**Contemporary Cyber Security Practices: An Evidence from the IT industry of UAE**

**Department of Management Sciences**

**SUC, SHJ, UAE**

**Approval Sheet**

**Copyright Form**

**Acknowledgement**

As part of my acknowledgements, firstly I would like to thank my God who gave me the knowledge, strength and opportunities to be in the position to complete this thesis.

I would also like to thank DR. Mohammed Kamaruddeen Head of Campus and management of SUC for approving and giving me the opportunity to be a part of the MBA program.

Furthermore express a deep sense of gratitude to my internal guide and supervisor DR. Mohammed Kamaruddeen, for sharing his invaluable experience, knowledge, guidance and useful suggestions which helped me in all the stages in order to complete the thesis work on time.

I would also like to appreciate all the professors of SUC Sharjah, for their encouragement and cooperation which had been a source of inspiration and valuable assistance for me.

I would also like to thank all the respondents for participating in filling out the questionnaires and sharing their honest opinions.

Finally, yet importantly, i would also like to express heartiest thanks to my parent for their blessings, my friends and colleagues for supporting me and helping me in stimulating discussions as well as providing moral and spiritual support.

**Khalifa Ahmed (17365)**

**Abstract**

Cyber security has turned out as the most threatening risk for business nowadays. Along with the growth of Information Technology, cyber security has also emerged and even has ranked as the top 10 threats toward the business in these modern days. The digital world has triggered the rise of cyber-attacks, and for this reason, tech-focused companies have started to recognize the need for implementing or improving cyber security systems to secure their business. Implementing a Cyber Security into the company now defines as managing with a developing role; facing the new demands of visibility into business operations, also the new expectations for information and privacy protection. This research covers a complete Contemporary cyber security practice evidence of IT industry**.**

**Key words: Cyber security, Threatening risk, Improving IT sector**

Contents

[**Approval Sheet** ii](#_Toc30733139)

[**Acknowledgement** iv](#_Toc30733140)

[Chapter 1 1](#_Toc30733141)

[1.1 Background Discussion 1](#_Toc30733142)

[1.2 SIGNIFICANCE OF THE STUDY 2](#_Toc30733143)

[1.3 Theoretical Contribution 2](#_Toc30733144)

[1.4 Applied Aspects 2](#_Toc30733146)

[1.5 Problem Statement 3](#_Toc30733147)

[1.6 Research objectives 3](#_Toc30733148)

[1.7 Rationale of the study 4](#_Toc30733149)

[1.8 Research questions 4](#_Toc30733150)

[1.9 Objective of the study 4](#_Toc30733151)

[1.10 Hypotheses development 4](#_Toc30733153)

[Chapter 2 5](#_Toc30733154)

[Literature Review 5](#_Toc30733155)

[2.1 Theoretical Framework 9](#_Toc30733156)

[2.2 SYNTHESIS OF LITERATURE 9](#_Toc30733157)

[Chapter 3 10](#_Toc30733158)

[Research Methodology 10](#_Toc30733159)

[3.1 Research Design 10](#_Toc30733160)

[3.1.1 Research Approach 10](#_Toc30733161)

[3.1.2 Type of investigation 10](#_Toc30733162)

[3.1.3 Unit of Analysis 10](#_Toc30733163)

[3.1.4 Time Horizon 11](#_Toc30733164)

[3.1.5 Research Strategy 11](#_Toc30733165)

[3.2 Research Methodology 11](#_Toc30733166)

[3.2.1 Population of the study 11](#_Toc30733167)

[3.2.2 Tool for Data Collection 11](#_Toc30733168)

[3.2.3 Data Collection Method 11](#_Toc30733170)

[3.2.4 Pilot Study 12](#_Toc30733171)

[3.2.5 Response rate 12](#_Toc30733172)

[3.2.6 Data Analysis Software and techniques 12](#_Toc30733173)

[CHAPTER 4 13](#_Toc30733174)

[DATA ANALYSIS AND RESULT’S DISCUSSION 13](#_Toc30733175)

[4.1 Chapter Introduction 13](#_Toc30733176)

[4.2 Data coding and recording 13](#_Toc30733177)

[4.3 Preliminary Analysis 13](#_Toc30733178)

[4.3.1 Analysis of Reliability of Data 14](#_Toc30733179)

[4.4 Frequency Analysis of survey 14](#_Toc30733180)

[4.5 Descriptive Statistics 19](#_Toc30733181)

[4.6 Correlation Analysis 20](#_Toc30733182)

[4.7 Regression Analysis 22](#_Toc30733183)

[CHAPTER 5 24](#_Toc30733184)

[CONCLUSION AND RECOMMENDATIONS 24](#_Toc30733185)

[5.1 CONCLUSION AND RECOMMENDATIONS 24](#_Toc30733186)

[5.2 Summary of Results 24](#_Toc30733189)

[5.3 Suggestions and Recommendations 25](#_Toc30733190)

[5.4 Conclusion 26](#_Toc30733191)

[References 27](#_Toc30733192)

[Appendix 1: Questionnaire 29](#_Toc30733193)

# Chapter 1

**Introduction**

## Background Discussion

It is a fact that cyber-attacks are a big threat to infrastructure and systems of companies, individuals and government. The use of technology is increasing with the passage of time, and this increased use is also coming up with several issues and vulnerabilities in the information technology systems. Keeping the cyber security attacks in mind, where credit cards data has been stolen, ATMs are not working, and mutual fund companies are unable to operate; all of them need to consider some counter measures.

