A Study of Cyber Laws in the United Arab Emirates

Mohammed Imranuddin
mxi5627@rit.edu

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
Rochester Institute of Technology (Dubai Campus)

A Study of Cyber Laws in the United Arab Emirates

By

Mohammed Imranuddin

A Thesis Submitted

In Partial Fulfilment

Of the Requirements for the Degree of

Master of Science

In

Networking and Systems Administration

Approved by:

Prof. Dr. Charles Border

Prof. Dr. Ali Raza

Prof. Dr. Charalampos Manifavas

ROCHESTER INSTITUTE OF TECHNOLOGY

ROCHESTER, NEW YORK

MAY, 2017
Declaration

I declare that this thesis has not been submitted as an exercise for a degree at this or any other university and it is entirely my own work.

I agree to deposit this thesis in the University’s open access institutional repository or allow the library to do so on my behalf, subject to UAE copyright Legislation and University, RIT Dubai College Library conditions of use and acknowledgement.

Mohammed Imranuddin.
First I would like to thank Almighty Allah guiding me to study in the RIT Dubai and then my company Alpha55 without their co-operation and Help I won’t be able to complete my Postgraduate degree, Never the less how I can miss the Lecturers and university where I have educated RIT Dubai Campus , The idea of this Study of UAE Cyber Laws started as early when I have completed my studies in the year 2011 , But due to unforeseen circumstances it keeps on delaying the writing and submission , How I could forget to thank two Chair committee’s which I had formed earlier and current year.

All the mentioned Professors guided me and push to complete the work in time. But as I am fulltime employee heavily loaded with office projects couldn’t able to complete in the seven-year deadline period then I again with the efforts of Dr. Qu Yu and with the efforts and cooperation of Dr. Charles Border, Dr. Ali Raza, and Dr. Charalampos Mani favas. And not the last and lease Dr. Khalid Khawaja. Although, it is not possible to mention and enumerate all of them, I would like to take this opportunity to thank them all for their useful contribution. However, I may mention a few deserved special gratitude for their greatest efforts in making this work successful. In doing so, I show profound appreciation and good will for being helpful to me.

In addition, I am especially indebted to my supervisor Prof, Charles Border, for his Endeavour to provide prompt and valuable intellectual inspiration and guidance. His constructive criticisms and positive encouragement made this scholarly effort successful. Moreover, I send special gratitude to Course Coordinator Mrs. Amani AL Nassar and the entire academic staff for their time and sharing experience and knowledge.
ABSTRACT

The United Arab Emirates, as a developing country has been experiencing cybercrime even more rapidly in the recent years. The overall Internet penetration as well as the use of cyber-based systems in Critical Infrastructure is growing with a never seen pace in the country just as in the rest of the world. UAE has emerged to be on the forefront of many technological advances in the recent past. However, in the case of technological advances security advances must follow or the whole state becomes vulnerable. In the modern world there are several options for a state that wants to improve its cyber-security, co-operating with various international agencies.

This report will consist of an overview of the existing cyber laws in the United Arab Emirates “UAE”. This will include a brief explanation of each law. Sensational cases of cybercrimes along with the illustration of how the existence of cyber laws or their lack affected the prosecution of the individuals in question. On occasions of cases where prosecution was difficult, a preview is provided of how the scenario would have been had there been proper laws put in to deal with such cases. In continuation of that is a comparative study of these laws and the laws present in technologically well-developed nations such as the USA, England, and other nations. There is a focus particularly on England since it is one of the first countries to implement cyber laws in response to cybercrimes. Finally, suggestive steps have been included which can considerably improve the control of cybercrimes, especially in fast-developing regions like the UAE.

UAE has long been rather passive when it comes to international cooperation in security. The main driving force of the research is the constantly growing importance of cyber security all around the world, and especially in the UAE.

Keywords: Cyber Security, United Arab Emirates, Information Technology, Critical Infrastructure.
# Table of Contents

**Declaration** ........................................................................................................................................... ii

**ABSTRACT** ................................................................................................................................................ iv

**List of Figures** ........................................................................................................................................... ix

**List of Abbreviations** ................................................................................................................................. 10

**Chapter 1** .................................................................................................................................................. 11

1. **Introduction** ....................................................................................................................................... 11

1.1. **Background and Problem** ............................................................................................................. 13

1.2. **UAE History and Evaluation of Computers in the Country** ........................................................... 14

1.3. **Implication of Research** ............................................................................................................... 15

1.4. **Thesis Statement** .......................................................................................................................... 15

1.5. **Methodology of the Study** ........................................................................................................... 16

1.6. **Cyber Crime Threats in UAE** ....................................................................................................... 16

**CHAPTER 2** ............................................................................................................................................... 21

2. **Cyber Crime** ....................................................................................................................................... 21

2.1. **The Purpose and Definition of Cyber Security** ............................................................................. 22

2.2. **Cyber Security & Cyber Crimes** .................................................................................................. 24

2.3. **What are Cyber-Threats?** ............................................................................................................. 26

2.4. **Types of Cybercrime and Statistics** ............................................................................................... 30

2.4.1. **Data Breach** ............................................................................................................................. 30

2.4.2. **Hacking** .................................................................................................................................... 31

2.4.3. **Botnets** ..................................................................................................................................... 31

2.4.4. **Virus and Worms** ..................................................................................................................... 32

2.4.5. **Ransomware** ........................................................................................................................... 33

2.4.6. **Email Phishing** ........................................................................................................................ 34
5. Cases of Cyber Crime in UAE

5.1. UAE: A target of 5 per cent of global cyber attacks

5.2. Face book Ghost allegedly selling drugs arrested by Abu Dhabi Police

5.3. Hacker Holds UAE Bank to Ransom, demands 3m$ 

5.4. Australian Women Deported from UAE over Facebook post:

5.5. Dubai football coach accused of cyber-blackmailing boy

5.6. Hacker who leaked details of 1,300 people to Islamic State gets 20 years in jail

5.6. Hack of Saudi Arabia Exposes Middle East Cybersecurity Flaws

5.7. Cyber-attacks in Middle East rise up to 15% in Q1 2016

5.8. Know UAE’s law on cybercrime to stay on the right side of the law!

5.10. UAE to get tough on IP address forgery

CHAPTER 6

6. Conclusions and Recommendations:

6.1. Conclusion:

6.1.1. GCC Cybercrime Center like ECC (European Cybercrime Center)

6.1.2. Proposed Computer Crime Legislation Like USA

6.2. Recommendations:

6.3. The State of Cybersecurity in the UAE

6.4. Cyber-wellness profile of UAE

6.4.1. Cyber Security and legal measures.

6.4.2. Technical Measures and Certifications

6.4.3. Recommended Security measures for Organization sectors

6.4.4. Building the capacity, manpower development and certifications

6.4.5. Child Online Protection

6.5. Practical Approach
6.6. KEEPING CHILDREN SAFE ONLINE: TIPS FOR PARENTS .................................................. 84

Appendix 1: ................................................................................................................................................ 85

REFERENCES: ........................................................................................................................................... 108
**List of Figures**

*Figure 1*: The Impact of attacks in Middle East Companies ................................................................. 19

*Figure 2*: Number of Incidents in past 12 months ................................................................................. 20

*Figure 3*: Sources of Security incidents ................................................................................................ 21

