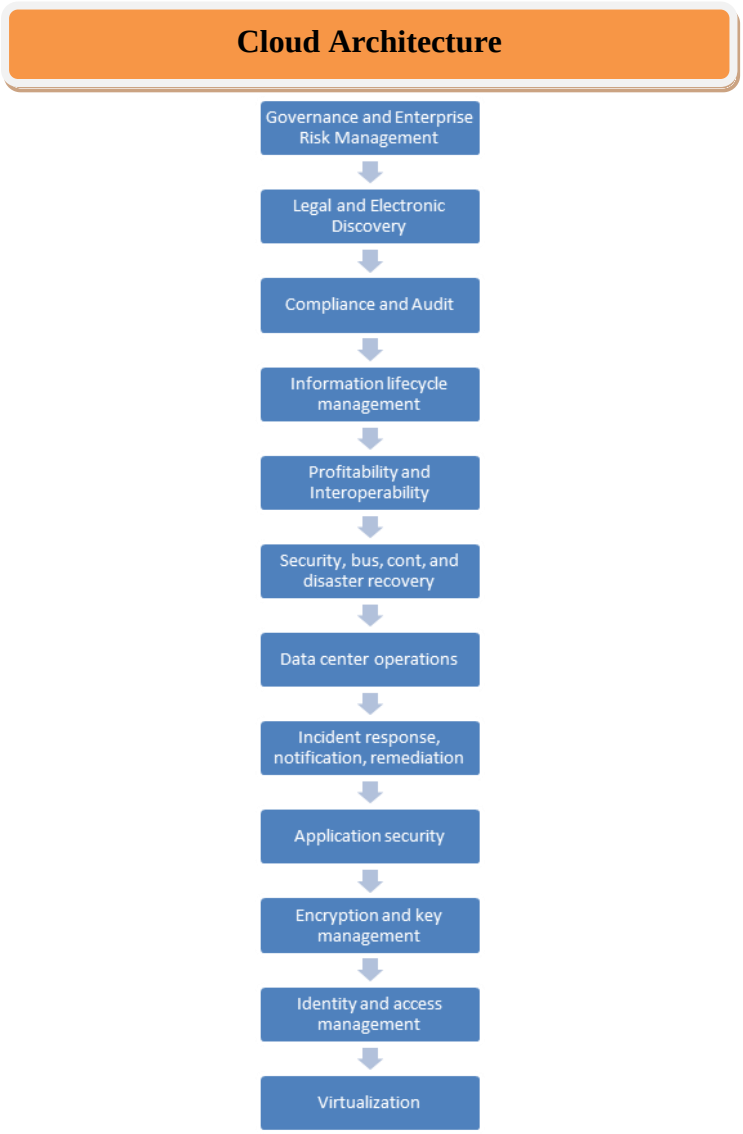

Figure 0.4 Cloud Architecture Diagram

(Thekkepat 2016, p. 49)

The process of risk management is required to be given high priority, thus must be maintained at all levels. The strategic development plan of risk management must be formulated for each department with respect to every online activity and action. The general outcomes in terms of prevention demonstrate the basic outlines where the specific outlay should be designed in the first place. The process must remain the same for each kind of threat. It must vary from the intensity of the threat, where the specific collaboration must be required for the management and the workforce. The threat management strategies are required to be updated on the monthly or quarterly basis by means of receiving the updates from the workers.

2.5 Benefits of Cyber Security

Rahman, Martí & Srivastava (2011) in their study elucidated that a compelling digital security structure can guarantee assurance in an electronic circumstance, yet the information that is used to advance security attempts contain singular information that in any occasion most spectators would see as private. Computerized security systems can be a strategy for avoiding undesired assembling and surveillance of essential and delicate information from the servers of an organization. Regardless, when concentrated on potential wellsprings of these digital dangers and assaults, (Kadivar 2014) explained that such preventive measures can in like manner be profitable to affect the overall security of the entire digital working of a company such as its online data, financial information, customer details and important files and folders.

Besides, the viewing of information stream inside a structure can be a part of the basic section of advanced security as it aids in keeping an eye on the information that leaves the framework, monitoring all the online working, and even keep tabs on which information in being added to the servers. This would help in identifying whether the altered data was added by the employee or an outside source. Alterations like these can severely damage the working of a system, therefore, cyber security is essential to ensure the safety of digital networks.

2.5.1 Trusted Digital Environment

According to (Han 2012), the development of a trusted computerized environment deduces that providers of login ids and passwords, suppliers of internet data usage and online clients could connect with each other on the web, in a secured and clear way. Starting in the not

so distant past, an ideal approach to performing this would have been for application providers to consolidate the different login plans, offered by the particular ID-suppliers, on a planned reason.

Kadivar (2014) indicated that the sheer time and resources required working up and staying aware of this setup in a split second sheds it as a down to earth game plan. Besides, this kind of technique does not incorporate the need for quality control, settlement and security. What is required is a sheltered stage that could likewise allow clients to connect with each other in a secured framework.

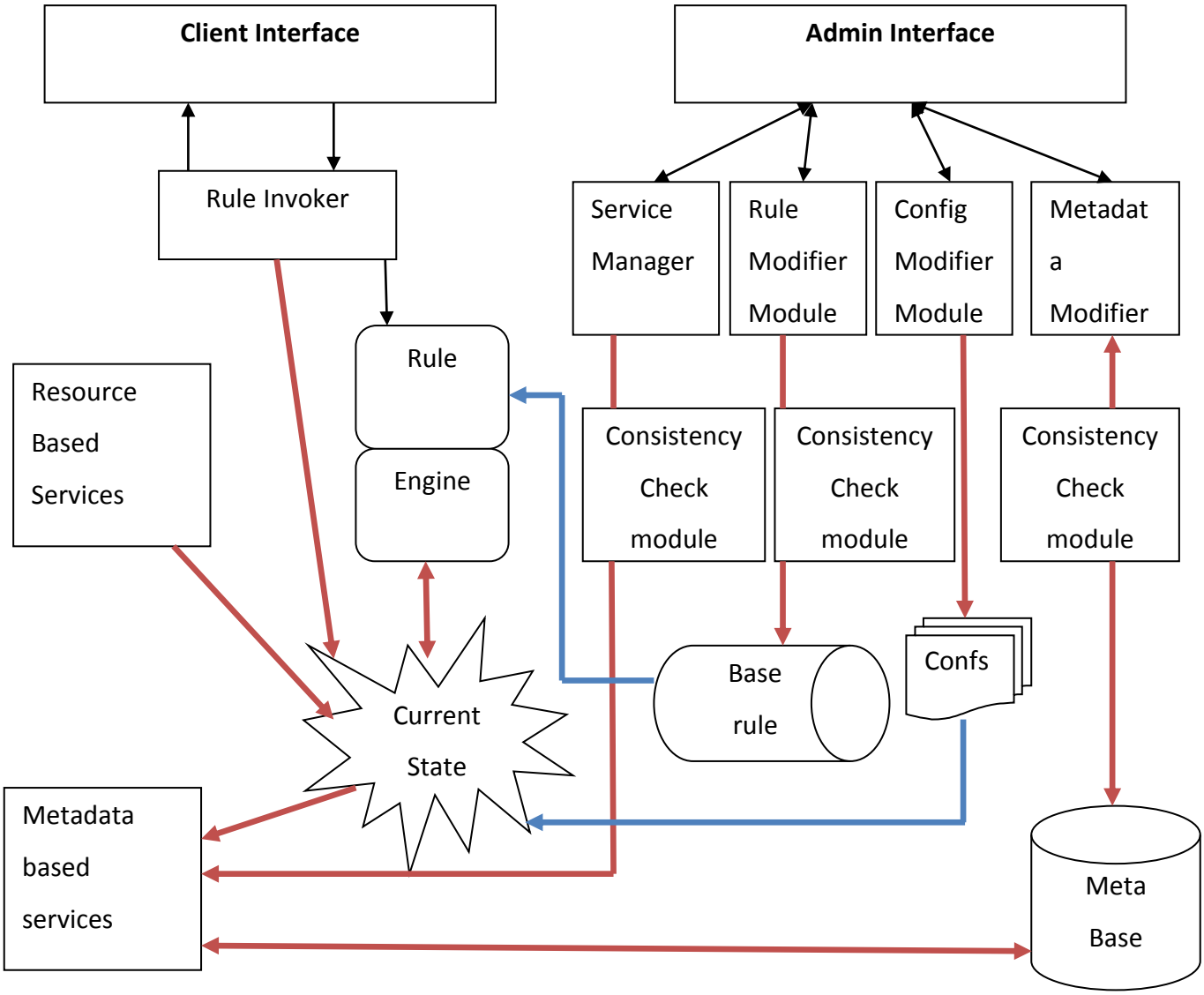

Figure 0.5 iRODS rule-based data management system architecture

(Kadivar 2014, p. 7)

According to (Madzima, Moyo & Abdullah 2014) access to this stage should be secured with easy to use, two-component affirmation convenience, for instance, a flexible application to deliver a password that is safe and cannot be hacked easily. Passwords must be created in such a way that they contain a combination of characters, digits, and alphabets in order to make it difficult for the hackers to hack into the computers by decrypting the passwords of the user ids of company's employees.

2.5.2 Requirements for SMEs to Build Trusted Digital Environments

For the SMEs of today, particularly the ones that are situated in UAE, it is imperative for them to furnish the workforce of their companies with a trusted computerized environment. The risk of digital assaults has expanded throughout the years, expanding the worries of numerous workers particularly concerning their own information and monetary data. The organizations need to ensure that they actualize digital security frameworks inside the organizations keeping in mind the end goal to ensure the insurance of information of the workers inside these organizations.

Rahman, Martí & Srivastava (2011) further explained that the prerequisite of building trusted advanced situations have expanded with an expansion in the framework of bring-your-own-device (BYOD). These frameworks ensure that the information of the worker is protected from any unapproved access or some other type of information break-in. Henceforth, the criticalness of such situations is apparent for organizations, particularly organizations that are not big in size as the danger is near all the more damaging for SMEs when contrasted with greater organizations. The threat of a cyber-attack is not a myth but a reality that is to be taken seriously. The working of the company depends on the environment that is provided to its employees, an environment that the employees can trust on especially with respect to their data.

2.5.3 Benefits of Project Management Approach

There are a number of ways for the methodology of project management can decrease the basic threats of digital assaults on gigantic endeavors for both the bigger and small sized firms. These frameworks are suitable for neutralizing the problem of cyber threats and cyber crimes. According to (Mallinder & Drabwell 2014), the same method can be used over and over as a part

of the business procedure, with lessons learned in the past used for modifying the methodology as time goes on.

Ville (2011) stated that the technology is changing at a great pace each day and with this change, the hackers are becoming even more skilled and dangerous. Therefore, modifications to the security systems are essential from time to time. While it is nearly impossible any large-scale project will ever be able to develop 100% secure environment, having a well-planned procedure for going through the whole venture and keeping it safe from outside threats would make the system less prone to these attacks. Consequently, these methodologies of project management are not just vital for dealing with the activities of the organization yet it is additionally vital for keeping the task and ventures that are under process, secured against digital assaults and breaches of important company information.

CHAPTER 3 RESEARCH METHODOLOGY

The research methodology section of the research provides necessary information regarding research tools and analysis methods. The methodology chapter clearly describes how the study was conducted. The methodology section also communicates the rationale for choosing a particular research method.

This chapter discusses the methodology chosen for this research project. The methodology section includes the research approach, sources of data collection, data analysis method, and ethical consideration. The methodology chapter also communicates the research philosophy, time horizon, sample size, and sampling method used in this research study.

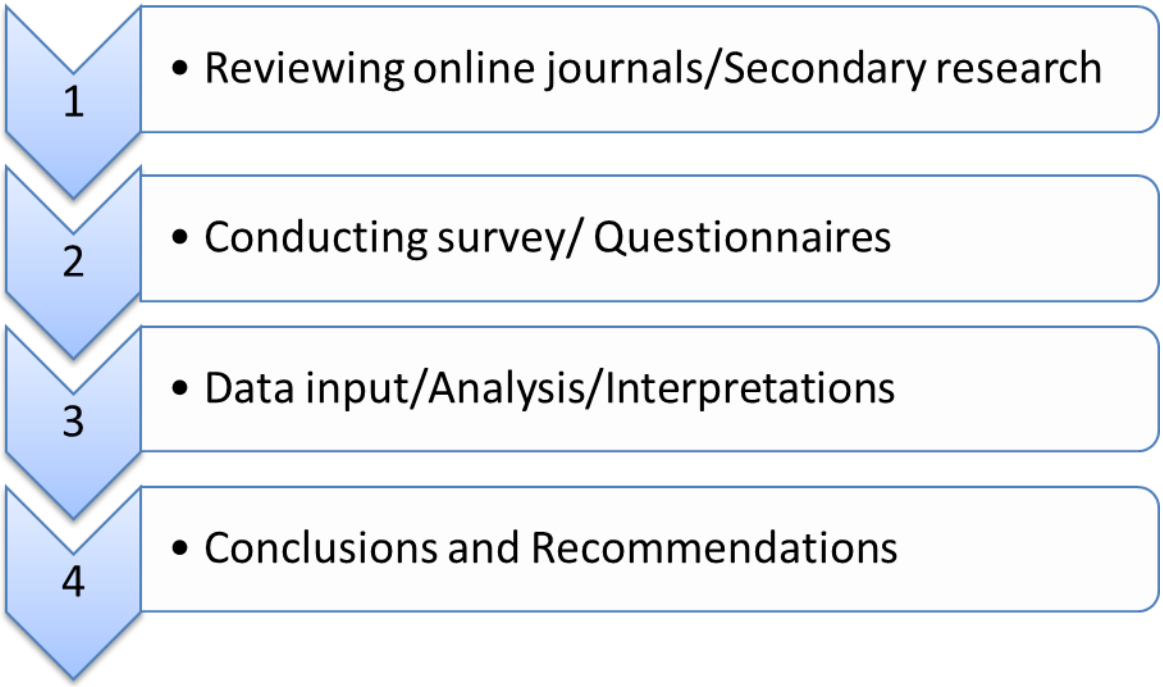

Figure 0.1 Methodology of Research

(Zikmund 2003, p. 12)

3.1 Research Approach

The research approach used for this study is a mixed approach which includes both qualitative and quantitative analysis techniques. The utilization of a combination research methodology allowed the researcher to utilize the benefits of both quantitative and qualitative research. According to Zikmund (2003), the qualitative approach allows an in-depth understanding of a subject's fundamental principles. The qualitative research approach focuses

mainly on the motivations and opinions of the research subjects. It can be used to gain an insight into the issue at hand. It is also helpful in the development of hypotheses or ideas prior to the commencement of quantitative research. Sekaran (2003) highlighted that qualitative research is helpful in revealing of philosophies, opinions, and thoughts. It focuses on being more subjective than being figurative and usually does not consist of any kind of statistical information. Alternatively, the aim of this approach is to get to the basis of ideologies. It is a method that is mostly used in literature analysis.