If any technology is used on a small scale, its issues and problems can also be small, but when things have become huge part of daily life and businesses as information technology has become, then its relevant issues are obvious to happen. That’s why it is critical for individuals and companies to stay alert and come up with various countermeasures so that they can avoid cyber-attacks in the first place, and if they do happen, then they must have a plan to deal with those threats (Amoroso, 2012).

Cyber security is one of the biggest concerns of recent times, and if considerable countermeasures will not be taken by stakeholders, then they may face severe consequences. The individuals, companies, and governments should come up with policies and systems to protect their data and sensitive information by developing and implementing above mentioned countermeasures because this is the only way to effectively deal with cyber security issues.

The companies are required to ensure that they are following the policy guidelines provided by the government and experts to keep countermeasures in their cyber security systems. If they will follow the policy guidelines and come up with a comprehensive strategy, then they has been in a better position to resolve vulnerabilities in their systems, and if something wrong happens, they would be better in making a response to those cyber-attacks (cyber defense magazine, 2019).

Cyber security has turned out as the most threatening risk for business nowadays. Along with the growth of Information Technology, cyber security has also emerged and even has ranked as the top 10 threats toward the business in these modern days. The digital world has triggered the rise of cyber-attacks, and for this reason, tech-focused companies have started to recognize the need for implementing or improving cyber security systems to secure their business. Implementing a Cyber Security into the company now defines as managing with a developing role; facing the new demands of visibility into business operations, also the new expectations for information and privacy protection. This research covers a complete Contemporary cyber security practice evidence of IT industry.

## 1.2 SIGNIFICANCE OF THE STUDY

## 1.3 Theoretical Contribution

## The researcher hasn’t found any study addressing that particular area hence the present study appears to be great contribution to body of knowledge.

## 1.4 Applied Aspects

The IT firms across the world will benefit from this particular research as the findings appear to be of highly applied in nature.

## 1.5 Problem Statement

Cyber threats and data breaches are getting common in society as information technology is improving and advancing. In the presence of such security threats, it is becoming difficult to make IT industry secure and data breaches controlled. Credit cards and banking system are also a point of attention for these security threats and cybercrimes. In short, cyber threats are a problem for cyber security. Keeping the same in view, the researcher planned to conduct a study to analyze the selected contemporary cyber security practices namely unauthorized access, suspicious activities and security measures, being implemented in the IT sector of UAE, and their impact on overall cyber security phenomenon

## 1.6 Research objectives

The key objectives of this research work are enlisted below:

1. To examine the impact of unauthorized access on the cyber security
2. To identify suspicious activities in IT industry
3. To explain the significance of the security measures for cyber security.

## 1.7 Rationale of the study

The rationale of this research study is the prime reason for conducting this research work. IT security issues are becoming a problem for the strength of the industry. IT security issues are also causing problems for customers availing services of banks and credit cards. Moreover, another reason is to identify problems which need to be controlled and managed for secure IT system (Hasib, 2014).

## 1.8 Research questions

Q1. What is the impact of unauthorized access on the cyber security?

Q2. What are the suspicious activities in IT industry?

Q3. What is the significance of the security measures for cyber security?

## 1.9 Objective of the study

## To analyze the selected contemporary cyber security practices such as unauthorized access, suspicious activities and security measures and their impact on overall cyber security

## 1.10 Hypotheses development

The hypotheses development is as given:

H1: Unauthorized access has an association with the cyber security threats.

H0 Unauthorized access has no association with the cyber security threats.

H2: Suspicious activities in IT industry has an association with the cyber security.

H0: Suspicious activities have no association with cyber security.

H3: Security measures have an association with cyber security threats

H0: Security measures have no association with cyber security threats.

# Chapter 2

# Literature Review

It is evident due to so many cyber-attacks that cyber-criminals are getting sophisticated with their approach, and if they continue in this fashion, then there will be more severe challenges for individuals and companies to deal with. There is a need to use the technology of automated security intelligence which keeps an automatic eye on systems, and if any vulnerability or issue is found, it is quickly detected (Gantz & Philpott, 2012). The role of AI can be crucial in placing considerable countermeasures so companies should use the essence of AI to improve cybersecurity. In addition to that, all security systems should be updated and they are placed in every aspect of the IT infrastructure so that attackers may experience resistance at every point (Shinichiro, 2017).

As Kazan (2016) described that as a function of five fundamental attributes of protected computing device, as well as the information security such as the confidentiality, accuracy, integrity, availability as well as authenticity, the effectiveness of the latest computer applications is usually observed. The concepts of the cyber security are usually applicable to different areas or the different departments such as education, government systems as well as the ordinary lives of the private individuals. The extended applications which are runnable on the internet or the special internet applications are involved by normally considerations with the name of cyber security.

As stated by Kazan (2016), the process to maintain as well as achieving secure cyberspace is very difficult and complex, as well as it also concerns with intellectual property, sustainability, privacy, the critical infrastructure as well as the personal identity of the organization. The threats for making secure the operating infrastructure are profound as well as serious such as cybercrime, cyber terrorism, cyber espionage as well as a cyber war for the kind of the technical community has responded with the procedures as well as safeguards and normally the private sector supplies. The whole study gives very brief information on the security within the cyber domain with the objective of the developing techniques of cyber security (Kazan, 2016).

As stated by Knowles, Prince, Hutchison, & Jones (2015), in isolation, it is operated by the contemporary industrial control system while distinguished networks are used such as the internet as well as the corporate networks, for the facilitation as well as for improving the business process. Furthermore, exposure to cyber threats increases the consequences of this kind of development. The whole survey of this study tells about the recent techniques and methodologies as well as the research to calculate the effects of the risks as well as handle those risks effectively.