*Figure 4*: Data Breach incident disclosures from 2005 to April 2015 ......................................................... 30

*Figure 5*: Botnets Statistics as of 30-06-2017 ....................................................................................... 32

*Figure 6*: Vulnerabilities in Last Month .................................................................................................. 33

*Figure 7*: Ransomware Families ........................................................................................................... 34

*Figure 8*: Phishing Activity Report ......................................................................................................... 35

*Figure 9*: Sex Crimes against children ................................................................................................ 35

*Figure 10*: Statistics of Cyber Bullying .................................................................................................. 36

*Figure 11*: International and Regional Instruments .................................................................................. 38

*Figure 12*: The UAE’s National Cyber Security Strategy ............................................................................ 44

*Figure 13*: The Privacy Score Board ....................................................................................................... 59

*Figure 14*: Number of virus-infected computing devices in the Middle East ................................................. 80

*Figure 15*: Occurrence of security breaches in past 12 months ................................................................. 80

*Figure 16*: Top Sources of Human Cyber Security Error ........................................................................... 81
List of Abbreviations

aeCERT: The Computer Emergency Response Team
C: C programming language file
CI: Critical Infrastructure
DPI: Deep Packet Inspection
GDP: Gross Domestic Product
GTM: Grounded Theory Method
GZ/SIT: Compressed file archive created by GZIP
IMF: International Monetary Fund
IT: Information Technology
NBS: National Bureau of Statistics of the United Arab Emirates
PL: PERL source code file
SH: UNIX shell script
TRA: Telecommunication Regulatory Authority
TXT: Text file
UAE: United Arab Emirates
ZIP: Compressed file archive created by PKZIP
Chapter 1

1. Introduction

The world is advancing with each second that passes by. Being on the brink of the second decade of the third millennium and with its birth one cannot help but perceive the truth around us—the truth that technology is slowly but surely beginning to dictate life. There is clear evidence of that nowadays. Observe closely, it will be noticed that people have reached a stage where they are handicapped without technology all around. It is obvious in human nature to take advantage of everything that revolves around oneself without paying attention to the repercussions. Talk about medication, transportation, communication or entertainment, there is nothing that people can do without equipment and logistics. In fact, mankind has become so addicted to the use of machinery for every activity that they not only over-think and over-work but persevere to give opportunities for technology to dictate lives.

The recent rise and growth of networking and cyber-technology is remarkable in that respect, to say the least. Although the inception of this ideology has been existent since a very long time its growth rate has evidently multiplied over the last decade. Every other day, people have new products and services, new devices, applications, and new ideas popping up in the networking cycle. With every passing day, networks are getting stronger with the inception of the same. Networking has become such a major tool that almost all the aspects of life have become dependent on this. Other technologies have now begun to act as peripherals revolving around the core, which is the network.

Although people complain of the dependency of man on machines, it is not necessarily a bad thing. Comparing the current state to the Stone Age one can easily say, ‘People got it good!’ However, we cannot expect to reap the benefits and enjoy the fruits of new technology without being ‘secure’. Yes, the most important issue that arrives as baggage with technology is ‘security’. Even if one has the world at his feet, but has not ensured enough security for what contributes to his joy, he will never be happy. It is ironic - once again people need ‘technology’ for the same. As the saying goes, only diamond can cut diamond, people need technology for their safe sailing and rescue from a
The remarkable pace of technological development has brought about issues that were once unimaginable. Although technological growth has enhanced security measures in perspective, it unfortunately has also granted attackers with additional tools to ‘break in’. Attacks using networks have become very diverse in nature and existing forms of security, no matter how hardened, are still not enough to keep out a ‘breach’. In such situations, individuals and organizations come into the firing zone and these attacks act as a gateway to their eventual destruction.

It is not just a theoretical treatise but a danger in prevalence. Why is it that nowadays people have continuously updated anti-virus software available? Why is it that they always require re-assured authentication before using the internet? Why do they need passwords? Why was CERT (Computer Emergency Response Team) formed? Fruit for thought, it is inferred that these have all occurred in the wake of numerous computer attacks that have caused severe consequences. There is a mighty battle going on between network security experts and attackers, but in the case of networking unfortunately the attackers are steps ahead and this trend may continue in the days to come. How can these attacks be categorised? Thieves, robbers, spies? Do they fall in the same category as that of physically committed crimes? The government of every country across the globe has responded by setting laws for prosecution of these ‘cyber criminals’. In addition, laws in this regard are being updated each and every day. However, cyber-criminals learn new, sophisticated and precise methods to attack, which affect us all including the government.

Are these laws global? Just to give an example, most network-related attacks originated in the developed regions like the United States and the United Kingdom. Are the laws followed there followed everywhere else? In United Arab Emirates (UAE) the network industry is multiplying at an exponential rate. Should the laws be the same in the UAE, though this region has not been as attacked as the sensitive areas of the US? These are some of the major points of discussion that this report will cover. Specific focus is on the UAE, as it is one of the fastest growing regions across the globe and the Middle East.
1.1. Background and Problem

UAE is one of the emerging economies of the world, and there is an urgent need to have cyber-security measures implemented in the country. This study will help us to understand the present cybercrime status in the United Arab Emirates, the cyber security measures taken to control them and the further improvements required in the cyber security in the international domain.

Even though the western world is contributing towards developing the cyber security in the UAE still UAE is fairly a young and fast growing economy which is presently in its way of upgrading its cybercrime laws to protect the interests of the people and also of the companies. This study will prove to be significant to understand the present cyber security measures that are being adopted by UAE and understanding the upgradation of the cyber security measures required in United Arab Emirates.

The objectives of my research include determining various patterns of Cyber-attacks in the United Arab Emirates. The research aims to unravel the different variables involved directly or indirectly with such crimes in the country. The identification of the effects and counter effects posed by each variable will lead to the finding of their individual roles in the cybercrime events.

The research shall prove fruitful in consolidating the study of patterns of attacks since one of the major questions tried to be answered is the relation between occurrence of cyber-attacks and holidays in the UAE (TRA. gov. ae., 2010).

Yet another objective of the present study is formulated in a way to study the outcome of cyber-attacks on political and Military arenas in the country.

Overall, this is a very comprehensive research work that shall prove to be a valuable source of learning about cyber-attacks and different measures implemented by the Government of UAE in order to control them in the country. This study will also be helpful to identify the different variables which can be used to anticipate future cyber-attacks in the country. So, the results of this research shall contribute towards the efforts in controlling the cybercrime activity in the United Arab Emirates.
1.2. UAE History and Evaluation of Computers in the Country

United Arab Emirates is also known as UAE. UAE is located in the gulf region of the world. Due to several tourist attractions in the country every year millions of tourists from all over the world visit UAE with their families and this gives a boom to the business activities and thereby necessitates development of the Information technology infrastructure in the country. In the recent years, there has been such tremendous development in the UAE that it is now included in the list of the most developed countries of the world.

The United Arab Emirates is situated strategically across the Straits of Hormuz from Iran. The country is among the richest countries of the Middle East having a population of approximately 5 million which includes 78 per cent immigrants. The immigrant population has increased with the progress taking place in the UAE.