However, it can also be useful in sociological studies, historical review, investigations of behavior and personality and ethical experiments. In contrast, the quantitative research approach has no association with hard data as stated by (Zikmund 2003). This approach is used in quantifying, investigating and using statistical analysis on the data collected. However, the quantitative research is not at all restricted to mathematics only. In fact, the quantitative research has many different types. Although opinions, behaviors, and attitudes are naturally subjective, they can also be quantitatively compared for the production of results. In the majority of the cases, a quantitative research approach involves drawing a sample from a large population pool or from a sizeable section of study subjects.

Zikmund (2003) states that by blending together both qualitative and quantitative research approaches, the researchers of a study are able to gain expansiveness and profundity of comprehension and authentication. As indicated by Teddlie & Tashakkori (2009), effective triangulation requires careful examination of the data obtained through each technique, including its weakness and strengths. According to Sekaran (2003), a mixed approach is considered a pragmatic approach to research.

3.2 Research Philosophy

Research philosophy is defined as the approach used to develop knowledge through research investigation. In other words, research paradigm describes the way in which the researcher undertakes a study in order to generate findings.

This research is based on the positivist philosophy in which the researcher generates scientific knowledge through the use of different scientific methods, such as data collection through structured interviews. When using this research philosophy, the researcher stays detached from the members of research. This allows the researchers to remain emotionally neutral. As stated by Bryman (2012), the positivist approach is suitable for this research because

it is an organized research approach. Creswell (2005) has described positivist research methodology as an approach that is based on gathering data and making interpretations by using objective approach. The use of positivist approach is appropriate because it helps in predicting cause-and-effect relationships based on facts and reasoning.

3.3 Time Horizon

The time horizons for a research are basically of two kinds, longitudinal and cross-sectional. This study is a cross-sectional study according to the requirements of the research. This means that the data was collected only once within a defined time period. According to Sekaran (2003), cross-sectional study is a data examining tool used to obtain at a particular point in time. The information assembled was gathered from a pool of members with variable qualities and demographics known as variables. Income, location, education, gender, age, and ethnicity are all examples of variables. The demographics or variables, utilized as a part of a solitary study depend on the kind of examination being directed and on what the study means to demonstrate or accept.

Bryman (2012) further elaborated that the exploration discoveries evacuate suspicions and supplant them with genuine information on the particular variables considered amid the time frame represented in the cross-sectional study. This kind of study is utilized crosswise over different commercial ventures. These commercial ventures incorporate sociology, retail, marketing, psychology, religion, education and government. In each of these commercial ventures, cross-sectional exploration gives vital information that illuminates a wide range of activities. Sekaran (2003) stated that this instrument is utilized to take in more about different demographics with the end goal of breaking down target markets to offer to or present services and products of a company.

Teddlie & Tashakkori (2009) explained that a longitudinal research is an interconnected research involving observations of the variables that are the same but repeated over a period of time, usually many decades. This type of time-specific research is usually employed in sociology for the study of life events throughout generations or lifetime, and also in psychology, for the study of developing trends across the life span. The reason behind this is that in contrast to the cross-sectional research, in which there is a comparison of different members bearing the same

personalities, the longitudinal research usually studies the same members so there are not many cultural differences observed in them across their generations.

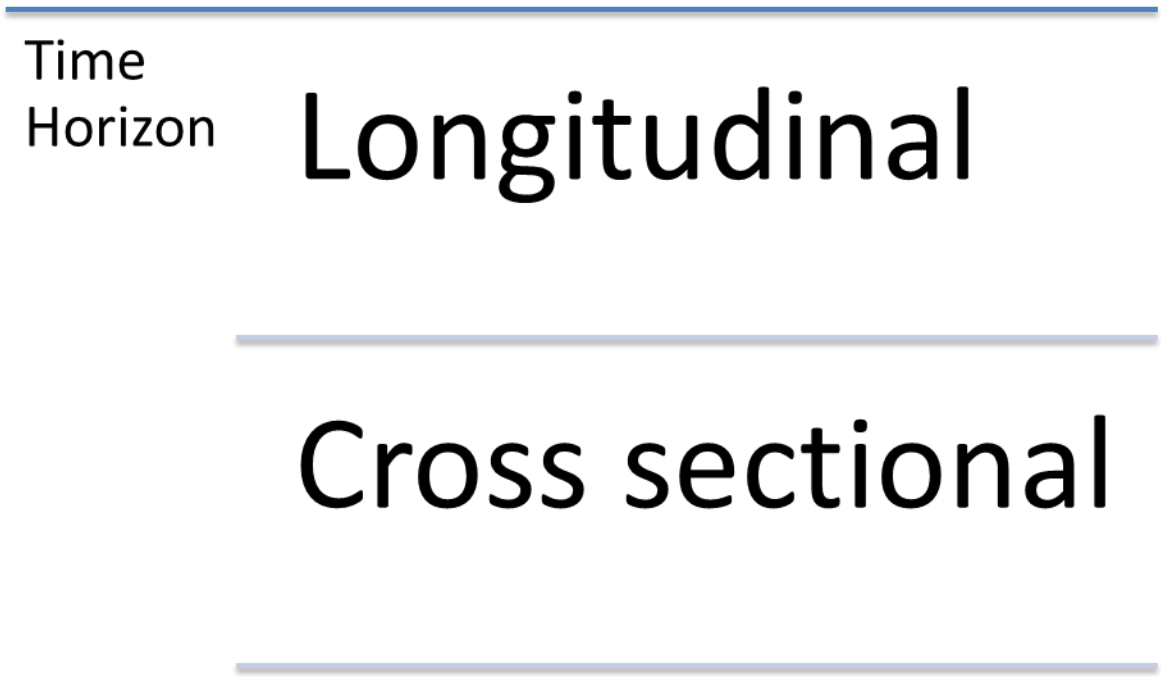

Figure 0.2 Time Horizon

(Teddlie & Tashakkori 2009, p. 14)

Thus, the observing changes are made even more accurate by the longitudinal research that is also used in many different fields. Some of the disadvantages of this type of research include the fact that the longitudinal research requires a lot of time, effort, and money. Therefore, this study is not very appropriate. The advantage of longitudinal research, on the other hand, is that the changes or developments in the features of targeted members at both levels either individually or group-wise, are easily detected by the researchers. An essential feature of this type of research is that they extend in time beyond a single moment, thus, establishing a series of events.

3.4 Research Population

Research population is defined as a group of people with same characteristics. According to Neuman (2013), research population can also be defined as the total number of people who are

the center of focus in a research. The population chosen for this study includes employees associated with SMEs in the UAE.

3.5 Sampling Technique and Size

The sampling technique that is used in this research is simple random sampling. The chosen sample size for the research comprises of a sample of 100 respondents. For this sampling method, every individual from the populace has an equivalent possibility of being chosen as the subject for the research. The probability sampling approach is selected because it results in reducing sampling bias. The chances of sampling bias in probability sampling, therefore, are lower than chances in non-probability sampling. The probability sampling technique consists of various sampling methods, which allows researchers to select participants who represent the entire population. The benefit of utilizing probability sampling has also been highlighted by Saunders, Lewis & Thornhill (2012). According to the researchers, probability sampling method is most appropriate when the population of the research is large.

The entire process of sampling is conducted in a way that allows each and every subject of the population to be chosen anonymously. Neuman (2013) elaborated that the best aspect of this technique is the simplicity of collecting the respondents for the sample. It is additionally considered as a reasonable method for selecting respondents from a given populace since each part is given equivalent chance of being chosen. Another key element of this sampling technique is its representativeness of the populace.

On the off chance that the sample is not representative of the populace, it is considered the error of sampling. An impartial irregular choice and a delegate test are essential in making determinations from the consequences of a study. One of the objectives of exploration is to have the capacity to make conclusions relating to the populace from the outcomes of a chosen sample. Saunders, Lewis & Thornhill (2012) highlighted that due to the representativeness of the chosen sample acquired by this technique, it produces valid and reliable research study results.

3.6 Sources of Data Collection

The information was collected from two main sources of data which are the primary sources and the secondary sources. The primary data sources are the sources which are original and are collected firsthand. According to Teddlie & Tashakkori (2009), they include the direct proof or the immediate testimony that concerns the topics under examination. Original

information is presented by the primary sources that are neither condensed nor interpreted by other writers.

For instance, an independence declaration speech that has been addressed by a famous politician would obviously be a secondary source for a scholar who is studying the philosophical basis of the document. However, it would be a primary source of research for a person who is studying how the meaning of the declaration had changed over a period of time. Some examples of primary research sources are photographs, newspaper articles, fiction, music, poems, data, manuscripts, experimental results and trial transcripts.

On the other hand (Bryman 2012), secondary sources are termed as the analysis or the interpretations that are derived from the primary data. They are helpful in explaining the primary research sources and are usually used for the supporting a particular argument or thesis, or convincing the reader to believe a specific perception. Examples of secondary sources include monographs, biographies, encyclopedias, and journal articles, works of interpretation and criticism and dissertations.

In addition to the questionnaire, this research also involves the use of interviews for data collection. The interviews have been conducted with three employees working in different small and medium-sized organizations.

3.7 Data Collection Method and Tool

The data was collected with the help of a semi-structured questionnaire. This questionnaire comprised of questions that were relevant to the topic and helped the researcher approach the research in a meaningful and objective manner. The data was also collected through face to face interviews with three of the employees chosen from different SMEs.

3.8Analysis

The data that obtained from the chosen sample was analyzed with the help of SPSS program. Based on the interpretations and results of the tests, recommendations and conclusions are further given.

3.9 Ethical Considerations

Primary research is a common type of research that is utilized in a wide array of fields and research disciplines. According to Creswell & Clark (2011), when conducting a professional or

academic research, one needs to be aware of the ethical considerations affecting the overall research process. Ethics comprise of the procedures, perspectives or values that guide the behavior and actions in complex moral issues and problems. Following are some of the considerations from an ethical perspective that need to be followed by researchers:

- Permission must be sought from the people who are to be studied in the research study that involves them.
- Not all research types need permissions. For instance, if the person who is conducting the research is interested in the analysis of something publicly available, like public messages commercials, etc., the participant's permission is not necessarily required.
- Another necessary ethical consideration involves the difference between subjectivity and objectivity. This simply means that the researcher has to be extremely careful with the selection of words for difficult or sensitive questions during the interviews.
- Various research types like observations or surveys should be administered under the condition that all the findings would be kept anonymous. However, there are certain types of interviews that could not be done keeping the subject's identity hidden. Thus, it is the duty of the researcher to let his subjects know whether the results of his research would be with a hidden identity or not.
- The researcher must assure the study respondents that no advantage is being taken. This is especially valid for a group of people who can be accessed easily such as children and the sick. Therefore, the subjects should be chosen on the basis of what would be the most beneficial for the research.
- There should be fairness in the distribution that means the participants should be selected equitably.
- Many research types that are conducted in universities usually require an approval from the Institutional Board. This means that the review committee of Ethics approves the research and ensures that there is no violation of any of the considerations mentioned above.
- The researchers should ensure that whatever they are representing is accurate and they have carefully expressed what they observed during the research study. The responses of the interviews should not be out of the context.

While conducting the different steps of the research, special consideration was given to the ethical aspect of this research. The respondents were first taken permission from before conducting the research study. People who did not wish to participate in the research were not forced into doing so. Only the individuals who were willing to contribute to the study were asked to fill the questionnaires.

3.10 Conclusion

In order to conduct this research study, mixed research methodology is used, which is a combination of qualitative and quantitative research approaches. Mixed research methodology has been used for this research because it is reliable and objective. This research methodology is free from personal bias. It also allows researchers to gather data from a large population. The use of this research approach greatly assisted the research investigator in determining the impact of cyber security breaches on SMEs in UAE. The use of quantitative data ensured a high degree of representativeness while qualitative data analysis resulted in providing a subjective view of the topic. The combination of quantitative and qualitative research methods led to better understanding and depiction of research outcomes.

CHAPTER 4 DATA ANALYSIS

The choice of data analysis methods depends on the type of data used. In quantitative research, different strategies are used for testing hypothesis including correlational, experimental, and general statistical methodologies. In correlational research, the relationship between variables is studied. In experimental research, the population is subjected to intervention and the impact of the intervention on the population is studied. The statistical methods involve the use of statistics techniques for the purpose of data analysis.