Knowles, Prince, Hutchison, & Jones (2015) also described that it has identified by the dearth of the security metrics for the specific industrial control system as a hurdle for the implementation of this kind the methodologies. Therefore, an agenda is outlined in the industrial security control system metrics for future research. To handle the fail-secure as well as a fail-safe of the industrial control system operations, the concept of functional assurance is also introduced (Knowles, Prince, Hutchison, & Jones, 2015).

As stated by Scully (2014), the attitudes that ‘it won’t happen to me’ still overcome within the industry’s boardrooms at the time of the consideration on the senior the executives of the threats of the cyber interruptions. In the commercial world of the cyber security, not too much changes occurred in the previous few years such as the data breach drivers, hackers or the attackers are not being confronted for identification of the new ways for the stealing the sensitive information as well as the intellectual property of the companies or the organizations. Furthermore, the consequences of the even main breaches of the security seem not to become felt by the leaders of those organizations which are a victim.

Furthermore, some questions are also raised in this study which is discussed in Scully (2016) which are: why is it so? Surely the practitioners or experts of the security of IT are determining the new methods for the identification as well as preventions of the chosen interruptions within the networks of the organizations? Are the consequences of the chosen interruptions as too much importantly, which the leaders of the organization tolerate them, or do only distinctions feel of the failure pain? The whole study is exploring all of the possible threats which can cause the failure of cyber security in the very beginning within the industry as well as contends. On the other side, the leaders of the industry must not be along for taking the responsibilities for such kind failures in the cyber security as well as they should take the initiative to prevent the cyber-attacks by making the lives of hackers harder. The concepts of cyber security are usually applicable to different areas or the different departments, such as education, government systems, as well as the ordinary lives of private individuals. Moreover, the leaders of the companies cannot wait for the governmental policy, coordination, or strategy for the leadership. The study is suggesting some kind of calculations that a chief executive officer may adopt for making a new approach for the company to increase cyber security (Scully, 2014).

As described by Nissenbaum (2005),the study on cyber security, which is determining the conception of the security into the two different ways within the contemporary concerns on the vulnerability of the networks as well as the computers for the hostile attack. In computer science as well as engineering ,the one conception is derived from the conceptions of focuses of the individual of computer security, which is developed. The concepts of the cyber security are usually applicable to different areas or the different departments such as education, government systems as well as the ordinary lives of the private individuals. Therefore, an agenda is outlined on the industrial security control system metrics for future research.

In the commercial world of the cyber security, not too much changes occurred in the previous few years such as the data breach drivers, hackers or the attackers are not being confronted for identification of the new ways for the stealing the sensitive information as well as the intellectual property of the companies or the organizations. The concerns of the security of the national agencies of the government information to others, as well as the distinguished owner of the intellectual property, are also informing others. In the last, the Copenhagen school of the international relations develops the securitization as well as the evaluation comparatively of this tow the conception are also using the theoretical construct of the securitization (Nissenbaum, 2005).

As described by Hare (2009) that the examination of whether the review interruption of some foreign companies is related to the relations of the audit companies along with the multinational companies. The study is based on the listed companies in the study around115 companies of the stock exchange for the end of the year 1998. Furthermore, to find any kind of important distinctions that exist between those companies working on the audits, they all have used the nonparametric tool. The outcomes of the past researches on the delay of the audit appear that the companies related to those international companies were doing audits for the provision of the motivation to the small delays of the audit. Although, the study highlights that the multinational companies within Bangladesh have larger delays of audits with the 6.31 mean months, while the global mean month is 5.86 (Hare, 2009).

As stated by Cook, Smith, & Janicke(2016),the underpin complicated national infrastructure may be classified as the low-frequency events or the high impact when the cyber attacks on the industrial control system come into form. Furthermore, the range and the quantity of the cyber attacks against the total foot prints of the industrial control system is small, as well as the outcome there is an inadequate dataset for the assessment adequately for the threats for the operator of ICS, and up till now, the effects are potentially catastrophic to date. So, the study is determining the very important elements of the current science of the decision which may be utilized for informing as well as for improving the cyber security of industrial control system against the aggressive risks as well as it also appears the parts where further development work is needed for discovering the assessments of the risks. Moreover, the research study is also proving the detail of how the informative data from the generated processes for safety may inform the process of decision making. The study is also concluding by providing some recommendation on how a data set after validation which can be made for the supporting the investments within the cyber security of industrial control system (Cook, Smith, & Janicke, 2016).

As described by Tikk (2010) that the contemporary global regimes of cyber security, as well as this artiocle, tells that the main focus of the cyber security regime is on the number of the different role of the multination organizations. The approach of the prevailing of such companies is disjointed as well as at odds with the priorities of the national-level policy. Furthermore, a comprehensive approach is required for the rectification of such kind conditions as well as it also increases the cyber security. For the acknowledgment, the full array of cyber threats as well as it also combines the dissimilar actors at the level of the country. Furthermore, the provided traditional profile is exclusively located for becoming the sources of such kind of comprehensive framework (Tikk, 2010).

## 2.1 Theoretical Framework

**Theoretical Framework**

**Independent Variables Dependent Variable**

Unauthorized Access

Cyber Security

Suspicious activities

Security measures

## 2.2 SYNTHESIS OF LITERATURE

The literature review indicates that the researches carried out in the past were addressing the factors, obstacles and processes in IT security.