Higher priorities for the ruling sheikhs is the source power of the state, growth of the economy, and the Islamic integrity. The biggest, richest, and politically most dominant of the 7 inherited sheikhdoms or emirates which include the UAE is Abu Dhabi. Dubai is the 2nd major and most densely populated emirate. Dubai has developed into an important city-state and has become a globalized economic hub.

The economy of the UAE has developed at a rapid rate in the recent years and one of the consequences has been an increase on internet penetration and increasing dependence of critical infrastructure on advanced electronic systems which could be vulnerable to cyber-attacks. Contrary to popular belief, the economy of the UAE is not anymore overwhelmingly oil-based.

With the passage of time use of information and technology has also increased in the country than previously. It became the responsibility of the UAE Government to safeguard the interests of the foreign investors. One of the major threats to the foreign investors was the large numbers of cyber-attacks launched by the hackers on the systems and servers of the companies
and it cost loss of millions of dollars to the foreign companies as they always lost something important as a result of these cyber-attacks (Khaleejtimes.com)\(^1\).

### 1.3. Implication of Research

“The cyber war has already left the pages of science fiction books and has become a reality,” said August Wilhelm Schemer, President of Backcomb\(^2\).

The truth circumnavigating is exposed by taking into account a penetrating statistical analysis of sample surveys conducted on heterogeneous usages of the internet and innumerable methods of attacks inflicted on the internet comprising flint-like hard boundaries of secured computer systems. These have come to surface the world over. The intelligence and the skills crafted by protective superlative engineering brigades have been smashed. The security measures calibrated and tools drafted and designed for ensuring of fool proof security measures, the expertise dispensed and the confidence reposed for the safe sailing of vital information exchange have been reversed and have become questionable.

Some malicious tools of attack used for sensational cybercrimes and the tricks used by the attackers have been presented as specimens for the awareness of the common users of the internet and their dependency on this ever-growing dangerous medium of common use.

### 1.4. Thesis Statement

Information technology is encompassing all lifestyles all over the world bringing about a transition from a paper to a paperless world. However, there is always a need to regulate the cyber space obviously. The initiative is to hunt for new cyber shielding mechanisms for the Middle Eastern countries specific

---


to the UAE, the region of my bread and butter provider and the responsibilities mandatory for it. The existing cyber laws in these places are undrafted or poorly drafted.

When I started to pen down my Thesis on this Subject in the Year 2010, the Federal Government of UAE felt necessary and redrafted a New Legislation on 27th August, 2012 to plug the gaps in the Cyber Laws.

But the lack of essence in the current modified laws and control methods demanded to maintain the pace to prevent the dangerous effects of cybercrimes. This can be achieved by comparing and contrasting the cyber laws of the developed regions like UK, USA etc. with UAE.

1.5. Methodology of the Study

- The present study is an exploratory one and hence a multipronged methodology is used to complete the study. This is included analytical and descriptive method as far as historical development and analysis of legal framework is concerned.
- The analysis of impact of cybercrimes and legal mechanism for compacting it in UAE based on data that gathered through published annual reports, Articles published in books, journals and newspaper etc. Electronic articles, books and materials posted on internet websites are consulted.
- Thus both primary and secondary sources are made use of in the completion of study. The selections of UAE - A Federal Decree-Law no. (5) of 2012 and selections of other related legislation and laws in UAE are already reviewed.

1.6. Cyber Crime Threats in UAE

The Computer Emergency Readiness Team (aeCERT)\(^3\) of Telecommunications Regulatory Authority (TRA) successfully foiled 1,054 cyber-attacks in 2016.

Mohammed Al Zarooni has stated that the cyber-attacks are mainly targeted upon the government websites. The attack involves fraud, deception, hacking, denial of service and other threats like document theft as mentioned by the director of TRA’s policy department to Emirates News.

He noted that private companies were the most vulnerable to such attacks registering 510 attacks targeted at them followed by 463 against government entities.

aeCERT conducts several workshops under the aegis of its Advisory, Education and Awareness program services. These workshops emphasise its role in spreading information security awareness across the corporate levels and the role of the employees in protecting their organisation. The workshops under the information security awareness campaign cover a wide range of topics, including social media, social engineering, email security and computer protection.

The government sector experienced phishing, fraud, web defacement, malicious code, unauthorised access, scans, theft of credentials and others while the private sector experienced phishing, fraud, malicious code, inappropriate content, and denial of service.

As a Cyber security, Coordination centre, aeCERT aims to improve the UAE’s overall cyber security conditions by co-ordinating the exchange of cyber information and copes with the cyber risks faced by the UAE.

aeCERT also enlightens the UAE government and its educational sectors regarding information security. It collaborates with different sectors of the government to design policies and methodologies to counter cyber threats.

Organization should monitor the employees’ internet browsing activity which will reflect on the company’s growth and productivity. If the organization fails to monitor the user activity of the employees, and then they would not know where they are investing their time whether in business or for personal activity.

Many will visit online shopping, peer-to-peer, social networking sites and even online dating or adult sites. All of these activities waste company’s time and expose the company’s network to Internet-based threats.

For instance, adult sites are notorious for hosting malware. These sites are easy and inexpensive to launch, contain content that attracts numerous visitors and are taboo enough to elicit silence from visitors who suspect they may have infected their system by visiting the sites. These attributes make these sites the ideal medium for spreading malware.

Online shopping sites are equally as notable for hosting Internet-based threats as their adult site counterparts. Spyware runs rampant throughout many of these sites. Additionally, they frequently link to third-party sites for many of their items; completely transparent to the user. Therefore, even if the main site is trustworthy the user rarely knows when he or she is on the "clean" site, or on one of an unknown third party.

(Maddison, 2016)\textsuperscript{5}

Middle East Companies suffered huge losses from cyber incidents compare to other regions of the World. They lost 56% more than $500,000 in comparison other world regions which lost 33% only. On a Minimum, there was a loss of 3 working days for the companies in this region which have been attacked. Below are the Stats from a report.

\textsuperscript{5} http://www.pwc.com/m1/en/publications/middle-east-information-security-survey-2016.html
Figure 1: The Impact of attacks in Middle East Companies

http://www.pwc.com/me/cybersecurity
In the ME Region, companies experienced as many as 5000 attacks in the last year, which is 9% more than the Global Cyber incidents rate. Attacks mainly originate from source vehicles such as Phishing Emails and visiting of Malware effected websites by the Company Employees. Most of the attacks remain dormant until the outside or third party or clients report suspicious messages or request of funds.

Much of this harmful usage and risky behaviour can be attributed to the nonchalant attitude many employees have towards their employers.

Many employees proceed with the irresponsible employment of Internet with the belief that since it is not their own computer that they are using, security doesn’t hold importance. Similarly, many users assume that security is the responsibility of IT and so risky behaviour will not have any negative impact; both of which are incorrect beliefs.

Even if the company employees are using the internet in appropriate manner the root cause and primary zone of a threat is the internet which includes cyber-attacks like ransomware, Trojan, backdoor etc.

The major interaction of the user to be infected by just visiting any website that leads to downloading in the background during a user browsing activity without any knowledge and interaction is known as drive by download.

These types of threats are mostly discovered from legitimate sites which are hacked by the intruders to create vulnerability. Around 79% of the legitimate sites get infected by the threats and if precautions and security measures are not taken into consideration and an appropriate patch not applied then the end user will the victim.