The methods used for analyzing qualitative research include grounded theory, case study, and narrative analysis. Grounded theory is the method of qualitative data analysis in which a theory is developed to explain the main concern of population and how the concern is resolved. In the case of study research, an empirical inquiry is carried out in order to investigate the phenomenon in the real life. In the narrative analysis, stories interviews, autobiographies, and other narratives are used to analyze data.

The aim of this research is to determine the impact of cyber security breaches in the UAE. In this research, quantitative research methodology has been used to utilize statistical techniques to analyze data. The population of this research consists of employees associated with SMEs in the UAE. The sample size consists of 100 employees working in different small and medium-sized businesses in the UAE. In order to gather quantitative data, a Likert-scale questionnaire was designed consisting of twelve items. Data was analyzed with the help of reliability analysis, correlation, chi-square, and regression.

In addition to quantitative data analysis, this research also involves qualitative analysis of interview questions. The interviews were administered on three respondents working in different small and medium-sized organizations. One of the participants was an administrative manager working in an SME. The second respondent was an IT manager and the third respondent was the owner of an SME.

4.1 Analysis of the Questionnaire

For the purpose of analyzing questionnaire, charts have been used. In order to find a relationship between variables, correlation analysis has been used. The relationship between cyber security crimes and SMEs has been studied with the help of correlation analysis. The respondents filled 150 questionnaires.

Question 1

Do you think small and medium enterprises feel secure behind their envisioned cover of irrelevance and humble business?

The first question of the questionnaire asked participants about the security of small and medium enterprises regarding their security. The responses of participants are as follow:

Strongly Disagree	**10**
Disagree	18
Neutral	27
Agree	23
Strongly Agree	22
Total	100

Table 0.1 Security of Small and Medium Enterprises Regarding Their Security

The above table shows the responses of participants in related to the first question. According to the responses, there were 10 participants who selected strongly disagree, 18 selected disagree, 27 selected neutral, 23 selected agree, and 22 selected strongly agree. These comments show that a majority of participants were neutral in response to this question. This highlights a lack of awareness among employees regarding the security of small businesses. The number of respondents who disagreed was higher than those who agreed.

This shows that a majority of participants disagreed that small and medium-sized enterprises feel secure.

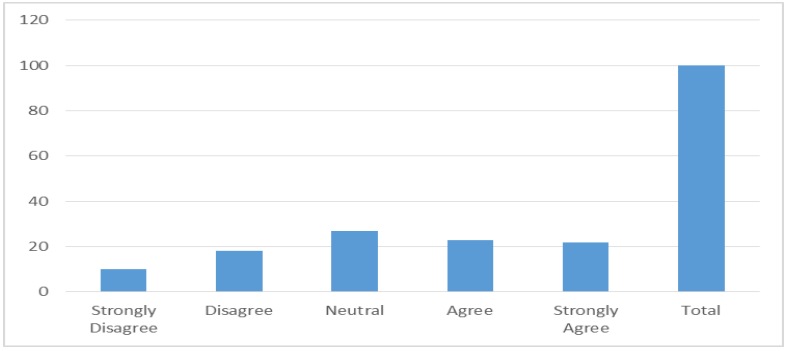

Figure 0.1 Security of Small and Medium Enterprises Regarding Their Security

Question 2:

Small and medium-sized enterprises frequently utilized method for access to their bigger accomplices and suppliers by these cyber criminals

Strongly Disagree	**14**
Disagree	11
Neutral	15
Agree	38
Strongly Agree	22
Total	100

Table 0.2 Frequently Utilized Methods to Getting Access to Bigger Accomplices and Supplier

In the next question, participants were asked about frequently utilized methods to get access to bigger accomplices and suppliers. There were 14 participants who strongly disagreed, 11 participants disagreed, and 15 participants remained neutral. On the other side, 38 respondents agreed and 22 strongly agreed. According to these responses, a majority of respondents agreed that small and medium sized enterprises use methods to get access to bigger accomplices and suppliers.

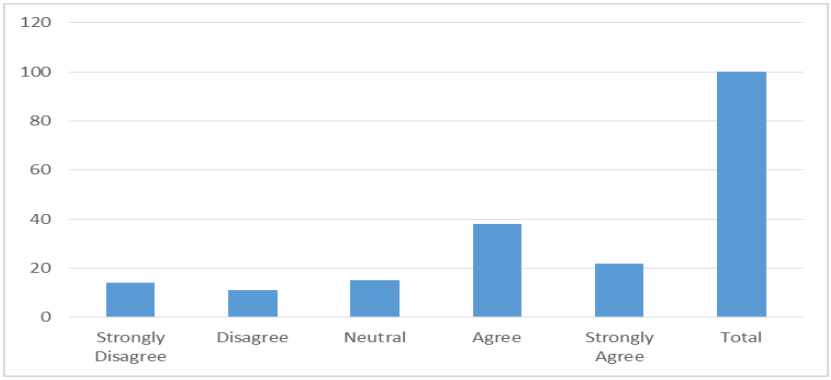

Figure 0.2 Frequently Utilized Methods to Getting Access to Bigger Accomplices and Supplier

Question 3:

Are you sure executing crisis measures and possibly advising the customers of the company?

Strongly Disagree	**6**
Disagree	17
Neutral	29
Agree	33
Strongly Agree	15
Total	100

Table 0.3 Crisis Measures Used By Small and Medium Sized Enterprises

The next question was related to crisis measures used by small and medium-sized enterprises. The participants were asked about the use of crisis measures for preventing cyber crime. There were 6 respondents who strongly disagreed and 17 disagreed with this statement. There were 29 neutral respondents. On the other side, there were 33 respondents who agreed and 15 respondents who strongly agreed. The responses show that a majority of respondents agree with the use of crisis measures in SMEs. However, there were 29 respondents who were neutral. This shows that these respondents might not be aware of the use of crisis measures by their respective organization.

The neutral response could also be because of a lack of awareness among respondents regarding crisis measures. There were 23 respondents who disagreed with the use of crisis measures. This shows that there are many SMEs where the awareness of employees regarding crisis measures is limited. Moreover, there are also organizations where employees are aware of crisis measures but their organizations are not using these measures to prevent cyber crime. The indication of the use of security measures by 48 respondents shows that security measures are being utilized in a few organizations. On the other side, the lack of awareness and the disagreement of employees show that small and medium-sized enterprises need to be aware of the importance of crisis measures. In the case of any cybercrime, the managers of small and

medium-sized organizations need to be aware of steps that need to be taken to prevent cybercrime.

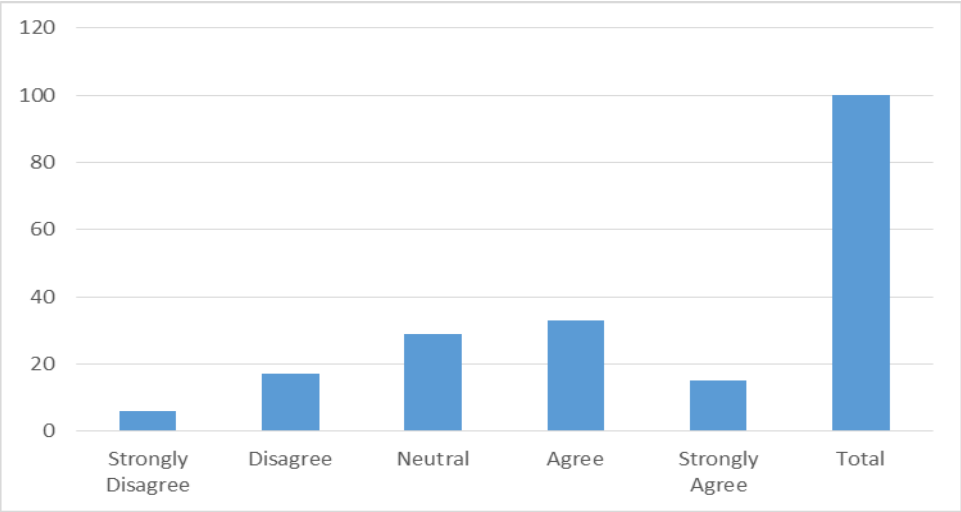

Figure 0.3 Crisis Measures Used By Small and Medium Sized Enterprises

Question 4:

Do you think cybercrime has significant risks?

The fourth question aimed to investigate participants about their perception of risks involved in cyber crime. The variables included in this question include the perception of risk and cyber crime. The aim of this question is to identify risks associated with cybercrime. The below responses show how participants perceive the risks of cybercrime.

Strongly Disagree	**7**
Disagree	19
Neutral	21
Agree	31
Strongly Agree	22
Total	100

Table 0.4 Perception of Risks Involved In Cybercrime

There were 7 respondents who strongly disagreed, 19 disagreed, and 21 remained neutral. There were 31 respondents who agreed and 22 strongly disagreed. According to the responses, a majority of respondents agreed that significant risks are associated with cybercrime. However, the neutral response of 21 respondents who that they are not aware of the risks associated with cybercrime. The lack of awareness is a reason that prevents small and medium sized organizations to utilize strategies that result in preventing cyber security risks. The awareness of 53 employees shows that there are some small and medium-sized organizations that are aware of security risks associated with cybercrime.

When small and medium-sized organizations are aware of security risks, they are likely to use security measures to prevent cyber crime. Moreover, the use of reactive measures to deal with cyber crime also depends on the awareness of small and medium sized organizations. The awareness of employees is an important factor because when employees are aware, they can promote the use of security measures to prevent cyber crime.

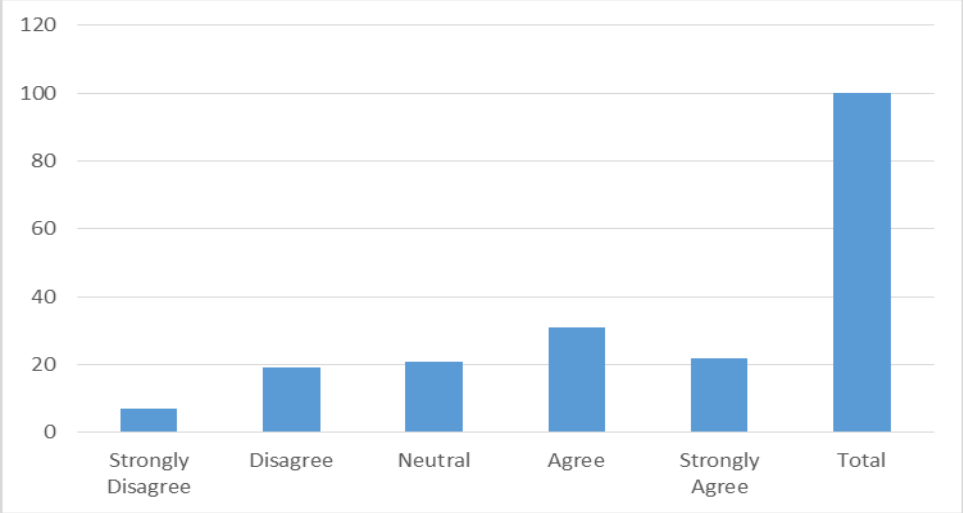

Figure 0.4 Perception of Risks Involved In Cybercrime

Question 5:

Do you think that there is a severe sense of unpreparedness in small businesses?

The next question aims to determine the perception of participants regarding the unpreparedness of small businesses. The participants were asked if they think that small businesses have a severe sense of unpreparedness. The below table shows the responses of participants:

Strongly Disagree	**8**
Disagree	13
Neutral	24
Agree	38
Strongly Agree	17
Total	100

Table 0.5 Unpreparedness of Small Businesses

According to the table, there were 8 respondents who strongly disagreed, 13 disagreed and 24 remained neutral. There were 38 respondents who agreed and 17 strongly agreed. There were 55 respondents who believe that there is a severe sense of unpreparedness in small businesses. The findings reveal that a majority of participants believe that small and medium-sized enterprises are not prepared to deal with security threats. The lack of preparedness is a serious threat for SMEs. It is because a lack of preparedness will make SMEs vulnerable to security threats. If SMEs are not prepared enough to deal with security threats, they will experience huge cost in case of any cyber-attack. The preparedness of SMEs can save the time required to deal with security threats. Moreover, it can also save cost required to deal with cyber-attacks.

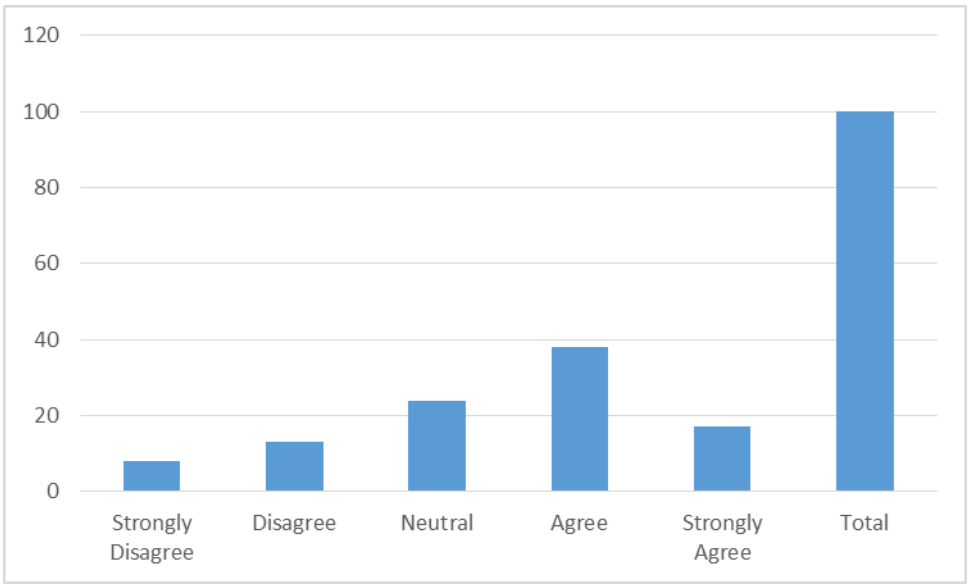

Figure 0.5 Unpreparedness of Small Businesses

Question 6

Half of the small businesses in the UAE have no plan to deal with cyber crime

The purpose of this question was to determine the perceptions of participants regarding the plan of the UAE to deal with cyber crime. The participants were asked to express the degree to which they agree or disagree that half of the small businesses in the UAE have no plan to deal with cyber crime.