The researcher hasn’t found any study addressing that particular area of Cyber Security practices in the IT industry that the present study appears to be contributing to body of knowledge while analyzing the selected contemporary cyber security practices namely unauthorized access, suspicious activities and security measures, being implemented in the IT sector of UAE, and their impact on overall cyber security phenomenon.

The absence of a study addressing the above factors is a clear cut knowledge gap and this research is an attempt to fill in that gap

# Chapter 3

# Research Methodology

For the current research work the questionnaire, regarding the cyber security, is used. It is distributed among 350 employees of 6 IT firms in UAE. SPSS is used to perform the tests on the data and evaluate the results. The correlation and the regression analysis is better suggested be used for the data analysis purposes.

## 3.1 Research Design

## 3.1.1 Research Approach

There exist various forms of the study. For the current research work, it is confirmed that the nature of the study is quantitative. The data nature better helped to evaluate the methodology for the said research. There exists the numerical data if it is the case of the quantitative methodology. In order to collect the data from the respondents, the self-administered survey is conducted.

## 3.1.2 Type of investigation

In order to get the desired results from the data, it is suggested to make use of the correlation analysis. Also, the use of correlation analysis is determined due to the numerical nature of the data. The use of regression analysis made it possible to decide whether to accept or reject the hypotheses.

## 3.1.3 Unit of Analysis

The data collection is based on the professionals of the IT firm. So, an employee who is working in the IT firm is the unit of analysis.

## 3.1.4 Time Horizon

This study is cross- sectional in nature based on the fact that the data is gathered for just once. There is no need for the follow ups for the data collection purposes.

## 3.1.5 Research Strategy

The data is collected by making use of the questionnaire. These are distributed among the individuals of IT firm in order to get their responses.

## 3.2 Research Methodology

The self-administered survey better helped to achieve the purpose of the study. The questionnaire is perceived to be the simple and quick tool for the data gathering purposes. The questionnaire is provided with the five-point likert scale having its range from 1 to 5. A questionnaire is if complete only then it is accepted for the analysis purposes.

## 3.2.1 Population of the study

Six IT companies were selected. Their names are kept confidential as advised by them. The population is all about the officer level employees involved in IT operations of the firm. The unit of analysis helped to determine the study population..

## 3.2.2 Tool for Data Collection

## The tool for this particular research was adapted from the part researches

## 3.2.3 Data Collection Method

The primary data collection is based on the self-administered survey. The questionnaire is considered to be the economical and the cheap resource for the data collection.

## 3.2.4 Pilot Study

The pilot study tends to determine both the instrument’s validity and the data reliability. The sample size of 25 employees is being taken for the pilot study. The value of Cronbach Alpha for all the study items is greater than 0.70 which depict the high reliability of the study items on the questionnaire.

## 3.2.5 Response rate

The questionnaires which are distributed among the employees of the IT firms in UAE are being filled and returned back for the analysis purposes. Out of 350 questionnaires, the count returned is 298 which depict 85% of the response rate.

## 3.2.6 Data Analysis Software and techniques

The data analysis is performed by making use of SPSS (Statistical Package for the Social Sciences), version 22. First the organized data is entered to the excel sheet. The data from the excel sheet is then copied & pasted to the SPSS. The reliability analysis, correlation analysis and regression analysis are performed by making use of SPSS.

The SPSS results will be helpful to determine if any technology is used on a small scale, its issues and problems can also be small, but when things have become huge part of daily life and businesses as information technology has become, then its relevant issues are obvious to happen. That’s why it is critical for individuals and companies to stay alert and come up with various countermeasures so that they can avoid cyber-attacks in the first place, and if they do happen, then they must have a plan to deal with those threats (Djekic, 2019; Bauman, Toomey, & Walker, 2013).

# CHAPTER 4

# DATA ANALYSIS AND RESULT’S DISCUSSION

## 4.1 Chapter Introduction

In chapter 4 of the current research work, the coding as well as the decoding of the gathered data is provided which better helped to make usage for Statistical Package for the Social Sciences (Version 22 of SPSS). The results obtained after performing different tests on the data as well as the relevant interpretations are the part of current chapter. There are certain categories & the digits which are first defined for each of the item of the questionnaire. In this chapter, the details about the demographics, the reliability analysis, descriptive statistics, and coefficient for correlation and analysis for regression are also discussed. Varying scale as well as the categories which are assigned to the questionnaire items better helped to evaluate the questionnaire items.

## 4.2 Data coding and recording

Initially, excel sheet has been used for data recording. It was then transformed the SPSS platform by copying the data from the excel sheet and pasting the same to the Version 22 of the SPSS. For current research work, questionnaire is being used. Different types have been assigned to both the study dependent as well as independent variables are assigned as per scale for response on the questionnaire.

## 4.3 Preliminary Analysis

In order to evaluate the data and to interpret the results, SPSS is used. Data set reliability is determined by Value of Cronbach Alpha. The mean and the standard deviation are also given. The association of the parameters is evaluated by the use of correlation coefficient. The regression analysis helped to make decisions whether to accept or reject the study hypotheses. The main aim behind conducting these tests is to determine the reliability as well as the association of the study dependent and the independent variables.

The questionnaire contains two parts as given:

* Demographics (for current work they are treated as the control variables)
* The dependent & independent variables of study.

Particular categories and digits are assigned to the variables first and then the data is gathered from the respondents. For the demographic variables, the assigned categories are as given:

## 4.3.1 Analysis of Reliability of Data

The data reliability is accessed by using the value of Cronbach Alpha. The range for the Cronbach Alpha lies between 0 and 1. It shows that all the items of the questionnaire are better evaluated on the similar concept & idea. The data set for which Cronbach Alpha value is more than 0.70 it means that the data is highly reliable (Nunnallly, 1978). For current research work, the overall Cronbach Alpha value is given in table 4.1.