Remaining 21% threats occur by the user random activity by visiting the rouge websites which replace as legitimate sites and are also designed that the users are diverted and forced into visiting illegitimate

---

7 [http://www.pwc.com/me/cybersecurity](http://www.pwc.com/me/cybersecurity)
sites. Hacker also take the advantage of digital marketing to advertise their sites to increase the number of visitors and spread vulnerability.

**Figure 3: Sources of Security incidents**

### CHAPTER 2

2. Cyber Crime

A crime committed or facilitated via the Internet is a Cybercrime. It is any criminal activity involving computers and networks. Cybercrime fraud can range from illegitimate emails to theft of government information or corporate sensitive data through remote devices around the world. Cyber-crime is not only hacking into others system or stealing millions from bank transfer but also downloading pirated or other illegal music files.

---

8 [http://www.pwc.com/me/cybersecurity](http://www.pwc.com/me/cybersecurity)
Cybercrime is also defined as non-money offenses like developing and spreading virus on other systems and posting confidential information on social media.

2.1. The Purpose and Definition of Cyber Security

The definition of cybercrime given by Babu & Parishat in 2004⁹; An illegal act where computer systems are used against a person, his property or the state to commit a cybercrime (Wiesen, 2012)¹⁰. Sukhai reported in 2004 that 60% of cyber-attacks are not even detected and out of the ones which are; only a paltry 15% are brought to the attention of the governing authorities (Townson, 2006).

There is no doubt that cybercrime is one of the most rapidly accelerating kinds of crime today. An increasing number of felons are making good use of the easiness, quickness and inconspicuousness offered by advanced technologies of the 21st century to indulge in a wide range of unlawful activities most of which consist of attacks on systems and data, stealing identities, the circulation of pictures pertaining to child sexual abuse, fraud involving online auctions, misusing financial services available on the internet, spreading viruses, botnets and numerous scams operated through electronic mail, of which phishing is a prime example (Julia, 2012)¹¹. Every country in the world needs to constantly modify its local offline controls in order to be well equipped to combat cybercrimes as the internet does not adhere to geographical boundaries and allows wrongdoers to carry out unlawful activities worldwide (Townson, 2006). One of the most potent threats to national and international security lies in the use of the internet by extremists specially to spread fundamentalism and to attract more people. (Lunjevich, 2010)¹²

The menace of terrorism has also forced authorities to focus on possible loopholes as far as the security of the infrastructure of information technology is concerned especially in strategic

---

⁹ http://www.crime-research.org/analytics/702/

¹⁰ http://www.zawya.com/Story.cfm/sidZAWYA20100118085552/UAEToEstablishSpecialistCybercrimeCourts/

¹¹ https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/reports.pdf

and/or high value assets such as power plants, electrical grids and databases; not to mention the software’s and systems of governments and multinational companies (Khaleejtimes.com, 2006)\(^\text{13}\).

According to Nissenbaum 2005, cyber security is a technical term for the securing of computers but it can have severe societal effects as well (Euromonitor International, 2009)\(^\text{14}\).

In addition, it includes problems related to electronic surveillance and camera systems, property and infrastructural protection, hacking by terrorists against other countries and computer networks used for communication at large (Latham 2003:1)\(^\text{15}\) (Higher Colleges of Technology, 2009)\(^\text{16}\). The term cyber security came into existence after authorities realized that the cyber infrastructure had to be protected (Aitoro 2010)\(^\text{17}\). Numerous terms regarding cyber security have come into existence. A deliberate cyber-attack by a person residing in one State to another with the intention to cause real-world harm is called Cyber warfare (Lunjevich, 2010). Moreover, Cyber-espionage is a similar the illegal attack where sensitive digital information is stolen from a state or a computer system (Van, 2008)\(^\text{18}\). Lastly, any sort of cyber theft committed online and where a computer or network has been used to carry out that crime is called Cybercrime (Aitoro 2010)\(^\text{19}\) (Lieberman, 2011)\(^\text{20}\).

The second part of Obama's speech reflects the facts that not only are governments of the modern day worried about matters pertaining to cyber security, they are also well aware of the obstacles they face.

\(^{13}\) http://www.zawya.com/Story.cfm/sidZAWYA20100118085552/UAEToEstablishSpecialistCybercrimeCourts/


\(^{17}\) https://www.bizjournals.com/washington/news/2012/08/02/epa-security-breach-exposes-personal.html


\(^{19}\) https://www.bizjournals.com/washington/news/2012/08/02/epa-security-breach-exposes-personal.html

"Cyberspace exists and so do the risks along with it. The irony lies with the limited information we have, as the system which encourages and gives us the power to create and develop also encourages others who intend to commit crimes in the cyber world" (Lieberman, 2011)\textsuperscript{21}.

According to Baggili and Rogers 2009, research on cybercrime has traditionally tried to come up with technological tools to combat it (Euromonitor International, 2009)\textsuperscript{22}.

### 2.2. Cyber Security & Cyber Crimes

With the advancement in the Information technology, the way of executing crimes has also changed nowadays. Gone are the days when robbers entered into the house and took away the valuables of its residents (Soma, 2011)\textsuperscript{23}. In these modern days, there are new ways of stealing and robbing others information and assets. This stealing is proving to be more dangerous than traditional robberies as the person might remain unaware of it for quite some period. (Jason, 2011)\textsuperscript{24}

Issues like Cyber security and Cybercrime are those issues that can barely be separated in a unified environment. The resolution of UN (2010) on cyber security 35 discourses Cybercrime as a major encounter (Soma, 2011)\textsuperscript{25}. In the enduring development of information technology Cyber security and internet services play a significant role (Penney, 2007)\textsuperscript{26}. Augmentation of Cyber security and protection of perilous information substructures are obligatory in nation’s security and as well for economic wellbeing. For the development of new services and state policies, it has become essential to take steps in order to make internet safer and provide the

\textsuperscript{23} [https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false](https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)
\textsuperscript{24} [https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false](https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)
\textsuperscript{25} [https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false](https://books.google.ae/books?id=2jp08gAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)
\textsuperscript{26} [https://books.google.ae/books?id=gQEAAAAAMBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false](https://books.google.ae/books?id=gQEAAAAAMBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false)
security to the internet users. Dissuading of Cybercrime is a vital element not only for national Cyber security but as well for the acute structure protection stratagem (Steiner, 2009)\textsuperscript{27}. This comprises the espousal of appropriate legislature in particular in contradiction of the misappropriation of ICTs for criminal or other tenacities which envisioned distressing the national precarious infrastructures integrity. This is a communal responsibility at the national level which requires synchronized action correlated to report, preparation, anticipation and retrieval from incidents on the fragment of state authorities, private sector and citizens (Urbas, 2008)\textsuperscript{28}. This calls for coordination and cooperation with pertinent partners at the international and provincial level.

Thus, the origination and implementation of a national agenda and tactics for cyber security necessitates an inclusive approach (Aecert.ae. 2006). The examples of cyber security policies can help in reducing the risk of cybercrime as through the expansion of technical security systems or by educating the users to avert them from becoming the victims of cybercrime. In the fight against cybercrime the development and support of cyber security strategies are vibrant elements (Blackwell, 2009)\textsuperscript{29}.