Strongly Disagree	**8**
Disagree	21
Neutral	17
Agree	19
Strongly Agree	35
Total	100

Table 0.6 Plan to Deal with Cyber Crime

There were 8 respondents who strongly disagreed, 21 disagreed, and 17 remained neutral. On the other side, there were 19 respondents who agreed and 35 strongly agreed. In sum, there were

54 respondents who agreed and 29 disagreed. According to the frequency table, it can be agreed that the number of participants who agreed was more than those who disagreed. The larger proportion of employees working in small and medium-sized organizations in the UAE believes that the SMEs have no plan to deal with cyber crime.

This finding of the research is alarming because it shows that SMEs are at higher risk of being attacked by cyber criminals. The attack of cyber criminals will be severe for SMEs because of a lack of planning. In order to deal with cyber crimes, it is important for SMEs to conduct effective planning. The planning should entail increasing awareness of different types of cyber crimes and the methods of dealing with attacks. Moreover, adequate planning should also be done regarding the use of different proactive and reactive measures to deal with cyber crimes.

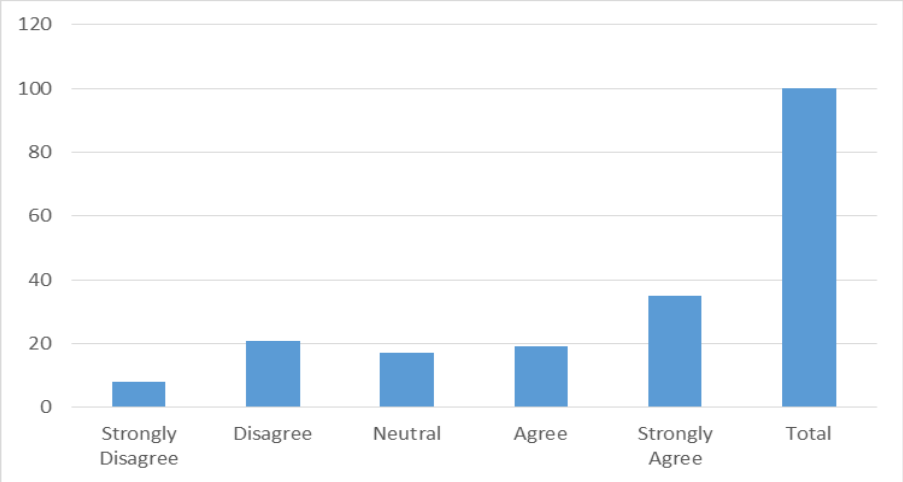

Figure 0.6 Plan to Deal with Cyber Crime

Question 7

SMEs consider threats to be genuine

In the next question, the respondents were asked to express their agreement or disagreement with the statement that SMEs consider threats to be genuine. The purpose of this question was to evaluate the perceptions of SMEs regarding the threats of cybercrime. The responses of participants have been presented in the following table:

Strongly Disagree	**9**
Disagree	11
Neutral	36

Agree	14
Strongly Agree	30
Total	100

Table 0.7 SMEs consider threats to be genuine

There were 9 respondents who strongly disagreed, 11 disagreed, and 36 remained neutral. On the other side, there were 14 respondents who agreed and 30 strongly agreed. According to the responses, a majority of respondents agree that threats faced by SMEs are genuine. There were 36 respondents who remained neutral in response to this question. This shows that 36 respondents did not express whether SMEs consider threats to be genuine or not. In order to prevent cybercrime, employees working at SMEs should be aware of the intensity of threats. A majority of participants believe that SMEs are aware of the intensity of threats. However, the above findings show that small and medium-sized enterprises are not prepared to deal with cyber crime. Moreover, the managers in SMEs have no plan to deal with cyber threats in the future.

The lack of planning and unpreparedness shows that SMEs are at risk of getting severely affected by cyber crimes. On the other side, the responses of participants show that some SMEs are aware of the intensity of threats associated with cyber-attack. It can be comprehended from these findings that although SMEs are aware of the fact that cyber crime is a threat, they have not prepared themselves to deal with the threat. Moreover, SMEs have not developed adequate plans in order to deal with threats.

This might be because of the reason that SMEs do not have possessed knowledge of ways that can be used to deal with cyber crime. The lack of resources of SMEs could also be associated with a lack of planning and unpreparedness. The role of national government is critical in this regard. It is important to conduct planning at the national level in order to ensure that small businesses are able to deal with security threats.

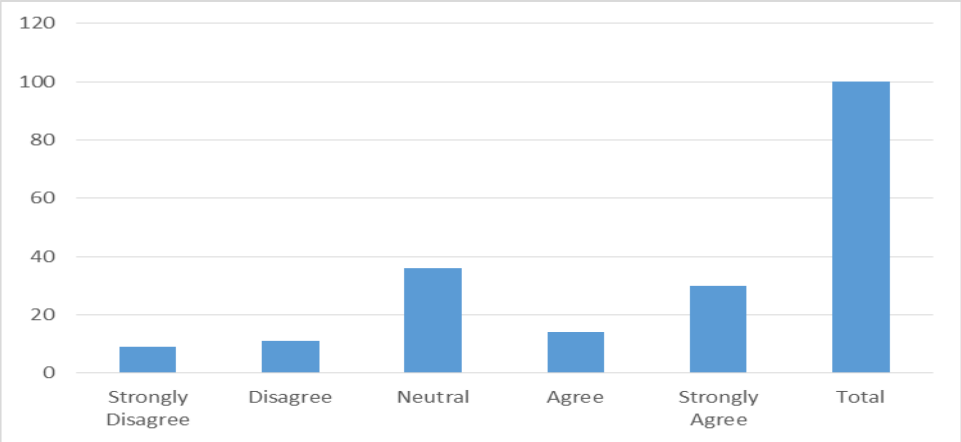

Figure 0.7 SMEs consider threats to be genuine

Question 8:

Is there a fact that the level of complexity intending to dangers differs broadly in the company?

The next statement given to participants said that the level of complexity intending to dangers differs broadly in the company. The participants were asked to express the degree to which they agree or disagree with the statement. The purpose of this question was to determine whether SMEs differ from each other in terms of the level of complexity or not. The question also aimed to identify the need for customized security programs by SMEs. The responses of the participants are as follow:

Strongly Disagree	**9**
Disagree	11
Neutral	36
Agree	14
Strongly Agree	30
Total	100

Table 0.8 Complexity Intending To Dangers Differs

There were 9 respondents who strongly disagreed, 11 disagreed, 14 agreed and 30 strongly agreed. There were 36 respondents who remained neutral. According to the responses, a majority of participants agreed that the level of complexity differs among organizations. There

were 36 neutral respondents. The neutral responses might indicate that the respondents were not aware of the differences between organizations in terms of dangers of security threats. The findings have led to the conclusion that the level of complexity intending to dangers differs among small and medium-sized organizations. The nature of threat faced by businesses is also different.

The differences exist because of differences in the nature of businesses. There are some businesses that make use of and store sensitive information on their databases. In service organizations, the information related to customers is of sensitive nature. In these businesses, it is important to develop security measures in order to prevent data theft. The nature of financial organizations is different from others. The cyber attack in these organizations can result in financial fraud. The loss of financial information involves huge cost. Therefore, it is important for these organizations to use security protocol that prevents cyber attackers from entering the system.

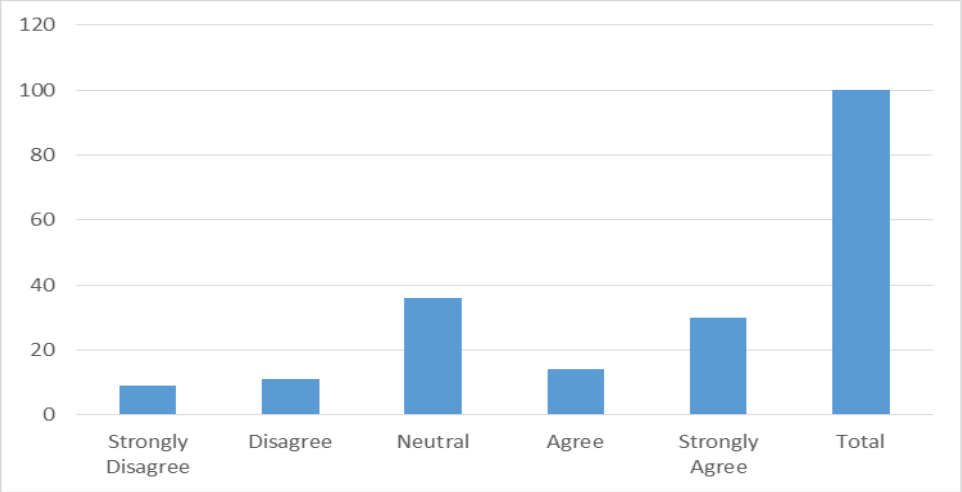

Figure 0.8 Complexity Intending To Dangers Differs

Question 9

Cyber security breach leaves a strong impact

The aim of this question was to evaluate the perception of participants regarding the impact of a cybersecurity breach. The participants were asked to express their agreement or disagreement with the statement that cybersecurity breaches leave a strong impact on small and medium-sized organizations. The participants gave following responses:

Strongly Disagree	**5**
Disagree	16
Neutral	30
Agree	26
Strongly Agree	23
Total	100

Table 0.9 Cybersecurity breach leaves a strong impact

There were 5 respondents who strongly disagreed, 16 disagreed, and 30 remained neutral. There were 26 respondents who agreed and 23 strongly agreed. The responses show that a majority of participants agreed that cyber security breaches have a strong impact. These findings are consistent with the findings of above question where respondents agreed that cyber security risks are genuine. These findings support that small and medium sized organizations are aware of the intensity of risk associated with cybercrime and the severe impact of this risk.

However, the steps taken by small and medium sized organizations to prevent cybercrime and to deal with cyber-13attack are not adequate. It is important for organizations to utilize their resources in an optimum manner in order to ensure that investment is made on systems to prevent security crime. Moreover, it is important for small and medium-sized organizations to hire employees who are aware of the security threats associated with cybercrime. Moreover, SMEs should also hire consultants who can prevent organizations from cybercrime.

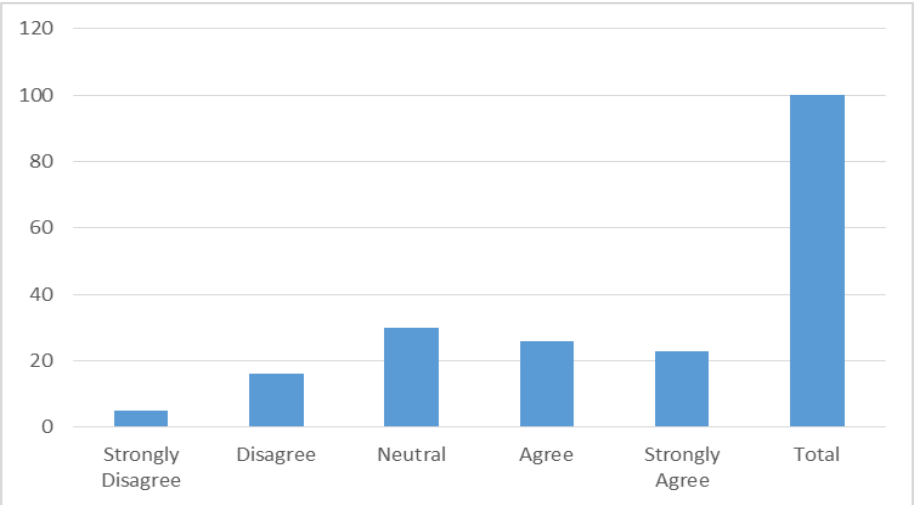

Figure 0.9 Cyber security breach leaves a strong impact

4.2 Reliability

Reliability Statistics

Cronbach's Alpha	N of Items
.917	12

Table 0.10 Reliability

According to (Bryman 2012), Cronbach Alpha test is used to measure the reliability of the scale. Bryman (2012) defined reliability, as the measure of consistency between different measurements of a variable. The Cronbach Alpha test measures the internal consistency of the questionnaire. In this research, the reliability of the scale has been measured with the help of Cronbach's Alpha test. As suggested by (Bryman 2012), the instrument is said to be reliable when the value of Cronbach alpha is higher than 0.70. The results of Cronbach's Alpha show that the instrument is acceptable and reliable. The value of Cronbach Alpha is 0.917 that is higher than 0.70.

4.3 Correlation

It has been discussed by Teddlie & Tashakkori (2009) that Pearson Correlation is used to measure the relation between different variables. The correlation test measures the nature and strength of the relationship between variables. The correlation table shows that the sig. value is 0.00, which is less than 0.05. Therefore, it can be agreed that the relationship between cyber security crimes and SMEs. The value of the Pearson Correlation shows the nature and strength of the relationship between variables. The positive sign shows that the nature of the relationship is positive. The value of Pearson Correlation is 0.883 that shows that the relationship between variables is strong. Therefore, a strong and positive relationship exists between cyber-crimes and SMEs.

4.3.1 Cyber Crimes and SMEs

Correlations

		cybercrime	SUMSMEs
cybercrime	Pearson Correlation	1	.883**
	Sig. (2-tailed)		.000
	N	100	100
SUMSMEs	Pearson Correlation	.883**	1
	Sig. (2-tailed)	.000	
	N	100	100

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

The correlation results show that there is a relationship between cyber-crimes and SMEs. The value of Pearson Correlation is 0. 883 which shows that the relationship is strong.