**Table 4.1: Value of Cronbach Alpha**

|  |  |
| --- | --- |
| **Analysis for Reliability** | |
| **Cronbach Alpha** | **N of Items** |
| .870 | 10 |

The above table is showing that the overall Cronbach Alpha value is greater than 0.70 i.e., .870. It shows high reliability for data items.

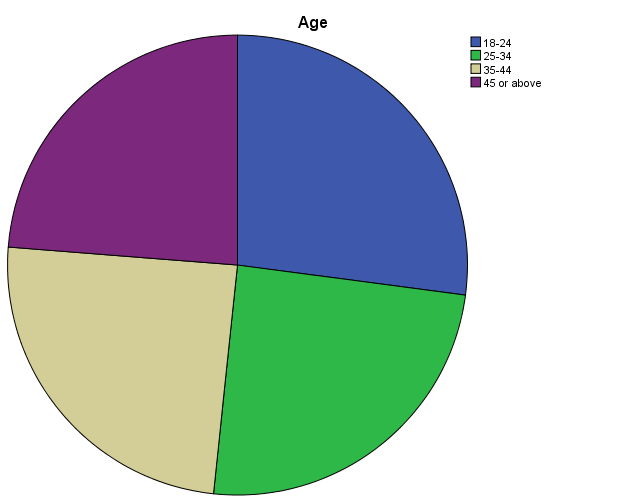
## 4.4 Frequency Analysis of survey

The responses of the respondents are better evaluated through the frequency distribution. Following is given the frequency distribution along with the respective pie-charts for the demographic variables.

|  |
| --- |
| **Table 4.2: age** |

**Interpretation**

The information related to the frequency distribution and the relevant percentages for the respondents of the age is given in the table 4.2. 27.6% of the respondents are a part of the age range 18-24 years and the frequency for the said age range is 65. 24.4% of the respondents belong to the age series of 25-34 years and the relevant frequency is 59 respondents. The respondents which belong to the age range of 35-44 years and 45 or above have the frequency of 59 and 57 respondents along with the relevant percentages of 24.4% and 23.6% respectively. Most of the respondents are the part of age range 18-24 years with 27.6%.



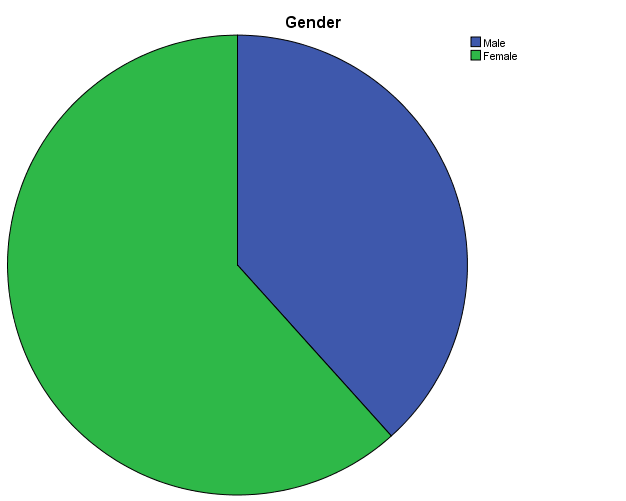
**Interpretation**

The varying percentages for the respondents of the age are shown with various attractive colors in the above pie-chart. The major area of the pie-chart is covered by blue color which is showing the frequency of the age range 18-24 years. At the second, third and the fourth number are the age series 25-34 years, 35-44 years & 45 or above which are shown in the pie-chart by the colors green, yellow and purple respectively.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Table 4.3: gender** | | | | | |
|  | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Male | 92 | 38.8 | 38.3 | 38.3 |
| Female | 148 | 61.2 | 61.7 | 100.0 |
| Total | 240 | 100 | 100.0 |  |
|  | |  |  |  |  |

**Interpretation**

The details related to the frequency distribution and the relevant percentages for the respondents of the gender are given in the table 4.3. 61.2% of the respondents are a part of the gender female with the frequency 148. 38.8 % of the respondents are a part of the gender male with the frequency 92. This frequency distribution shows that most of the respondents are the female.



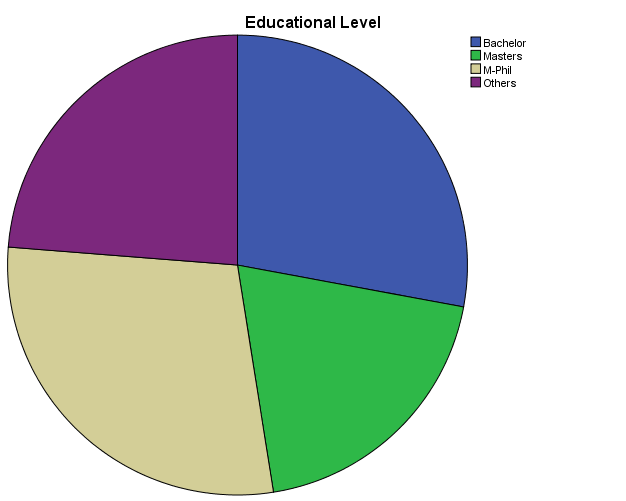
**Interpretation**

The varying percentages for the respondents of the gender are shown with various attractive colors in the above pie-chart. The major area of the pie-chart is covered by green color which is showing the frequency of the female gender. At the second number is the gender male which is shown in the pie-chart by the blue color.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Table 4.4: Educational Level** | | | | | |
|  | | Frequency | Percent | Valid Percent | Cumulative Percent |
| Valid | Bachelor | 67 | 28.5 | 27.9 | 27.9 |
| Masters | 47 | 19.4 | 19.6 | 47.5 |
| M-Phil | 69 | 28.5 | 28.7 | 76.3 |
| Others | 57 | 23.6 | 23.8 | 100.0 |
| Total | 240 | 100.0 | 100.0 |  |
|  | |  |  |  |  |