Crime exists in society since thousands of years but with the passage of time, its shapes kept on changing. Traditionally, stealing the money was included in the crime but nowadays stealing the information also comes under the definition of crime (Blackwell, 2011)\textsuperscript{30}. The most obvious reason behind this is that the world is growing so fast that sometimes information available with the person is far more important than the money available with him. A person might be able to bear the loss of the money, but he might not be able to bear the loss of his information (Sean, 2007)\textsuperscript{31}.

\begin{thebibliography}{9}
\bibitem{27} http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7249&context=jclc
\bibitem{28} https://www.aph.gov.au/binaries/house/committee/coms/cybercrime/subs/sub41.pdf
\bibitem{29} http://www.sei.cmu.edu/reports/12tr007.pdf
\bibitem{30} http://onlinelibrary.wiley.com/book/10.1002/9781444395433
\bibitem{31} http://www3.weforum.org/docs/GITR/2013/GITR_Chapter1.5_2013.pdf
\end{thebibliography}
Nowadays, everything is based on the information available with the person. Even the organizations that are doing their businesses in a highly competitive market make their decisions on the basis of the information available with them (Biever, 2005)\(^{32}\). Organizations are spending millions of dollars in making their IT infrastructure and servers strong and inaccessible. Information stored in the computer systems of the company are very important for them as they can use the information in the future in order to gain a competitive advantage over their competitors and after all this hectic efforts, if the information available with the company is stolen then it will be a far bigger loss to the company than losing its money because lot of effort was put in by the company in gaining its information. The decision making process of the company will also be affected due to this loss of information. Hence, sometimes loss of information becomes the bigger loss than the loss of money (Bronitt, 2008)\(^{33}\).

### 2.3. What are Cyber-Threats?

Any given threat to a computer system, whether it is hardware related or software related, is termed as "cyber security risk." These threats are inevitable in the digital world and are deemed to exist just because the system exists (Wiesen, 2012). They cannot be entirely avoided or fixed that easily regardless of the technical advancements in cyberspace. (Julia, 2012)\(^{34}\). The important part of cyber security is to pay close attention to the security of the computer system because without suitable and comprehensive security measures, the threat is set even if the computer system has not been a victim to one (Townson, 2006)\(^{35}\). No disastrous incidents have been reported till date hence taking complete cyber securitization measures is the number one priority for everyone. There are no limitations to cyber-attacks; therefore, the security of computer systems is highly important on a regular basis especially because these systems may contain vital information

---


\(^{34}\) [http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers](http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers)

\(^{35}\) Townson P 2006 Call for legal steps to fight cybercrimes [www.gulf-times.com](http://www.gulf-times.com) [accessed on 3 March 2009]
Another important factor is that the cyber security is an integral part of expert Security Studies whether they are individual, collective, economic, political, public or private. If cyber security is not dealt with significantly private security, network security, state security, national security and every related body are all considered to be at the risk of cybercrime (Van, 2008). Cybercrimes can be defined thus as: “an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and phrasing, and stealing personal information like bank account details. A crime can be distinguished as a cybercrime if the central players are computer(s) and internet.”

Cybercrime doesn’t have a rigid definition and is multi-layered. The organization victimized are ignorant of their vulnerability. Hence essential preventive measures aren’t being able to be implemented.

Cybercrime ranks as one of the top four economic crimes and has become the rising type of fraud for the following reasons:

- Due to social media and reported news of recent cybercrime threats brings awareness for the organization to start protecting and implementing extra security for this type of fraud.
- Cybercriminal sitting somewhere in the world and causes vulnerability to the organization using by the internet.
- It’s easier these days because of the advanced technology.

Cybercrime presents different types of risk to the organization. For instance, cybercrime is different from physically stealing money from a bank. In cybercrime, the fraud is initiated from the internet and has remote connections with the bank system. The offenders transfer the money to their account or steal the sensitive data of the bank. In this case the fraudster is

36 http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers
37 http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf
not present physically in the bank location so it’s very difficult to get hold on these cyber criminals.

• It is very difficult to find or to identify the perpetrator and it's not easy to find exactly from where they were based when the crime was committed.
• It becomes more difficult when the hackers are in different parts of the country, which makes it more difficult to arrest them according to the traditional prosecution law. There are different laws in different locations. It’s not mature enough to catch the cyber criminals. With the rise of the technology there’s growth in the cybercrime as well so the organization need to implement more secure infrastructure to prevent their information and need to be updated with corporate security policies.

These five types of cyber-attacks are distinct with overlapping objectives of their own:

1. **Economic crime**—This type of attacker is well organized and highly funded to use hacking system and technology tools to create vulnerability and commit fraud.

2. **Espionage**—As of today’s, world of communication most valuable intellectual property is the electronic communication and data which also includes development and research property. This type of attack does not even come into knowledge until it appears in the market or some other company introduce declaring themselves as actual developers of the product.

3. **Activism** — some attacks are caused for idealistic cause; WikiLeaks were the recent supporters of this cause.

4. **Terrorism** — this type attack is mostly targeted on the private or state sector, also includes national infrastructure like financial system, power and telecom sectors.

5. **Warfare**—this attack is targeted on the organizations involved in private and state sectors.

The perception of cybercrime is changing earlier it was perceived as an external threat. Organisations are now understanding the risk as internal implicating the IT department because IT personnel are quite adopt at using the system and the skills required to ‘misuse’ it. IT personnel might have 'super
user’ access, which gives them extra administrative rights to access systems and the ability to delete audit trails, making it harder to detect their wrongdoing.

Along with financial cost, it also includes other commercial cost and consequences such as business disruption, insiders wrong practise, lack of knowledge and training to the employees, reputation of the company. Some of the instances of cybercrimes are mentioned below in detail. A disgruntled employee gets hold of confidential information they should not have, like payroll, bonuses and other rewards, and uses this information to their advantage.

- A disgruntled employee gets hold of confidential information they should not have, like payroll, bonuses and other rewards, and uses this information to their advantage.
- An employee gets hold of information from the accounts payable department, sets up dummy supplier information and extracts money from the company in this way.
- An employee shares some sensitive information with their 'friends' or connections on social media and it leaks out into the public domain.
- An employee accesses a colleague's email account and sends malicious emails from it, bullying other members of staff ('cyber-bullying'). Although this might not result in direct financial losses, it could certainly affect the organisation’s reputation, disrupt operations, or result in business continuity.
- Whether these are definable Cybercrimes or financial crimes where computer and internet act as medium? Definition and constitution of cybercrimes is not important. Aforementioned examples exemplify that threat comes from all quarters of an organization.
- We asked organisations if they thought the risk of external cybercrime mainly came from inside their own country or from abroad. Cybercrime is really a global threat which can attack from anywhere and jurisdiction cannot restrict completely only can have some boundaries to the crimes.
- Mostly every country has a black market where they can find the stolen consumers goods in very low price similarly in cybercrime world there's a dark market where stolen credit cards information is sold in a very low amount of cents. Attackers hacked
into credit cards organization the reason they were not supporting the companies like Wiki leaks.

2.4. Types of Cybercrime and Statistics.

2.4.1. Data Breach

A data breach is an incident wherein information is stolen or taken from a system without the knowledge or authorization of the system’s owner. A small company or a large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information, such as credit card numbers, customer data, trade secrets or matters of national security.