4.3.2 Relationship between Cyber Security Breaches and SMEs

Correlations

		cybercrime	BREACHSU
cybercrime	Pearson Correlation	1	.745**
	Sig. (2-tailed)		.000
	N	100	100
BREACHSU	Pearson Correlation	.745**	1
	Sig. (2-tailed)	.000	
	N	100	100

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

The correlation results show that there is a positive and strong relationship between cyber security breaches and SMEs. The value of Pearson Correlation is 0.745 which shows that the relationship is strong and the positive sign shows that the relationship is positive. Therefore, the hypothesis that there is a negative relationship between these variables has been rejected.

4.3.3 Relationship between Organizational and Operational Activities of SMEs and Cyber Crimes faced by SMEs

Correlations

		cybercrime	BREACHSU
cybercrime	Pearson Correlation	1	.745**
	Sig. (2-tailed)		.000
	N	100	100
BREACHSU	Pearson Correlation	.745**	1
	Sig. (2-tailed)	.000	
	N	100	100

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

According to the results of correlation analysis, there is a strong and positive relationship between organizational and operational activities performed by SMEs and their risks for cyber-crimes. The value of sig. is 0.00, which is less than 0.05. The value of Pearson Correlation is 0.745, which shows that the strength of the relationship between these variables is strong. Hence, it can be agreed that the relationship between variables is significant.

4.3.4 Relationship between Extra Steps Taken by SMEs and Cyber Crimes faced by SMEs

Correlations

		cybercrime	extrasteps
cybercrime	Pearson Correlation	1	.932**
	Sig. (2-tailed)		.000
	N	100	100
extrasteps	Pearson Correlation	.932**	1
	Sig. (2-tailed)	.000	
	N	100	100

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

The correlation analysis shows that there is a relationship between extra steps taken by SMEs and prevention of cyber-crimes. The value of Pearson Correlation is 0.932, which shows that the strength of the relationship between variables is 93%. The positive sign shows the

presence of a positive relationship between variables. Therefore, the security measures can result in the prevention of cybercrimes.

4.3.5 Relationship between Overcoming of SMEs and Cyber-crimes faced by SMEs

Correlations

		Overcomingandrisks	cybercrime
Overcomingandrisks	Pearson Correlation	1	.916**
	Sig. (2-tailed)		.000
	N	100	100
cybercrime	Pearson Correlation	.916**	1
	Sig. (2-tailed)	.000	
	N	100	100

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

According to the results of correlation analysis, there is a strong and positive relationship between risks and overcoming of SMEs and cyber-crimes. The value of Pearson correlation is 0.916 that shows that the strength of the relationship is strong. The positive sign shows that the relationship between variables is positive. The value is a sig. is 0.000 which is less than 0.05; hence it can be agreed that the relationship between variables is significant.

4.4 Regression Analysis

The regression analysis was used in order to measure the association between independent and dependent variables. The dependent variable in the research is SMEs and the independent variable is a cyber crime.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.883[a]	.779	.777	1.89904

a. Predictors: (Constant), cybercrime

The model summary shows the value of the r-square in the research. The value of r-square is 0.779, which shows a high level of association between cyber security breaches and SMEs. The impact of cyber security breaches is 77% of SMEs. In other words, cyber-crimes are explaining 77% variance in SMEs' performance.

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1246.619	1	1246.619	345.675	.000[a]
	Residual	353.421	98	3.606		
	Total	1600.040	99			

a. Predictors: (Constant), cybercrime

b. Dependent Variable: SUMSMEs

The ANOVA table in regression is based on the null hypothesis that regression model is a chance model. If the value of sig. is less than 0.05, the null hypothesis is rejected and vice versa. The sig. value in ANOVA table is 0.00, which is less than 0.05. Therefore, the null hypothesis has been rejected. Hence, it has been accepted that regression model is the best fit.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.321	.497		2.658	.009
	cybercrime	.582	.031	.883	18.592	.000

a. Dependent Variable: SUMSMEs

The coefficient table explains the association between dependent and independent variable. The table also explains the significance of variables in the regression model. In order for a variable to be significant, its value should be less than 0.05. The sig. values for constant and cyber crimes are 0.009 and 0.000 respectively. Therefore, it can be agreed that both variables are significant in the regression model. Hence, it can be accepted that there is a significant impact of cyber-crimes on SMEs.

On the basis of regression results, the following equation has been formulated:

$$=1.321 + 0.582 \text{ cyber crime}$$

4.4.1 Impact of Cyber Security Breaches on SMEs

In order to assess the impact of impact of security breaches on SMEs, linear regression was applied.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.875[a]	.766	.763	1.95557

a. Predictors: (Constant), BREACHSU

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1225.262	1	1225.262	320.392	.000[a]
	Residual	374.778	98	3.824		
	Total	1600.040	99			

a. Predictors: (Constant), BREACHSU

b. Dependent Variable: SUMSMEs

The model summary shows that the value of r-square is 0.766; hence, cyber security breaches are explaining 76% variance in SMEs. The sig. value in ANOVA table is 0.00, which shows that the regression model is the best fit.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.389	.461		5.183	.000
	BREACHSU	3.037	.170	.875	17.899	.000

a. Dependent Variable: SUMSMEs

The coefficient table shows that the sig. values for cyber security breaches and SMEs are 0.00 and 0.00 respectively. Since these values are less than 0.05, it can be agreed that there is a positive association between cyber security breaches and SMEs. The results of regression analysis have rejected the hypothesis that says that there is a negative relationship between cyber security breaches and SMEs.

4.4.2 The Organizational and Operational Activities of SMEs

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.765[a]	.584	.580	2.60470

a. Predictors: (Constant), SPREPAREDNESS

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	935.160	1	935.160	137.838	.000[a]
	Residual	664.880	98	6.784		
	Total	1600.040	99			

a. Predictors: (Constant), SPREPAREDNESS

b. Dependent Variable: SUMSMEs

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.405	.608		5.596	.000
	SPREPAREDNESS	2.657	.226	.765	11.740	.000

a. Dependent Variable: SUMSMEs

According to the results of regression analysis, the level of variance explained by operational and organizational activities of SMEs is 58%. The ANOVA table shows that the regression model is the best fit. According to the coefficient table, the operational and organizational activities of SMEs have an impact on cyber-crimes faced by them. The organizational and operational activities are undertaken by SMEs can have a significant impact on their preparedness for cyber-crimes. Therefore, it is important for SMEs to engage in activities that result in increasing their security.

4.4.3 Impact of Extra Steps Taken by SMEs

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.742[a]	.551	.547	2.70673

a. Predictors: (Constant), extrasteps

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	882.053	1	882.053	120.394	.000[a]
	Residual	717.987	98	7.326		
	Total	1600.040	99			

a. Predictors: (Constant), extrasteps

b. Dependent Variable: SUMSMEs

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.253	.660		4.927	.000
	extrasteps	1.385	.126	.742	10.972	.000

a. Dependent Variable: SUMSMEs

According to the results of regression analysis, the extra steps taken by SMEs such as crisis measures and other prevention techniques have an impact on the prevention of cybercrimes. The value of R-square is 0.551, which shows that extra steps taken by SMEs have an impact on the occurrence of cyber-crimes. The results of ANOVA table show that the regression model is the best fit. The results of the coefficient table show that there is a significant association between variables.

4.4.4 Overcoming and Risks

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.896[a]	.803	.801	1.79316

a. Predictors: (Constant), Overcomingandrisks

ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1284.928	1	1284.928	399.614	.000[a]
	Residual	315.112	98	3.215		
	Total	1600.040	99			

a. Predictors: (Constant), Overcomingandrisks

b. Dependent Variable: SUMSMEs

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.561	.452		3.451	.001
	Overcomingandrisks	1.104	.055	.896	19.990	.000

a. Dependent Variable: SUMSMEs

The research was based on hypotheses that the activity of inaccurate information, the activity of unauthorized people accessing information, and cyber-attacks are major overcoming and risks faced by SMEs. In order to test these hypotheses, regression analysis was applied. The results show that cyber-attacks and access to information have a significant impact on SMEs. The variance explained by these factors is 80%. The results of ANOVA table show that the regression model is the best fit. The results of the coefficient table show that there is a significant association between variables.

4.5 Chi-Square

Test Statistics

	SUMSMEs	cybercrime
Chi-Square[a,b]	48.480	61.700
df	15	20
Asymp. Sig.	.000	.000

a. 0 cells (.0%) have expected frequencies less than 5. The minimum expected cell frequency is 6.3.

b. 21 cells (100.0%) have expected frequencies less than 5. The minimum expected cell frequency is 4.8.

Table 0.11 Chi-Square

The association between dependent and independent variables was also measured with the help of chi-square test. The results of the test have shown that the value of sig. is less than 0.00. Hence, it has been accepted that there is a significant impact of cyber security breaches on SMEs.

4.6 Analysis of Interview

In order to conduct qualitative analysis, data was gathered through interviews. The interviews were conducted with three respondents. The aim of the interview was to get an in-depth understanding of the research and to determine how the findings of this research can address the research question. When conducting interviews, the participants were ensured that their identity will remain confidential.

Question 1: What do you know about different kinds of cybercrime?

Respondent 1:

The first respondent was an administrative manager and was aware of the threat of cybercrime. The participant revealed that there are different types of cyber crimes including data theft, financial fraud, and the unauthorized access to the system. The participant also agreed that there is a serious threat of cyber crime for SMEs that are not prepared to deal with the crime.

The role of the Respondent: The respondent has been working as an administration manager in the respective organization for 10 years. The respondent is involved in database administration and the implementation of firewall systems to prevent data theft.

Relationship with Cybercrime: The respondent has been dealing with the administration of database since 10 years.

Respondent 2:

According to this respondent, there are different kinds of cybercrime including the theft of sensitive information and hacking. The respondent is the CEO of a small business and believes that data related to customer information is sensitive. Therefore, it is important for the business to use measures to prevent the theft of this information. The respondent also added that it is important to develop policies within the organization to prevent the misuse of data by employees.

The role of the Respondent: The respondent is the owner of a small food business. The respondent is responsible for managing the overall operations of business.

Relationship to Cybercrime: The respondent is the owner of a small business and has five years of dealing and managing customer information.

Respondent 3

The last respondent also added that data theft and hacking of system are cyber crimes faced by businesses. The respondent further added that small businesses often lack resources to prevent cyber crimes. Moreover, the participant also believes that the technical knowledge of SMEs is also limited.

Role: IT manager, responsible for overseeing IT related operations

Relationship to Cybercrime: Seven years of experience as an IT manager

Question 2: What are your views regarding the awareness of SMEs regarding cyber crime?

Respondent 1

According to the respondent, the awareness of small and medium-sized enterprises regarding the cyber crime is limited. Although organizations are aware of the threats associated with cyber crime, they are not aware of the ways to deal with it.

Respondent 2

According to this respondent, small and medium sized organizations are aware of the threats associated with cybercrime. However, a lack of resources prevents them from using measures to prevent cyber crime

Respondent 3

According to the third respondent, the awareness of SMEs regarding the cyber crime is not sufficient. Therefore, there is a need to increase awareness regarding different types of cybercrime and the ways used to prevent it.

Question 3: How the awareness of employees regarding cybercrime can be increased?

Respondent 1:

According to the first respondent, the awareness of employees regarding the cyber crime is important in order to prevent the attack. The awareness of employees can be increased with the help of training programs that increase awareness of employees.

Respondent 2:

According to the second respondent, communication between employees as well as the communication between employees and managers is important in order to increase the awareness of employees.

Respondent 3:

According to the third respondent, in order to increase employees' awareness, it is important for managers to communicate necessary information to employees. The information shared by managers in SMEs can prevent towards increasing the awareness of employees.

Question 4: What are some of the preventive measures that can be taken to prevent cyber crime?

Respondent 1:

The participants were asked about preventive measures that can be taken to prevent cybercrime. According to the participant, cybercrime can be prevented with the use of antivirus and firewall systems.

Respondent 2:

The second participant believed that in order to prevent cybercrime, it is important to educate employees about different measures. First of all, employees should be advised to prevent sharing of information with outsiders.

Respondent 3:

The third respondent added that firewalls and advanced technology need to be adopted in order to prevent cybercrime.

4.7 Hypothesis Assessment Summary

1	**The breaches of cyber security present negative effect on SMEs.**	**Rejected**
2	The organizational and operational activities are ready for the cyber security attacks.	**Accepted**
3	The extra steps taken by SMEs will be useful for the prevention of cyber security attacks	**Accepted**
4	The activity of inaccurate information present major overcoming in terms of SMEs	**Accepted**
5	The activity of unauthorized people assessing wrong information present major overcoming in terms of SMEs	**Accepted**
6	The activities of cyber-attacks present major overcoming in terms of SMEs.	**Accepted**

Table 0.12 Hypothesis Assessment Summary

The first hypothesis of the research was to determine the impact of cyber security breaches on SMEs. The results of regression and correlation analysis have rejected the hypothesis that cyber-security breaches result in a negative impact on SMEs. The preparedness

of SMEs for cyber-crimes was assessed by measuring their operational and organizational activities. It has been found from the results of correlation and regression analysis that the organizational and operational activities of SMEs are ready. The extra steps taken by SMEs such as crisis measures and security measures can result in the prevention of security threats. The major overcoming and risks faced by SMEs include the access of unauthorized people to information and cyber-attacks.

CHAPTER 5 DISCUSSION

This research was based on the objective of determining the impact of cyber-crimes on SMEs. The research was carried out in the UAE because it is a hub for businesses. There has been an increase in the number of SMEs resulting in an increase in cyber-attacks on online activities performed by SMEs. According to a report published by Symantec, 52.4% cyber-attacks are made on SMEs alone.