**Interpretation**

The information related to the frequency distribution for the educational level and the relevant percentages for the said respondents is given in the table 4.4. 27.6% of the respondents are a part of the bachelor’s degree and the frequency for the said educational level is 67. 19.4% of the respondents belong to the Masters degree and the relevant frequency is 47 respondents. The respondents which belong to the M-Phil and the Others educational level have the frequency of 69 and 57 respondents along with the relevant percentages of 28.5% and 23.6% respectively. Most of the respondents are the part of the educational level M-Phil with the frequency 69.



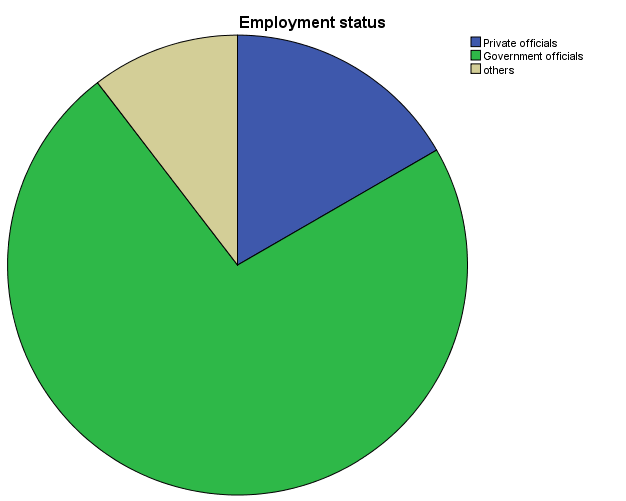
**Interpretation**

The varying percentages for the respondents of the educational level are shown with various attractive colors in the above pie-chart. The major area of the pie-chart is covered by skin color which is showing the frequency of the educational level M-Phil. At the second, third and the fourth number are the respondents from the Bachelors, Others and Masters which are shown in the pie-chart by the colors blue, purple and green respectively.

|  |
| --- |
| **Table 4.5: employment status** |

**Interpretation:**

The details related to the frequency distribution for the employment status and the relevant percentages for the said respondents are given in the table 4.5. 17.4% of the respondents are serving as the private officials and the frequency for the said employment status is 40. 72.3% of the respondents are the government officials and the relevant frequency is 175 respondents. The respondents which belong to the Others employment status have the frequency of 25 respondents along with the relevant percentage 10.3%. Most of the respondents are the part of the employment status as the government officials with the frequency 175.



**Interpretation**

The varying percentages for the respondents of the employment status are shown with various attractive colors in the above pie-chart. The major area of the pie-chart is covered by green color which is showing the frequency of the employment status government officials. At the second and the third number are the respondents from the private sector and others which are shown in the pie-chart by the colors blue and skin respectively.

## 4.5 Descriptive Statistics

**Table 4.6: Mean & Standard Deviation**

**Descriptive Statistics**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | N | Minimum | Maximum | Mean | Std. Deviation |
| Unauthorized access | 240 | 2.00 | 5.00 | 4.4583 | .55738 |
| Suspicious activities | 240 | 2.00 | 5.00 | 4.3278 | .62489 |
| Security measures | 240 | 2.00 | 5.00 | 4.4708 | .61466 |
| Cyber security | 240 | 2.50 | 5.00 | 4.2500 | .74878 |
|  |  |  |  |  |  |

**Interpretation**

The data related to the mean and the standard deviation is given in the table 4.6. The mean values for all the study variables (i.e., Unauthorized access, Suspicious activities, Security measures, Cyber security) are greater than 4 (i.e., 4.4583, 4.3278, 4.4708 and 4.2500 respectively). The value 4 is if measured on the five-point likert scale it shows that the respondents are highly agreed to the statements of the questionnaire. The values .55738, .62489, .61466 and .74878 are showing the variance percentage of the study variables from the respective mean values.

## 4.6 Correlation Analysis

The association of the study variables can better be determined by the Pearson product moment correlation coefficient. It is developed by Karl Pearson in 1985. The test results for this coefficient lie between +1 and -1. For positive correlation, test result is +1. For no relationship, test result is 0. Negative relation between the variables is depicted by -1. The correlation analysis and its results are shown in table 4.7.