![Data Breach incident disclosures from 2005 to April 2015](https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf)

*Figure 4: Data Breach incident disclosures from 2005 to April 2015*³⁸

2.4.2. Hacking

Computer hacking is encroaching upon and modifying a hardware or software which is not originally conceived by the creator. Hackers are the individuals who indulge in such programming skills and have expertise in handling the entire setup.

2.4.3. Botnets

A 'bot' is a form of malware which hackers employ to control an infected system. Networks connected and co-operated under a single hacker is termed as a ‘botnet’.
2.4.4. Virus and Worms

Virus is a malware that spreads by inserting its copy to become an integral part of another program. It transports from one system to another leaving behind infection. Worms cause a similar damage. They replicate functional copies of themselves and infect the system.

Figure 5: Botnets Statistics as of 30-06-2017

2.4.5. Ransomware

Ransomware is the most widespread threat ranging from domestic to social terrains. It targets domestic users, business, and government networks which leads to temporary or permanent access of sensitive information. They can also be source of disruption of services, financial loss involved in restoration of files and tarnishing of an organizations reputation.

---

40 [https://securelist.com/statistics/](https://securelist.com/statistics/)
2.4.6. Email Phishing

Phishing is a criminal offence using social engineering and technical subterfuge to steal consumer’s personal identity details and financial credential. Social engineering schemes are spoofed emails deceiving recipients as being from data like username and passwords.

2.4.7. Child Pornography

Child pornography refers to any content that depicts sexually explicit activities involving a child. Visual depictions include photographs, videos, digital or computer generated images indistinguishable from an actual minor. These images and videos that involve the documentation of an actual crime scene are then circulated for personal consumption. More recently, live-streaming sexual abuse has begun to surface.

Figure 9: Sex Crimes against children

2.4.8. Cyber Bullying

Bullying done using electronic technology via devices like cellphones, computers, tablets, as well with communications tools like social media sites and websites is called as cyberbullying.


2.5. Laws & structures

Legal actions play an important role in the deterrence and fighting against cybercrime. These are needed in every area that includes criminalization, procedural controls, authority, global collaboration, and internet service source responsibility as well as liability. At the state level, both present and latest (or designed), cybercrime legislation most frequently concerns criminalization that mainly emphasizes on setting up offences for important acts of cybercrime (Ghosh, 2010)\textsuperscript{45}. States gradually identify but there is a need for laws in other areas. Compared to existing legislation, latest cybercrime legislation more often deals with investigative measures, jurisdiction, electronic proof & global support. Internationally, below half of responding states recognize their criminal and procedural legislation frameworks being enough, even though this masks huge regional disparities (Clark, 2011)\textsuperscript{46}. Like over 2/3 of states in European region report adequate

\textsuperscript{44} https://www.reportlinker.com/insight/americas-youth-cyberbully-life-skill.html

\textsuperscript{45} https://books.google.ae/books?hl=en&lr=&id=afJqtsfQhSkC&oi=fnd&pg=PR3&dq=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&ots=CsVW70Ptt7W&sig=cT5pHo2OXrmA7DVzOv1NTQgwsDI&redir_esc=y#v=onepage&q=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&f=false

\textsuperscript{46} http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7456&context=jclc
laws, and this image is reversed in America, Africa, Asia and Oceania, where over 2/3 of states consider legislation as just partially adequate, or not adequate in any way. Only one half of the states that reported that legislation is not sufficient, also showed newest or planned legislation, hence focusing on the vital need for legislative reinforcing throughout these regions.

The past few years have seen important developments in the proliferation of global as well as regional instruments focused on countering cybercrime (Ghosh, 2010)\textsuperscript{47}. These include binding & non-binding instruments. 5 clusters may be recognized, containing instruments built up in the context of, or encouraged by: (a) the UN (b) the League of Arab States, (c) intergovernmental African organizations, (d) the Commonwealth of Independent States or the Shanghai Cooperation Organization, and (e) the Council of Europe or the European Union (Brown, 2010)\textsuperscript{48}. An important sum of cross-fertilization is present between each and every instrument that include, particularly, ideas and approaches built up in the Council of Europe Convention on Cybercrime. Investigation of the articles of 19 bilateral instruments related to cybercrime demonstrates general major provisions, yet, also significant deviation in substantial areas dealt with (Jo-Ann M, 2011)\textsuperscript{49}.

At global level, eighty-two states have signed and approved the binding cybercrime instrument.

\textsuperscript{47}https://books.google.ae/books?hl=en&lr=&id=aFJqtsfOhSkC&oi=fnd&pg=PR3&dq=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&ots=CsW70Pt7W&sig=cT5pHo2OXRmA7DVzOv1NTQgwsDI&redir_esc=y#v=onepage&q=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&f=false

\textsuperscript{48} Brown, I., 2010. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology,

\textsuperscript{49} http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1206&context=chtlj
Also to formal association & implementation, bilateral cybercrime instruments have impacted state legislation indirectly, by being used as a model by non-States parties, or by the result of laws of States parties on other states (Laura, 2007). Multilateral cybercrime instrument’s memberships correspond with the perspective of better adequacy of state criminal as well as procedural legislation that show that recent multilateral provisions in such areas are usually supposed efficient. For over forty states which gave information, the Council of Europe Convention on Cybercrime is the most utilized multilateral instrument for the advancement of cybercrime laws (Reid, 2008). Overall, multilateral instruments from other ‘clusters’ were used in about half as many states.


In general, 1/3 of responding states report that their law is extremely, or much extremely, coordinated with states seen as significant for the idea of global collaboration. This differs at regional level, but, high levels of coordination have been reported in the US & European area. This can be because of the use, in certain regions, of multilateral instruments that are intrinsically planned for playing the part in coordination (Dana, 2009). Fragmentation at a global level & diversity of state legislation, in terms of cybercrime acts criminalized, instruments of harmonization and jurisdictional bases can associate with the presence of multiple cybercrime instruments with different thematic as well as geographic range. Both instruments, as well as regions, currently show deviations derived from fundamental legislation and legal differences that include differing views of rights and confidentiality.

CHAPTER 3

3. Evolution of Cyber Laws in UAE:

The UAE has the most detailed and comprehensive cyber-crime law in the Arabian Gulf and wider Middle East. The UAE-Law No. 5 of 2012 concerns with the Combating of Information Technology Crimes. Better known as the Cyber Crimes Law 2012, this law replaced the earlier Cyber Crimes Law 2006.

The Cyber Crimes Law 2012 provides for a range of new offences, including offences intended to address the UAE’s obligations pursuant to international treaties. Additionally, in 2006 cyber-criminal law declares high penalties to those who commit the offense.

The range of crimes committed by using the internet is codified by the first time along with sentences for a fraudster found guilty. Punishable crimes are declared under the new law, for promoting or publishing pornographic material or indecent act and gambling activities.

To protect the possible vulnerability these types of laws are implemented to manage to reduce the risk of cybercrime which can easily take place in this advanced world of technology. Publishing of others information and photos on internet and offences of violating others privacy by eavesdropping and publishing the information using the social media all comes under the cybercrime offences for which law is created and its sentence and punishment is declared.