This research was based on quantitative research methodology and involved the collection of primary and secondary data. Primary data were gathered from employees working in different SMEs in the UAE. The secondary information was gathered from published sources including articles, journals, and research papers. The sample size consisted of 100 employees working in different SMEs. The participants were selected with the help of random sampling method in which every member of the population has an equal chance of getting selected. Data analysis was carried out with the help of SPSS software.

The reliability analysis was performed by using Cronbach's Alpha test that helped in measuring the internal consistency of the instrument. The instrument was based on Likert scale and consisted of 12 questions. The values of Cronbach Alpha proved the reliability of research instrument. In order to measure the relationship between variables, the correlation was applied whereas regression was applied to measure the association between variables. The chi-square test was also applied in order to test the association between variables.

The findings of quantitative data analysis helped in achieving research objectives. The first objective of the research was to determine the impact of cyber security breaches on SMEs. The second objective was to investigate the readiness state of cyber security attacks on SMEs. The third objective was to determine the benefits of being prepared for cyber security breaches. The fourth objective was to identify steps that can be taken to prevent cyber security attacks. The fifth objective was to determine the benefits of cyber security for SMEs.

5.1 Impact of Cyber Security Breaches on SMEs

It has been discussed by Han (2012) that the impact of cyber security is damaging for businesses. The businesses need several years in order to recover from the loss created by cyber-attacks. The damages also result in the long-term reputation of businesses. The research conducted by Muegge & Craigen (2015) has also highlighted the negative impact of cyber-

crimes on businesses. Hugthes & Cybenko (2013) explained that cybersecurity crimes result in a negative impact on SMEs.

The following table shows the effects of cyber crimes on SMEs. Loveland & Lobel (2012) in their survey came across where the majority of the business reported suffering from financial loss, intellectual property loss of reputation, fraud, lawsuit filed against the suffering organization, loss of values of shareholder and extortion from cyber attackers due to cyber-attacks. According to the chart, the most significant impact of cybercrime is in the form of financial loss.

37.5%
Financial Loss
31.8%
Intellectual Property Theft
31.2%
Branded/reputation compromised
15.8%
Fraud
12.2%
Legal exposure/Lawsuit
11.3%
Loss of shareholder value
7.1%
Extortion

Figure 0.1 US business impact of security incidents

(Loveland & Lobel 2012, p. 1)

Bailey, Miglio & Richter (2014) discussed that SMEs need to believe that they are not vulnerable to cyber security breaches. In fact, SMEs are vulnerable to cyber crimes because of a lack of cyber security system. Therefore, SMEs have greater chances of being attacked by cyber criminals. It has been discussed by Choras et al. (2015) that 22% of data breaches involve SMEs.

The most common security breach faced by SMEs is the mishandling of data. Hughes & Cybenko (2013) discussed that small and medium sized organizations in the UAE are at a serious risk of getting attacked by cyber crimes. The researchers also discussed that SMEs in the UAE do not have counter plans to deal with cyber-crimes. Muegge & Craigen (2015) discussed that cyber risks faced by SMEs in the UAE can be classified into human risks, physical risks, and network risks.

The association between dependent and independent variables was also measured with the help of the chi-square test. The results of the test have shown that the value of sig. is less than 0.00. Hence, it has been accepted that there is a significant impact of cyber security breaches on SMEs. However, the results of chi-square have not proved that the relationship between security breaches and SMEs is positive. The results of statistical tests have revealed that SMEs face different risks that have an impact on SMEs.

This research is based on the analysis of SMEs in the UAE. It has been found from the results of results of regression and correlation that the association and relationship between cyber security and SMEs are positive. Therefore, the null hypothesis has been rejected. The findings of the primary data analysis have rejected the findings of secondary data. The differences in the results could be because of differences in the population and sample selected for research.

5.2 Readiness State for Cyber Security Threats

The second objective of this research was to evaluate the readiness state of SMEs for cyber security threats. It has been discussed by Miron & Muita (2014) that SMEs are vulnerable to cyber-attacks because of a lack of preparedness of the management. The management of SMEs believes that cyber criminals often attack large businesses; therefore, they do not prepare themselves for attacks. In order to evaluate the readiness state for cybersecurity threats, the operational and organizational activities of SMEs were evaluated. It has been found from regression analysis that the operational and organizational activities of SMEs have a strong and positive relationship with cyber crimes faced by SMEs.

The risks faced by SMEs have necessitated the need for being prepared for cyber security threats. The access to inaccurate information and activity of unauthorized people are major security threats faced by SMEs. The impact of these factors on cyber-crimes is 80%. The following table shows that cyber crimes in the UAE have been increasing. According to Hadbini

(2014) Dubai, official statistics demonstrated that 88% of the increase in contrast to 2013 was notified in the number of electronic crime cases. A total of 1419 reported in 2013, 792 in 2012 and 588 in 2011 reports were received by the cyber investigation department of Dubai Police.

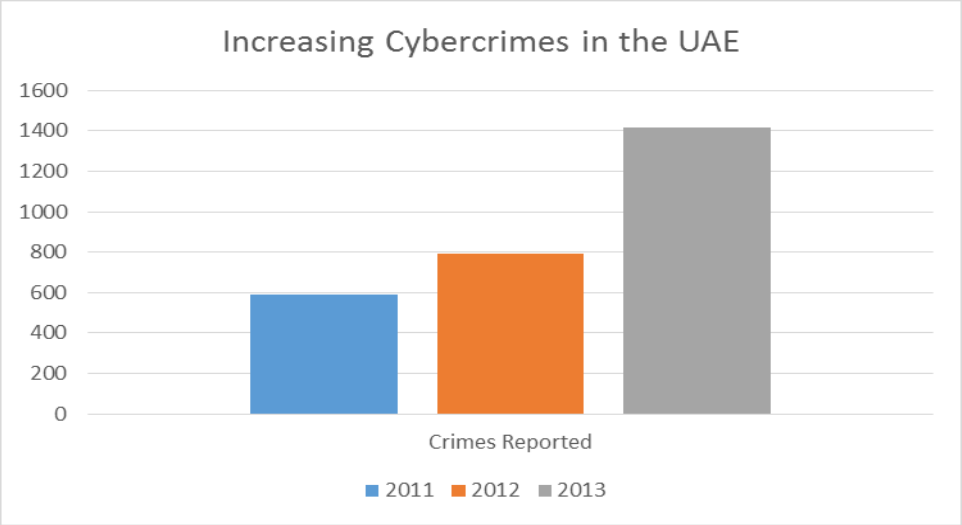

Figure 0.2 Increasing Cybercrimes in the UAE

(Hadbini 2014, p. 1)

It has been discussed by Payette et al., (2015) that organizations the readiness level of public firms is different from that of private firms. Similarly, the readiness level also differs on the basis of the size of organizations. The large corporations have the technology and updated systems to deal with cyber-crimes. However, small businesses often lack the system required for preventing cyber-crimes. The large businesses install the best security systems that are often not accessible to small businesses.

The research was based on hypotheses that the activity of inaccurate information, the activity of unauthorized people accessing information, and cyber-attacks are major overcoming and risks faced by SMEs. In order to test these hypotheses, regression analysis was applied. The results show that cyber-attacks and access to information have a significant impact on SMEs. The variance explained by these factors is 80%. The results of ANOVA table show that the regression model is the best fit.

The results of the coefficient table show that there is a significant association between variables. It has been discussed by Kroll (2015) that there is an increase in cyber-attacks on

SMEs in the UAE. The cyber-attacks have caused serious damages to the targeted businesses. In this environment, Choras et al. (2015) have highlighted the need for increasing readiness by small businesses.

The readiness of SMEs for cyber-crimes has also been explained by Miron & Muita (2014). According to the researchers, a digital attack counter program can offer several benefits to small businesses. The research of Kaur & Mustafa (2013) has supported that the preparedness of SMEs results in the prevention of cybercrimes.

5.3 The Benefits of Being Prepared For Cyber Security Breaches

The third objective of the research was to determine benefits of being prepared for cyber security breaches. According to Miron & Muita (2014), the counterattack program has a significant impact on the security of small businesses. Therefore, it can be agreed that being prepared results in increasing the security of small businesses. Miron & Muita (2014) also discussed that being prepared results in minimizing the damages caused by cyber-attacks. The research conducted by Kaur & Mustafa (2013) has revealed that being prepared can result in cost savings in the case of cyber-attack.

According to their research, approximately 154 Dirham can be saved for records of SMEs by being prepared for cyber-attacks. Jhon (2015) stated that being prepared increases the chances of success and prosperity for small businesses.

In this research, preparedness of SMEs in the UAE was evaluated with the help of regression and correlation analysis. The correlation analysis was carried out to determine the relationship and operational and organizational activities of SMEs and extra steps taken by them to prevent cyber-crimes.

The results of statistics test revealed that there is a strong and positive relationship between organizational and operational activities undertaken by SMEs and the prevention of cybercrimes. The relationship between extra steps taken by SMEs and prevention of cyber-crimes is also positive. Therefore, this research has revealed that the preparedness of SMEs results in reducing the chances of cyber-crimes. According to Cherrayil (2015) in his article explained that majority 42 percent of Millennials which accounts for two million citizens of UAE in contrast to Generation X have encountered online crime specifically in UAE, resulting in

loss of Dh 4.9 billion. The graph below explains the cyber security insight of the UAE in contrast to Global cyber security.

Cybercrimes	UAE	Global
Number of consumers get affected by cyber crime	**2 million**	**594 million**
Amount lost by consumers because of cyber crime	**$1.3 billion**	**$150 billion**
Time lost by consumers to deal with the impact of cyber crime	**30 hours**	**21 hours**
Financial information was stolen because of cybercrime	**20%**	**16%**
Consumers who feel in control over online security	**26%**	**15%**

Table 0.1 Cyber security Insights

(Cherrayil 2015, p. 1)

Hence, the findings of this research have supported the findings of research conducted by Jhon (2015), Kaur & Mustafa (2013), and Miron & Muita (2014). The regression analysis was applied in order to test the association between preparedness of SMEs and the prevention of cyber-crime. According to the results of regression analysis, organizational and operational activities of SMEs explain 58% variance in the cyber-crimes faced by SMEs. Moreover, the extra steps taken by SMEs explain 55% variance in the prevention of cybercrimes. Hence, it can be agreed that the benefit of preparedness for small businesses is the prevention of cybercrimes. The benefits, discussed in the secondary research, include cost saving and the control on damages caused by cyber-attacks.

5.4 Steps for SMEs to Prevent Cyber Security Attacks

It has been discussed by Jhon (2015) that prevention of cyber security attacks can prevent businesses from operational loss. Jhon (2015) discussed that managers and owners of small businesses need to follow some standards in order to prevent cyber-crimes. Thekkepat (2016) discussed the need for systems to prevent cyber-crimes. The associations need to be formed in order to ensure the security of SMEs' data.

There are different activities that are performed by SMEs in order to prevent cyber security attacks. The results of regression analysis have revealed that the operational and organizational activities result in 58% variance in the prevention of cybercrimes. Therefore, it can be agreed that one of the ways through which SMEs can prevent cyber-crimes is to develop operational and organizational activities that result in crime prevention.

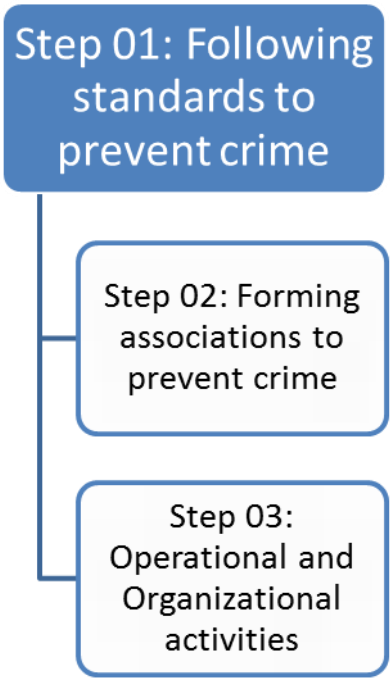

Figure 0.3 Steps to prevent cyber crimes

(Thekkepat 2016, p. 15)

In order to prevent cyber-crimes, it is also important for SMEs to overcome risks. The overcoming and risks of cyber-crime are explaining 77% variance in cyber-crimes faced by SMEs. The results show that in order to prevent cyber-crimes, it is important to overcome shortcomings and risks. These findings show that one of the steps that SMEs should take to prevent crimes is the risk management techniques.

According to the results of regression analysis, the extra steps taken by SMEs to prevent cyber-crimes have 55% impact on the prevention of cyber-crime. The results of ANOVA also show that the impact of extra steps in preventing cyber-crimes is significant. The extra steps involve the development of extra rules and regulations in order to guarantee the protection of information of SMEs.

5.5 Hypothesis Testing

Following hypotheses were developed for the research:

5.5.1 The Breaches of Cyber Security Present Negative Effect on SMEs

In order to test this hypothesis, regression analysis, correlation analysis, and chi-square test were applied. The results of regression analysis show that cyber security breaches are explaining 76% variance in the SMEs. These results also reveal that as a result of cybercrime, 76% variation in SMEs is taking place. The percentage shows that cybercrime has a significant impact on SMEs in the UAE. The results of correlation analysis and chi-square analysis show that sig. values are less than 0.05. Therefore, there is a positive relationship between these variables. Hence, the null hypothesis has been rejected.

Miron & Muita (2014) discussed that there are different types of cyber crimes that occur to SMEs including financial fraud, sabotage of data, information theft, and penetration to the system, service denial, unauthorized access, and unstructured access. The percentage of these effects on SMEs is different. The percentage of financial fraud is 10%. This shows that as a result of cyber crimes, 10% organizations are likely to lose financial information. The percentage of data sabotage is 18% which indicates that in 18% cases, firms lose data as a result of cybercrime.