**Table 4.7: Correlation Coefficient**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Variables** | **Unauthorized access** | **Suspicious activities** | **Security measures** | **Cyber security** |
| **Unauthorized access**  Pearson Correlation  Sig. (2-tailed)  N | 1  240 |  | | |
| **Suspicious activities**  Pearson Correlation  Sig. (2-tailed)  N | .792\*\*  .000  240 | 1  240 |  | |
| **Security measures**  Pearson Correlation  Sig. (2-tailed)  N | .605\*\*  .053  240 | .664\*\*  .000  240 | 1  240 |  |
| **Cyber security**  Pearson Correlation  Sig. (2-tailed)  N | .590\*\*  .042  240 | .537\*\*  .018  240 | .516\*\*  .000  240 | 1  240 |

|  |
| --- |
| \*\*. Correlation is significant at the 0.01 level (2-tailed). |
| \*. Correlation is significant at the 0.05 level (2-tailed).  The relationship of the study dependent and the independent variables is determined by using the Pearson correlation coefficient. For p<0.01, the value of the Pearson coefficient is showing that there exist the strong positive correlation between the study dependent and the independent variables (i.e., Unauthorized access, Suspicious activities, Security measures, Cyber security). These variables are positively significantly associated with each other. 4.7 Regression Analysis  |  |  |  |  |  | | --- | --- | --- | --- | --- | | **Table 4.8: Model Summary** | | | | | | Model | R | R Square | Adjusted R Square | Std. Error of the Estimate | | 1 | 0.7a | 0.67 | 0.63 | .58879 | | a. Predictors: (Constant), Unauthorized access, suspicious activities, security measures | | | | |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Coefficientsa** | | | | | | | | Model | | Unstandardized Coefficients | | Standardized Coefficients | t | Sig. | | B | Std. Error | Beta | | 1 | (Constant) | .267 | .328 |  | .812 | .000 | | Unauthorized access | .529 | .114 | .394 | 4.653 | .000 | | Suspicious activities | .086 | .108 | .072 | .799 | .025 | | Security measures | .280 | .084 | .230 | 3.329 | .001 | | a. Dependent Variable: Cyber security | | | | | | | |

**Interpretation**

In the regression model, the value of R-Square provides the measure for the goodness-of-fit. This value tends to depict the %age variance change in the dependent variable due to the independent variables. Based on the regression analysis for the current data set, it is evaluated that the value of R is 0.7. As far as the value of R-square for the current study variables is concerned, it is 0.67. This value is determining a significant percentage change on the dependent variable (i.e., Cyber security) due to the study independent variables (i.e., Unauthorized access, suspicious activities, security measures). The value of adjusted R-square provides for a comparison between the study models. This value is 0.63 which shows that out of total variation narrated by the regression line, the variation %age is not that significant. In case we talk about the value of p for the regression model, this value is less than 0.05 for all the study independent variables. The value of p<0.05 shows that the study independent variables (i.e., Unauthorized access, suspicious activities, security measures) are positively significantly associated with the study dependent variable (i.e., cyber security). It can be said that these parameters better help to determine the payment card frauds which can have the varying reasons to take place.

# CHAPTER 5

# CONCLUSION AND RECOMMENDATIONS

## 5.1 CONCLUSION AND RECOMMENDATIONS

## In recent studies, it is concluded that the cybersecurity is needed more for the fields of IT, as cybercrime is getting threatening for IT fields. Cyber-attacks are a big threat to infrastructure and systems of companies, individuals and government. The use of technology is increasing with the passage of time, and this increased use is also coming up with several issues and vulnerabilities in the information technology systems. Cybersecurity is one of the biggest concerns of recent times, and if considerable countermeasures will not be taken by stakeholders, then they may face severe consequences. The companies are required to ensure that they are following the policy guidelines provided by the government and experts to keep countermeasures in their cybersecurity systems.

## Based in the study findings, it is concluded that the selected contemporary cyber security practices such as unauthorized access, suspicious activities and security measures have an association with overall cyber security threats.

## 5.2 Summary of Results

In this heading summary of findings can be done. In the recent world, cybercrime is becoming one of the most threatening crime, to reduce these threatening cyber security can be developed and essential methods can be described the effectively of this system and survey method can be used for the analysis with the sample size of 350 employees of 6 IT firms in UAE. SPSS is used to perform the tests on the data and evaluate the results. The correlation and the regression analysis is better suggested to be used for data analysis purposes. The data is quantitative and numerical in type.

The main objectives can be described in conducting the research such as to examine the impact of unauthorized access on cyber security, to explain the significance of the security measures for cyber security as well as to identify suspicious activities in the IT industry. The main objective of this research study is the prime reason for conducting this research work. IT security issues are becoming a problem for the strength of the industry. IT security issues are also causing problems for customers availing credit cards and other services of banks. The relationship between the variables that have been studied in the third chapter by using regression analysis as well as using correlational analysis.

The questionnaire includes some of the questions on the topic on which we want to conduct our study. These questionnaires are stated as: What is the impact of unauthorized access on the cybersecurity? What is the significance of the security measures for cybersecurity? What are the suspicious activities in the IT industry?

The data for the latest research work can be collected from the questionnaire and for secondary purposes data collected from previous research work. To obtain the purpose sample size of respondents 240 employees of 6 IT firms whom questionnaire can be filled. and we find a response rate of almost 80% from all over. First, the organized data is entered into the excel sheet. The data from the excel sheet is then copied & pasted to the SPSS. The results of the correlation analysis revealed that the study of dependent variables (Cybersecurity) is significantly positively correlated with the study of independent variables (Unauthorized Access, Security measures, Suspicious activities).

## 5.3 Suggestions and Recommendations

The study should have to increase their sample size although the sample size is small according to me. The companies are required to ensure to attain better systems for their firms. as we all know that cybercrime is getting verse nowadays and organizations need to make more proper solutions. The organization should have to make strong password that cannot easily access. The organization should have to install anti-virus to configure the meditation on a daily basis and ensure that your system and software were regularly provided to fix the security. Keep your E-mail security strong and make sure not to share sensitive data through E-mail. It is recommended to make the security of these systems stricter and tight. So may it can help to avoid the hacker’s attacks. The Cybersecurity systems and the software need to be upgraded to the level whereby they can meet all the security requirements of the users. All the technical issues related to such systems need to tackled by formulating effective plans as well as the strategies. It will definitely help the users to get more effective & efficient services.

