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

# Chapter 1

**Khalifa Ahmed (17365)**

**Supervisor: DR. Mohammed Kamaruddeen**

**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.

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 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.

## 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.