The percentage of the theft of proprietary information is 20% suggesting that in 20% cases organizations lose proprietary information because of cybercrime. The percentage of system penetration is 22% which is also a serious risk faced by businesses associated with cybercrime. There are 28% cases in which denial of services takes place because of cybercrime. The percentage of cases where unauthorized access takes place by insiders is 70%.

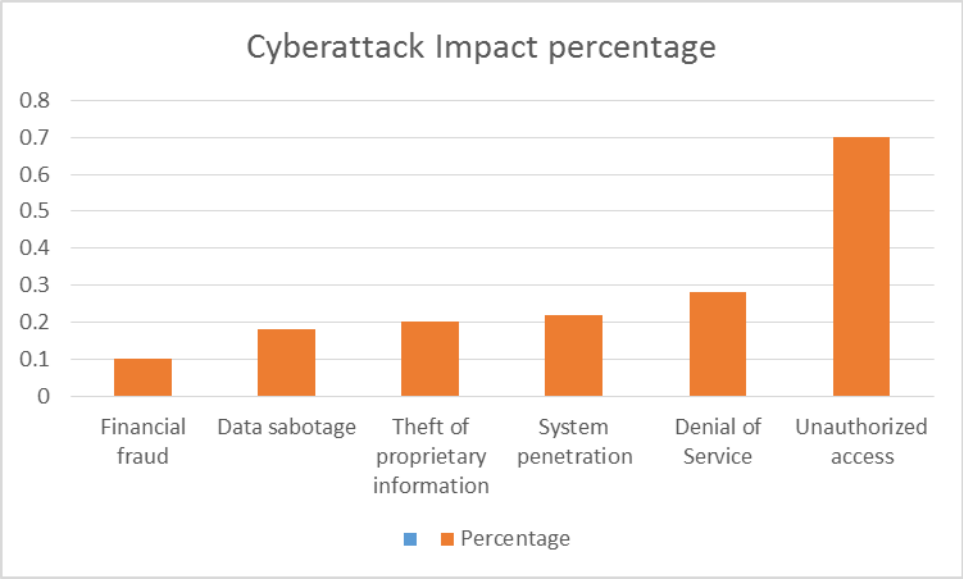

Figure 0.4 Steps to prevent cyber crimes

(Miron & Muita 2014, p. 5)

5.5.2 The Organizational and Operational Activities Are Ready For the Cyber Security Attacks

According to the results of regression analysis, the impact of operational and organizational activities of SMEs on cyber security attacks is 58%. The correlation analysis has proved that the relationship between these variables is positive. The strength of the relationship is 75%. Hence, the operational and organizational activities of SMEs have a significant impact on cyber security attacks of SMEs.

Jhon (2015 suggested that it is important for organizations to undertake different operational and organizational activities to prevent cybercrime. At the organizational level, procedures and policies should be developed to prevent the occurrence of cybercrime. For instance, employees should be prevented from discussing sensitive information with outsiders. Moreover, the penalty should be charged on employees in case they share information with others. At the operational level, it is important to use security systems such as firewalls in order to prevent cybercrime.

5.5.3 The Extra Steps Taken By SMEs Will Be Useful For the Prevention of Cyber Security Attacks

The third hypothesis was to determine the relationship between extra steps taken by SMEs and the prevention of cyber security attacks. According to the results of correlation analysis steps taken by SMEs results in the prevention of cybercrimes. The strength of the relationship between variables is 93%. The variance explained by these factors is 55%. Hence, it can be agreed that the extra steps were taken by the SMEs result in the prevention of cyber security attacks.

There are different extra steps that can be taken by SMEs to prevent cyber security attacks. Jhon (2015) explained that one of these steps involve creating an internal policy. Another important step that can prevent cyber security attacks is the use of cloud services. The cloud services can be used for handling application needs and data storage. The other important step involves hiring a security expert who can discover loopholes in the current security system. Since cyber crimes are becoming advanced with the passage of time, it is important to hire consultants who have updated knowledge of ways that can be used to prevent crimes.

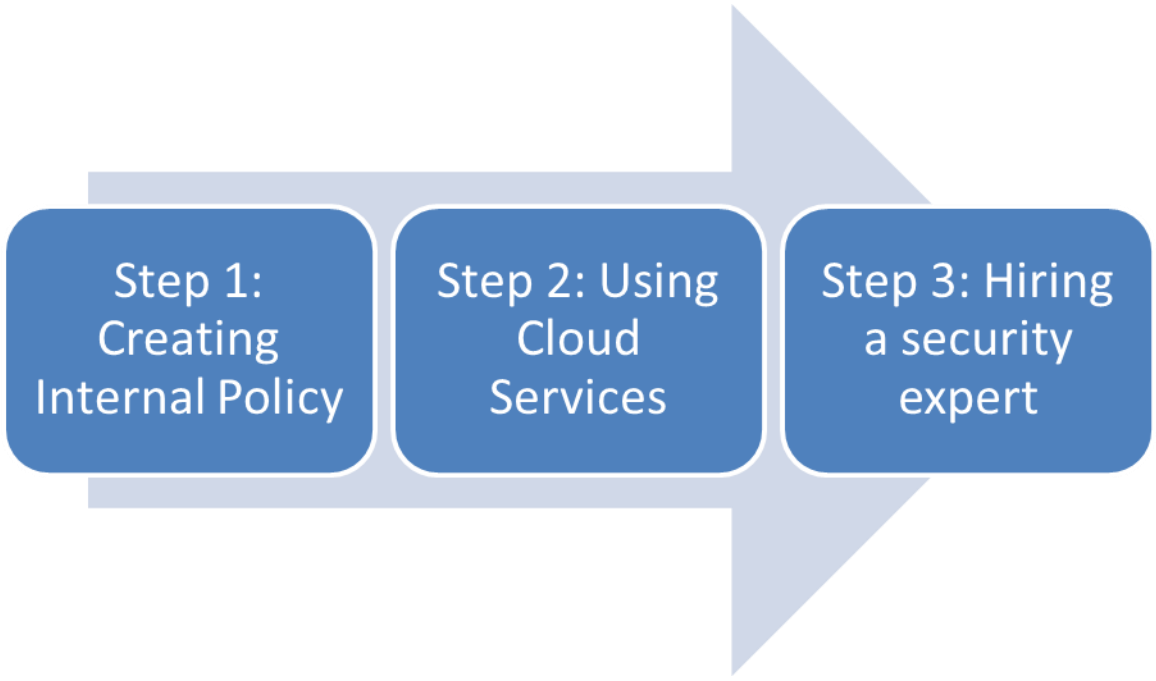

Figure 0.5 Extra steps for the prevention of cybercrime

(Jhon 2015, p. 25)

5.5.4 The Activity of Inaccurate Information Present Major Overcoming In Terms Of SMEs

The analysis of overcoming and risks faced by SMEs has revealed that the inactivity of inaccurate information is a major overcoming in terms of SMEs. The results of correlation and regression analysis have revealed that there are a significant association and relationship between inaccurate information and the prevention of cybercrimes. These results have highlighted the importance of information security in SMEs. It is important for SMEs to use advanced systems for information manager. It is also important to hire an expert who can manage and protect the sensitive information of businesses.

5.5.5 The Activities of Cyber-Attacks Present Major Overcoming In Terms Of SMEs

The results of regression analysis show that the variance explained by different overcoming is 80%. The ANOVA results show that the impact of overcoming is significant on cyber-crimes faced by SMEs. According to the results, the activities of cyber crimes are contributing 89% towards increasing challenges for SMEs. These results have highlighted the importance of taking measures to prevent cyber crimes. The above statistics also show that cyber crime is a significant threat faced by SMEs. In order to prevent this threat, it is important for SMEs to take extra steps such as hiring consultants and using cloud services.

5.5.6 The Activity of Unauthorized People Assessing Wrong Information Present Major Overcoming In Terms Of SMEs

The results of regression and correlation analysis show that the activity of unauthorized people is a major overcoming in terms of SMEs. The results of correlation analysis show that there is a positive relationship between overcoming of SMEs and prevention of cyber-crimes. The use of cloud services and firewalls can prevent the activity of unauthorized people in SMEs. The access of unauthorized people can cause serious damage to sensitive information. The unauthorized people can also contribute towards sharing sensitive information with others. Hence, it is important to take steps to prevent the activity of unauthorized people.

5.5.7 The Trusted Digital Environment Can Be Formed By Allowing The Protocols For Cyber Security.

It has been discussed by Han (2012) that the trusted environment included log in ids and passwords and secured information. Kadivar (2014) discussed that the digital environment can be made secure by allowing the protocols for cyber security. In order to develop a secure digital environment, it is important for SMEs in the UAE to develop a trusted computerized environment.

In order to create a trusted digital environment in the UAE, it is important to take various steps. The first step involves the creation of a central cyber security body. The second step involves the development of a cyber-security strategy at a national level. In the third step, there is a need to establish a national dialogue. The next step involves the development of preventive cyber security capabilities in order to ensure that citizens in the UAE remain protected from cybersecurity risks. The development of reactive capabilities to deal with cyber security is also necessary in order to deal with the consequences of cyber security. The last step involves the development of a national talent strategy.

Figure 0.6 Extra steps for the prevention of cybercrime

(Kadivar 2014, p. 15)

5.6 Summary

The aim of the research was to determine the impact of cyber-crime security breaches on SMEs. The research also aimed to determine the current state of readiness for cybersecurity attacks. The findings of the research have revealed that the cyber security breaches have a significant impact on SMEs in the UAE. The current state of readiness of SMEs for cyber security attacks shows that the SMEs take various steps to prevent cyber-crimes. These steps involve different organizational and operational activities that result in the prevention of cyber-crime. Small and medium sized organizations also take different extra steps in order to prevent cyber-crimes.

The cyber security breaches are damaging for businesses regardless of their size. The damages caused by cyber-crimes are very devastating for businesses. The security breaches cause serious damages to the reputation of businesses. The businesses need to be careful about cyber-crimes in order to prevent the misuse of sensitive information. The instances of cyber-crimes have been increasing in the current era despite advancements in IT. There are different kinds of cyber breaches faced by businesses. One of these breaches involves the misuse of login id and password to unauthorized people. This results in the access of unauthorized people to a firm's data. The hacking of a firm's system is also a threat faced by businesses.

CHAPTER 6 CONCLUSION

6.1 Conclusion

Small and Medium Sized Enterprises (SMEs), in the worldwide financial situation of today, vigorously rely upon information technology or the World Wide Web for representing their services, products, and expertise. SMEs are the creators of job opportunities which thus produce beneficial salary. With regards to multi-tasking, these companies are extremely adjustable in their endeavors. They are substantial suppliers for real segments, their inward business endorsement choices are usually taken rapidly.

Moreover, they are fast in settling on basic choices and extremely adaptable to change their structure with any given business necessity. Be that as it may, with regards to the security threats faced by SMEs, it is assumed that these small and medium-sized enterprises do not have the specialized aptitude, the assets, the learning, and security designers to ensure their frameworks against the dangers that could be caused by a security breach. These companies lack authoritative arrangements and undertakings related to the privacy and security of their company's sensitive information.

The administration of an SME does not see their organization as an at risk focus for digital wrongdoing aggressors or programmers. The greater part of the thought of implementing the security framework within the company is mostly to set a firewall or an anti-virus software which is a misguided judgment, believing that digital security issues are just implied for companies that are larger in size. Preparedness for security measures associated with online information and reliance on the World Wide Web are developing at a quick rate, which has turned into the prime issue for big business data security.

The greater part of these small and medium-sized firms rely upon the internet and IT for their different business exercises without knowing of how to secure their sensitive information from the employees who have left the company or have been fired and also the outside parties such as the hackers and other cyber criminals. Very few of these companies have their own particular system of security, however at an exceptionally insignificant expense as putting resources into the insurance of their company's data is not their primary worry until or unless they are actually attacked by a cyber-threat.

In the business surroundings of today, weaknesses and threats caused by cyber security breaches with respect to the resources and data frameworks are the real obstacles confronted by

small and medium-sized firms without their usage of security techniques and strategies for IT, information assurance system and so on. Without such measures, it prompts change, misfortune and loss of information, and leaking of confidential data of the company. It also treats the physical assets, as hackers can send viruses to the networks and servers of the company that could damage the company used devices and computers. A small sized firm's customers dependably have a high impression that their delicate information is ensured under the best security instruments.

The companies that are larger in size and who work with the SMEs needs to be guaranteed that their colossal information which is streaming all through the company is safe. On the off chance that the security falls flat, can bring about the loss of the trust of many loyal customers. As found with the help of the research and as the findings suggest, cyber security breaches can also cause financial adversity and there can be high odds of compensations and fines from lawful powers which the company might not be able to pay. It is particularly important to secure data, (for example, administration control, company equipment and the computer applications being used by the company).There is dependably a cost required in not ensuring data, and can cause future troubles especially for a company which is smaller in size and might take years to regain their lost position back. The image below represents different sources from which a company can expect a cyber-attack

Figure 0.1 Sources of Cyber Threat

(Han 2012, p. 16)

Protecting company's data from the threats cyber-criminal activities is the most widely recognized and essential for SMEs and their partners. It is also important to increase the awareness of people regarding law enforcement agencies where cyber crimes can be reported. There are 15% Internet users who are aware of where to report cyber crimes whereas 84% are not aware.