## 5.4 Conclusion

In recent studies, it is concluded that the cybersecurity is needed more for the fields of IT, as cybercrime is getting threatening for IT fields. cyber-attacks are a big threat to infrastructure and systems of companies, individuals and government. The use of technology is increasing with the passage of time, and this increased use is also coming up with several issues and vulnerabilities in the information technology systems. Cybersecurity is one of the biggest concerns of recent times, and if considerable countermeasures will not be taken by stakeholders, then they may face severe consequences. The companies are required to ensure that they are following the policy guidelines provided by the government and experts to keep countermeasures in their cybersecurity systems.

The present research work and its findings tend to contribute significantly to the existing literature. both the theoretical and the practical implications. It will serve as the basis for future research work. Also, it will help the managers to use the findings and the discussions of the current research work for the strategy formulation.

The main research objectives of the current research work can better be achieved by following the suggestions and recommendations such as to examine the impact of unauthorized access on cybersecurity, to identify suspicious activities in the IT industry, to explain the significance of the security measures for cybersecurity. The ultimate effect will be the increased customer count and organizational profitability.

# References

Amoroso, E. (2012). *Cyber Attacks: Protecting National Infrastructure, STUDENT EDITION* (illustrated Edition ed.). Elsevier.

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence* *, 36*, 341-350.

Cook, A., Smith, R., & Janicke, L. M. (2016). Measuring the Risk of Cyber Attack in Industrial Control Systems. *Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research (ICS-CSR 2016)* , 23-25 .

cyberdefensemagazine. (2019). *Some counter measures of cyber attack*. Retrieved from https://www.cyberdefensemagazine.com/some-countermeasures-to-cyber-attacks/

Djekic, M. D. (2019). *Some Countermeasures to cyber attacks*. Retrieved from https://www.cyberdefensemagazine.com/some-countermeasures-to-cyber-attacks/

Gantz, S. D., & Philpott, D. R. (2012). *FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security.* Newnes.

Hare, F. B. (2009). Private Sector Contributions to National Cyber Security: A Preliminary Analysis. *Journal of Homeland Security and Emergency Management* *, 6* (1), 1547-7355.

Hasib, M. (2014). *Cybersecurity Leadership: Powering the Modern Organization.* Tomorrow's Strategy Today, LLC.

Hurley, R. F. (1998). Innovation, market orientation, andorganizational learning: an integration and empirical examination. *Journal of Marketing* *, 62* (3), 42-54.

Kazan, H. (2016). Contemporary Issues in Cybersecurity. *Journal of Cybersecurity Research (JCR)* *, 1* (1).

Knowles, W., Prince, D., Hutchison, D., & Jones, J. F. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection* *, 9*, 52-80.

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology* , 61–73.

Scully, T. (2014). The cyber security threat stops in the boardroom. *Journal of Business Continuity & Emergency Planning* *, 7* (2), 138-148.

Shinichiro, N. K. (2017). Countermeasures against Unknown Cyberattacks Using AI. *NEC Technical Journal* *, 12*.

Spry, A. P. (2011). Celebrity endorsement, brand credibility and brand equity. *European Journal of Marketing* *, 45* (6), 882-909.

Tikk, E. (2010). Global Cybersecurity–Thinking About the Niche for NATO. *SAIS Review of International Affairs* , 105-119.

# Appendix 1: Questionnaire

The purpose behind conducting this survey is to meet up the objectives of this research. It will take almost 10 minutes to fill out this questionnaire. It is assured that the information will be kept confidential and anonymous to others. For the completion of research work, your assistance is required. All of your efforts are highly appreciated.

Name (optional)

**Age:** a) 18-24 b) 25-34 years c) 35-44 years d) 45 or above

**Gender:** a) Male b) Female

**Educational Level**: a) Bachelor b) Masters c) M-Phil d) Others

**Employment status**: a) Private officials b) Government officials c) others

For the said questionnaire five-point likert scale is used. It ranges from 1 to 5. Here,

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Strongly Disagree**  **1** | **Disagree**  **2** | **Neutral**  **3** | **Agree**  **4** | **Strongly Agree**  **5** |

Kindly provide your response for each of the given statements:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Sr.#** | **Statements** | **SD**  **1** | | **D**  **2** | **N**  **3** | **A**  **4** | **SA**  **5** |
|  | **Unauthorized Access:** | | | | | | |
| **UA1** | Unauthorized access tends to increase the cyber security threats. |  | |  |  |  |  |
| **UA2** | The digital assets are manipulated through the unauthorized access. |  | |  |  |  |  |
|  | **Suspicious Activities:** |  | | | | | | |
| **SA1** | Unusual traffic on a site is perceived to be the suspicious activity. |  | |  |  |  |  |
| **SA2** | A process or task if takes more time than normal is considered a threat for the cyber security. |  | |  |  |  |  |
|  | **Security measures:** |  | |  |  |  |  |
| **SM1** | The use of effective security policies help to detect and prevent the threats. |  | |  |  |  |  |
| **SM2** | Security measures help to avoid the manipulation, deletion or modification of the data. |  | |  |  |  |  |
|  | **Cyber Security:** |  | | | | | |
| **CS1** | Cyber security helps in the identification of the thefts and the ransomware attacks. |  |  | |  |  |  |
| **CS2** | The data breaches can better be avoided through the cyber security. |  | |  |  |  |  |