When talking about the positive points of the cybercrime law of the United Arab Emirates, the local government specifically the Telecommunications Regulatory Authority (TRA) realizes the need for such law and how it is important to stay up-to-date in the world of Cyber Crime. Since the legal framework of the law covers a good number of different crimes categories such as Human Trafficking, Data Forgery of prohibitive data, and unauthorized use and interception of computer services. It includes penalties for imprisonment for a term which may extend to ten years and a fine up to 200,000 AED. The Act also stresses the respect for religion and the Islamic identity of the state and respect for other religions as a total of 202 different nationalities exist in the UAE
labour market according to the Under- Secretary of the Ministry of Labor (khaleejtimes.com 2006). Dwyer (2010) supports the idea that with the increase in cyber-attacks and the motives behind them, governments should be more encouraged to avoid letting the crimes divert their attention from the Cyber Crimes. Moreover, the local government has created a Computer Emergency Response Team (aeCERT) with a dictated website to provide awareness, information, advice, and receive problem alerts from users, as well as has created Cyber Crime Courts to deal with the jump in the computer-related crimes (UAEinteract.com, 2007).

Carrying out electronic businesses in a well-defined legal structure will definitely contribute positively to the nation's economy and even create more opportunities to the businesses themselves (Robert et al.; 2010).

UAE government has legalized entities to process the cyber security legal Frame Works.

The entities are,

3.1. UAE Telecommunications Regulatory Authority (TRA)

They send government authorities policies to follow, and security rating, they are one step above the ISP (Etisalat/Du)

Cabinet Resolution No. (42/23) of 2008 Session No. (3), Regarding the Abolition of the Supreme Committee for the Supervision of the Telecommunication Sector and delegating its functions to the Board of Directors of the Telecommunications Regulatory Authority (TRA).

http://www.tra.gov.ae

---


3.2. UAE aeCERT

The UAE CERT (Computer Emergency Response Teams)\textsuperscript{58} was established under the supervision of TRA of UAE to help the Government Sectors and Educational sectors for cyber security information sharing and improving the overall Cyber Security condition in the country. They are first institution to report the Cyber Incidents and they follow proactive approach to protect the systems, they collaborate with different government and law enforcement agencies to design policies and methodologies to counter the Cyber Threats.

aeCERT collaborates and shares data with other countries CERTS around the globe, which provides opportunities for researchers to improve the posture of Information Security

3.3. Standard Information Security Policy (SISP)\textsuperscript{59}

It is defined as a set of standards, guidelines and procedures that specify in more or less detail the expectations in regard to the appropriate use of information and/or information assets and network infrastructure. SISP is a policy approved and supported by the senior management. The intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to the organization’s established culture of openness, trust and integrity, however, it is the Information Security Department’s commitment to protect the organization and its users from illegal or damaging actions by individuals, either intentionally or unintentionally. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, applications, data storage media, network accounts providing electronic mail, Internet browsing, and FTP, are the property of the organization. These systems are to be used for business purposes in serving the interests of the organization, and of our users in the course of their normal business operations. Effective security is a team effort involving the participation and support of every employee in the organization and affiliate who deals with information and/or information systems. It is the responsibility of every user using the

\textsuperscript{58} \url{https://www.tra.gov.ae/aecert/en/home.aspx}

\textsuperscript{59} \textit{European, Mediterranean & Middle Eastern Conference on Information Systems 2010 (EMCIS2010)}
April 12-13 2010, Abu Dhabi, UAE
\url{https://www.academia.edu/RegisterToDownload#ChooseAccountChecklists}
organization’s resources to know these standards, guidelines and procedures and conduct their activities in compliance to this policy. The SISP contains and is not limited to the following sub-policies to be adhered by all users:

• Anti-Virus Policy
• Password Management Policy
• E-mail Usage Policy
• Information Handling and Classification Policy
• Encryption Policy
• Desktop & Laptop Usage Policy
• Software Compliance Policy
• Backup and Restoration Policy
• Remote Access Policy
• Wireless Communication Policy
• Mobile Phone Policy
• Disposable of Media Policy
• Visitor Premises Policy
• Physical Access for Data Centre Policy
• Patch Management Policy
• Physical Access for Operation Centre Policy
• Change Management Policy
• User Access Management Policy
• Information Security and Business Continuity Incident Management Policy
• Acceptable Use of IT Equipment Policy
• Clear Desk and Clear Screen Policy
• Data Centre Document Management Policy
• Log Management Policy
• Physical Access for organization office Policy

Adapting these policies will assist in complying with Information Security Management standard (ISO 27001:2005) and Business Continuity (BS 25999-2:2007)
3.4. NESA (National Electronic Security Authority)\textsuperscript{60}

The UAE's National Electronic Security Authority (NESA), the federal body set up to oversee the country's cyberspace, on June 25\textsuperscript{th}, 2014 announced the publication of a range of strategies, policies and standards to "align and direct national cyber-security efforts". His Highness Sheikh Khalifa bin Zayed Al Nahyan, President of the UAE and Ruler of Abu Dhabi, established NESA through Decree No. 3 of 2012. NESA is a government body tasked with protecting the UAE’s critical information infrastructure and improving national cyber security to achieve this, NESA have produced a set of standards and guidance for government entities in critical sectors. Based on ISO/IEC 27001:2013 and ISO/IEC 27002:2013 Compliance with these standards is mandatory.

Figure 12: The UAE’s National Cyber Security Strategy

http://www.innovationandtech.ae/cybersecurity-mobility-age/

3.5. DUBAI ISR  Information Security Regulation (ISR) \(^{61}\) standards

ISR standards from Dubai Smart Government mandates government entities in Dubai to implement requirements and controls stated in the standard to ensure appropriate level of confidentiality, integrity, and availability of information assets.

By complying with ISR standard, organizations can ensure the following:
- Protection of information assets
- Compliance with local regulations
- Effective mitigation of information security risks
- Raising information security awareness
- Mandatory for Dubai governments

Dubai Smart Government has issued an implementation plan that was planned to end in December 2015.

3.6. Abu Dhabi (ADSIC\(^{62}\))


The Control Standards contained within this document provide an expression of the Information Security expectations that the government has upon Entities and business partners handling classified government data. The control standards manifest in twelve fields of information security which are mutual and interrelated.

The second version aims to enhance information security and its consistence across governmental organizations of Abu Dhabi. This programed has already started and is planned to go into 2016 Part of this program is regular feedback from entities to ADSIC to measure their progress.

ISO/IEC 27001:2013

Information Security Management System


CHAPTER 4

4. Comparison and Contrast:

UAE has established a special act on computer-related crimes, which made it comparatively easier to include many illegal activities conducted by using computers. This advantage is shown in the act revised in 2012 in order to include many articles and contents which were not handled in the law established in 2006. While the other countries penal code has abstract examples of activities which are subject to punishment, the penal code of the UAE has a specific and concrete punishment for each illegal activity. The difference in such a legislation system of the basic law is related to the possibility to handle computer-related crimes and illegal activities by revising the current penal code.