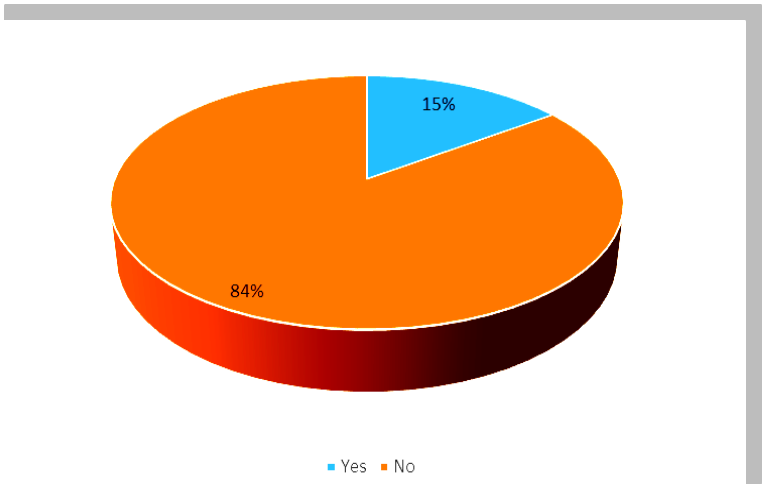

Figure 0.2 Sources of Cyber Threat

(Han 2012, p. 24)

The essence of any Information security frameworks is the spending cost connected with its configuration, advancement, and implementation. Huge speculations should be completed in building an exceptionally solid framework for security of company's technology and information. The companies which are small and medium in size work in a different manner as compared to a company which is larger in size. SMEs don't actualize the digital risk control framework found in multi-associations like information security auditors, manager, security professionals or different rules and policies.

Inside the domain of a small and medium-sized firm, cyber associated protection should be executed taking its constrained assets and spending plan into thought. It was discovered that at any rate half of the SMEs were not utilizing the most well-known and basic digital security assurance of implementing a firewall or setting anti-virus software. Keeping the previous idea into consideration, digital assailants have expanded their scope more towards the companies that are not large, as these SMEs are simple targets for them. It is even easy for them to hack into their networks within very less time period because of the type of protection used by these companies.

In the course of recent years, the interest for the SME offered services has exceptionally expanded. In the following research, many of the major digital security risks and dangers have been identified and how these threats have impacted the working of SMEs, especially in the United Arab Emirates. Monetary spending plans and expertise of technological expertise are few of the limitations where small and medium sized firm would prefer not to put resources into the insurance component.

The study gives comprehension of such criminal activities and how to alleviate them at a negligible expense. When dangers are surely known by the SME and the right insurance is executed, the company would have the capacity to accomplish their focused on results with no interruption in their administrations. The further research could incorporate investigating more digital security dangers, for example, utilization of unauthorized gadgets, social engineering, and unauthorized use of company computers, which are as yet persevering inside a small sized firm and how these companies can protect themselves against cyber-related crimes.

6.2 Recommendation

The recommendations for the research and its findings are given below for the SMEs to prevent themselves from getting attacked by cyber criminals. It is important for these small and medium-sized enterprises to stay vigilant and alert at all times as they are more vulnerable to cyber-attacks compared to large sized companies.

- The employees of the companies must be trained well and stay alerted in case of any emails asking for sensitive information regarding their company. It is an important fact to consider that a genuine company would never ask for another company's personal and sensitive data.
- It is recommended that the employees always keep their spam filters turned on for their emails. In this way, any unnecessary email would automatically go to the 'spam' folder and will be deleted within a 30 day time period. Spam filters are important as these filters can also detect viruses sent in the form of an email.
- Organizations ought to get their employees well trained to make sure that they are careful about spontaneous messages, especially those that request a rapid reply because such responses do not give much time to the employee to think whether to reply or not to.

- It is recommended that the companies save the important data in different locations and must constantly back up their data and keep the system updated.
- Firewalls, anti-virus and malware protection software must be installed on all the systems in order to prevent any unauthorized access to the system. The firewalls protect the system against any outside threat. However, the hackers of today have become cleverer and have found ways to breach firewalls and anti-virus software. Therefore, it is necessary that the applications are being updated constantly and leave no room for a breach.
- The potential harm from a conscious or indiscreet documents' leaking by the employees ought not to be neglected. Constraining the amount of information that can be accessible to the employees is a key stride towards moderating the span of any information leaking.
- It is additionally critical to consider managing the utilization of data storing gadgets that are portable (such as USBs), media players and versatile hard drives. In specific circumstances, organizations can likewise consider the monitoring of the behavior of an employee over the internet. For instance, keeping track of all the websites visited by the employees.
- If an employee resigns from the company or is fired, his/her digital access must be instantly blocked so that they do not get the time to access their account and copy any sensitive information of the company.
- In order to protect the data stored on the smartphones of the employees, all employees' cell phones must be embedded with an application that self-destructs the data when the phone is stolen. This application can be accessed from any other nearby device so that their cell phones can be cleaned before the perpetrators could get their hands on the information. This is an important step because the security of personal gadgets is often very low and has the highest risk of getting breached.
- When utilizing portable storage devices, it is highly recommended that those devices are embedded with encryption software. Encrypting the data will save it from getting into the wrong hands. It is also important that the encryption codes are made in such a way that decrypting them becomes difficult for the thieves.
- A future study is also recommended in order to get a better insight on the issue of cyber threats and study it from different perspectives.

References

Bailey, T., Miglio, A.D. & Richter, W. (2014). The rising strategic risks of cyber attacks. *McKinsey Quarterly*, vol. 2, pp. 17-22 [Online]. [Accessed on 1 May 2017]. Available at: http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks

Bryman, A. & Bell, E. (2011). *Business research methods.* 3rd ed. Oxford: Oxford University Press.

Center for Strategic and International Studies. (2013). *THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE* [online]. [Accessed 28 September 2016] Available at: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

Cherrayil, K. N. (2015). Cybercrime impacts more than 2m UAE citizens. *Gulf News* [online] 3 October 2016. [Accessed 30 September 2016]. Available at: http://gulfnews.com/business/sectors/technology/cybercrime-impacts-more-than-2m-uae-citizens-1.1626294

Choras, M., Kozik, R., Torres Bruna, M.P., Yautsiukhin, A., Churchill, A., Maciejewska, I., ... & Jomni, A. (2015). Comprehensive Approach to Increase Cyber Security and Resilience [online]. In *Availability, Reliability and Security (ARES), 2015 10th International Conference on* (pp. 686-692). IEEE. [Accessed 17 May 2016] Available at: http://www.fp7-camino.eu/assets/files/CAMINO-ARES.pdf

Creswell, J. & Clark, V. (2011). *Designing and conducting mixed methods research*. 2nd ed. Thousand Oaks, CA: Sage.

Duncan, G. (2016). Cyberattacks in the UAE: The threat to your wallet. *The National* [online] 3 June. [Accessed 29 September 2016]. Available at: http://www.thenational.ae/business/personal-finance/cyberattacks-in-the-uae-the-threat-to-your-wallet#full

Etzioni, A. (2011). Cyber security in the Private Sector. *Issues in Science and Technology*, vol. 28 (1), pp. 58.

Gendron, A. (2013). Cyber threats and multiplier effects: Canada at risk. *Canadian Foreign Policy Journal*, vol. 19 (2), pp. 178-198.

Gupta, A. & Hammond, R. (2005). Information systems security issues and decisions for small businesses. *Information Management & Computer Security*, vol. 13 (4), pp. 297-310.

Hadbini, A. M. (2014). The Rise of Cybercrime in Dubai and UAE. [online]. [Accessed 30 September 2016]. Available at: https://securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae/

Han, D. R. (2012). SME Cyber security and the Three Little Pigs [online]. *ISACA Journal*, vol. *6*, pp. 37. [Accessed 16 May 2016]. Available at: http://www.isaca.org/Journal/archives/2012/Volume-6/Pages/SME-Cybersecurity-and-the-Three-Little-Pigs.aspx

Herath, T. & Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. *Decision Support Systems*, vol. 47 (2), pp. 154-165.

Hughes, J. & Cybenko, G. (2013). Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cyber security. *Technology Innovation Management Review*, vol. 3 (8), pp. 15–24.

Jhon, I. (2015). One-third of UAE firms in cyber security breaches. *Khaleej Time* [online] 21 December. [Accessed 17 May 2016]. Available at: http://www.khaleejtimes.com/business/local/one-third-of-uae-firms-in-cyber-security-breaches-

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review*, vol. *4* (11).

Kaur, J. & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME. Research and Innovation in Information Systems (ICRIIS). *International Conference on Research and Innovation in Information Systems (ICRIIS)*, pp. 286-290.

Kelly, B.B. (2012). Investing in a centralized cyber security infrastructure: Why "hacktivism" can and should influence cyber security reform. *Boston University Law Review*, vol. 92 (5), pp. 1663–1711.

Kozik, R. & Choras, M. (2013). *Current cyber security threats and challenges in critical infrastructures protection.* In Informatics and Applications (ICIA), 2013 Second International Conference on, pp. 93-97. IEEE.

Kroll. (2015). *Data Breach Best Practices to Safeguard Data* [online]. [Accessed 17 May 2016]. Available at: http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-breach-prevention-tips

Loveland, G. & Lobel, M. (2012). *Cybersecurity: the new business priority.* [online]. [Accessed 29 September 2016]. Available at: http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.html

Madzima, K., Moyo, M. & Abdullah, H. (2014,). *Is bring your own device an institutional information security risk for small-scale business organizations?.* In Information Security for South Africa (ISSA). IEEE.

Mallinder, J. & Drabwell, P. (2014). Cyber security: A critical examination of information sharing versus data sensitivity issues for organizations at risk of cyber-attack. *Journal of business continuity & emergency planning*, vol. *7* (2), pp., 103-111.

Miron, W. & Muita, K. (2014). Cyber security Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review*, vol. *4* (10).

Muegge, S. & Craigen, D. (2015). A Design Science Approach to Constructing Critical Infrastructure and Communicating Cyber security Risks. *Technology Innovation Management Review*, vol. *5* (6), pp. 6.

Neuman, W.L. (2013) Social Research Methods: Qualitative and Quantitative Approaches. 7th edn. Harlow:Pearson Education Ltd.

Northcutt, S. (2016). Security Controls. [online]. [Accessed 29 September 2016]. Available at: http://www.sans.edu/research/security-laboratory/article/security-controls

Payette, J., Anegbe, E., Caceres, E. & Muegge, S. (2015). Secure by Design: Cyber security Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review*, vol. *5*(6), pp. 26.

Quigley, K., Burns, C. & Stallard, K. (2015). 'Cyber Gurus': a rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly*, vol. *32*(2), pp. 108-117.

Rahman, H.A., Martí, J.R. & Srivastava, K.D. (2011). A Hybrid Systems Model to Simulate Cyber Interdependencies between Critical Infrastructures. *International Journal of Critical Infrastructures*, vol. 7(4), pp. 265–288.

Saunders, M., Lewis, P. & Thornhill, A. (2012). *Research Methods for Business Students.* 6th edn. Harlow, England: Prentice Hall.

Seals, T. (2015). *Insider Threats Responsible for 43% of Data Breaches* [online]. [Accessed 29 September 2016]. Available at: http://www.infosecurity-magazine.com/news/insider-threats-reponsible-for-43/

Sekaran, U. (2003). *Research methods for business*. 4th edn. Hoboken, NJ: John Wiley & Sons.

Silverman, D. (2011). Interpreting qualitative data: methods for analysing talk, text and interaction. London: Sage.

Sood, A. & Enbody, R. (2014). *Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware*. Elsevier Science

Sveen, F., Rich, E. & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Information Systems Frontiers*, vol. 9(5), pp.481.

Symantec. (2016). Security Response Publications [online]. [Accessed 29 September 2016]. Available at: https://www.symantec.com/security_response/publications/monthlythreatreport.jsp

Teddlie, C. & Tashakkori, A. (2009). *Foundations of mixed methods research: Integrating quantitative and qualitative approaches in the social and behavioural sciences*. Los Angeles: Sage.

Thekkepat, K.S. (2016). UAE government among top 20 in cybersecurity [online]. *Friday Magazine*. [Accessed 18 May 2016]. Available at: http://fridaymagazine.ae/features/uae-government-among-top-20-in-cybersecurity-1.1653134

Ville, D. (2011). The SME security challenge. *Computer Weekly* [online]. [Accessed 18 May 2016]. Available at: http://www.computerweekly.com/opinion/The-SME-security-challenge

Zikmund, W.G. (2003). Business Research Methods. OH: Cengage South-Western.

APPENDIX 1: QUESTIONNAIRE

Gender

- Male
- Female

Age group

- 25-30
- 31-35
- 36-40
- 40 above

Do you think small and medium enterprises feel secure behind their envisioned cover of irrelevance and humble business?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Small and medium-sized enterprises frequently utilized method for access to their bigger accomplices and suppliers by these cyber criminals?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Do you think criminals associated with cyber-crime would target any firm?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Are you sure executing crisis measures and possibly advising the customers of the company?

- Strongly disagree
- Disagree

- Neutral
- Strongly agree
- Agree

Do you think cyber-crime has significant risks faced by almost all the companies?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Are you sure small that there is a severe sense of unpreparedness in small businesses when it comes to dealing with the potential cyber crisis?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Do you think almost half of the small business in the UK has no plan in place to deal with data breach?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Do you think SMEs consider threats to be sufficiently genuine for a risk management program?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

Is there a fact that the level of complexity intending to dangers differs broadly in the company?

- Strongly disagree
- Disagree
- Neutral

- Strongly agree
- Agree

Do you think cyber security breach could leave a huge impact on a company?

- Strongly disagree
- Disagree
- Neutral
- Strongly agree
- Agree

APPENDIX II: INTERVIEW QUESTIONS

- What do you know about different kinds of cybercrime?
- What are your views regarding the awareness of SMEs regarding cyber crime?
- How the awareness of employees regarding cybercrime can be increased?
- What are some of the preventive measures that can be taken to prevent cyber crime?