In the next chapters, the major focus is to explain, understand, and examine the acts on prohibition of unauthorized computer access, publicity of immoral activities through the internet, destruction of information in computers, computer fraud, and the unauthorized creation of electromagnetic records in UAE law & other countries.
A Comparison Study of Cyber Law: Personal Study

<table>
<thead>
<tr>
<th>Crime</th>
<th>United Arab Emirates</th>
<th>Penalty in USA</th>
<th>Penalty in Saudi Arabia</th>
<th>Penalty in Pakistan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer espionage and abuse</strong></td>
<td>Maximum 2 years imprisonment and/or fine AED 500,000-1,000,000 Article 11</td>
<td>Usually imprisonment is not more than five years, but can reach ten years for repeated convictions. A fine under Title 18, 18 U.S.C. 1030(c)(4) can be titled with or without imprisonment, and under 18 U.S.C. 1009(g), victim can be compensated for damages and/or sue for injunctive relief. Other federal laws can be applied for different types of fraud such as 18 U.S.C. 1343 for wire fraud, 18 U.S.C. 2319 for copyright infringement, and 18 U.S.C. 1029 for fraud involving credit cards and device access</td>
<td>Usually imprisonment not more than ten years and/or a fine of $1.3 million (Article 7)</td>
<td>Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both.</td>
</tr>
<tr>
<td><strong>Obtaining information by unauthorized computer access</strong></td>
<td>Imprisonment and/or fine AED 250,000-500,000 Article 14</td>
<td>Imprisonment can be from one year to five years or can reach ten years depending on whether the offence was simple or repeated and/or a fine under Title 18, 18 U.S.C. 1030(c).</td>
<td>Usually imprisonment not more than a year and/or a fine of $130,000 (Article 3)</td>
<td>Whoever with dishonest intention gains unauthorized access to any critical infrastructure information system or data shall be punished with imprisonment which may extend to three years or with fine which may extend to one million rupees or with both.</td>
</tr>
<tr>
<td><strong>Trespassing in government cyberspace</strong></td>
<td>Minimum 5 years imprisonment and fine AED 500,000-2,000,000 Article 4</td>
<td>Imprisonment is usually one year and can reach ten years for repeated offences and/or a fine under Title 18. The fine can reach $100,000 for misdemeanors and $250,000 for felonies or can be calculated to be double the loss or gain resulted from this crime according to 18 U.S.C. 1030(e)</td>
<td>Usually imprisonment not more than ten years and/or a fine of $1.3 million (Article 7)</td>
<td>Whoever commits shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.</td>
</tr>
<tr>
<td><strong>Computer fraud</strong></td>
<td>Minimum 1 year imprisonment and/or fine AED 250,000-1,000,000 Article 11</td>
<td>Usually imprisonment is not more than five years, but can reach ten years for repeated convictions. A fine under Title 18, 18 U.S.C. 1030(c)(1) can be titled with or without imprisonment, and under 18 U.S.C. 1003(g), victim can be compensated for damages and/or sue for injunctive relief. Other federal laws can be applied for different types of fraud such as 18 U.S.C. 1343 for wire fraud, 18 U.S.C. 2319 for copyright infringement, and 18 U.S.C. 1029 for fraud involving credit cards and device access</td>
<td>Usually imprisonment not more than ten years and/or a fine of $520,000 (Article 4)</td>
<td>Whoever with the intent for wrongful gain interferes with or uses any information system, device or data or induces any person to enter into a relationship or deceives any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment for a term which may extend to two years or with fine which may extend to ten million rupees or with both.</td>
</tr>
</tbody>
</table>

Source: Author’s own research, based on comparison of Cyber laws

4.1. UAE Cybersecurity Laws 63

- Cyber Crimes Laws:

  President His Highness Shaikh Khalifa Bin Zayed Al Nahyan issued Federal Law No. 5 of 2012 (“New Cyber Crime Law”) a comprehensive piece of legislation on combating cybercrimes.

  Issued on 25 Ramadan 1433 AH, Corresponding to 13 August 2012 AD, ON COMBATING CYBERCRIMES


Federal Law 5 of 2012 have broadened the range of offences, definition of privacy violation and monetary penalties.

- Offenses: Any unauthorized access to the information or to the electronic sites is strictly charged under liability standard.
- Penalties: Disclosure or access to sensitive information shall raise the penalty and most of the violation crimes are entitled to deportation or imprisonment.
- Limitation on data protection law for comprehensive data.
- Information and policy related to internet regulation, information technology and another overseas telecommunication.
- Those caught gaining access to a website, network or system without authorization are to be imprisoned and fined at least Dh50,000, but fines can go as high as Dh1 million if personal information is stolen or deleted.
- Additionally, the law stipulates various penalties for a number of other cybercrimes, including insulting religions and their rituals, slandering public officials, forging electronic official documents, sending or re-publishing pornographic materials, reproducing credit or debit card data, and obtaining secret pin codes or passwords.
- The UAE has clear - and strict - laws with 51 Articles against cybercrimes, with various penalties that can include lengthy prison terms and fines of up to AED 3 million.
- All 51 Articles mentioned in the Appendix 1 on Page :84.

4.1.1. United States Cybersecurity Law

United States Cyber Laws and Privacy system is oldest in the History it most Robust and operational compare to other nations of the world. It has Federal Government Regulations and as well as State Level Directive Acts. It comprises of directives from the Executive Branch and legislation from Congress that safeguards information technology and computer systems of USA.
The Congress responded to the problem of computer crime by enacting several laws. The first federal computer crime statute was the Computer Fraud and Abuse Act of 1984 ("CFAA"). The fact that only one indictment was ever made under the original CFAA before it was amended in 1986 shows how difficult it is to write effective computer crime legislation.

CFAA is the most important computer crime statute in the U.S. because almost every other statute that deals with computer crime modifies the CFAA.

Originally CFAA had a major limitation because it required proof that the person accessed the computer without authorization. Thus, by focusing on the method of entry into the computer instead of the use of the computer, the statute excluded any crimes committed by an insider, which couldn’t be prosecuted under the CFAA. Another limitation of CFAA was specifically written into it, the statute forbade prosecution for access to a computer where the only thing of value gained by the intruder was the use of the computer itself. As such, according to CFAA, merely viewing data stored on the computer was not illegal even if access was gained without authorization. In 1994 Computer Fraud and Abuse Act was modified again in order to deal with the problem of “malicious code” such as viruses, worms and other programs designed to alter, damage or destroy data on a computer.

This was necessary because the old law only focused on access of the computer system and not on how that computer system was used. The amended CFAA could now be used to prosecute

those who transmitted "a program, information, code, or command to a computer or computer system" with the intent to cause damage to the computer or information in the computer or prevent the use of the system without the knowledge or the authorization of the owners of that computer. In addition, the law made it a crime to act "with reckless disregard of a substantial and unjustifiable risk" of damage or loss occurring.

Cybersecurity Information Sharing Act (CISA) – 65

Its objective is to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. The law allows the sharing of Internet traffic information between the U.S. government and technology and manufacturing companies. The bill was introduced in the U.S. Senate on July 10, 2014, and passed in the Senate October 27, 2015

Cybersecurity Enhancement Act of 2014: 66

It was signed into law December 18, 2014. It provides an ongoing, voluntary public-private partnership to improve cybersecurity and strengthen cybersecurity research and development, workforce development and education and public awareness and preparedness.

Federal Exchange Data Breach Notification Act of 2015:


This bill requires a health insurance exchange to notify each individual whose personal information is known to have been acquired or accessed as a result of a breach of security of any system maintained by the exchange as soon as possible but not later than 60 days after discovery of the breach.

**National Cybersecurity Protection Advancement Act of 2015:**

This law amends the Homeland Security Act of 2002 to allow the Department of Homeland Security’s (DHS’s) national cyber security and communications integration center (NCCIC) to include tribal governments, information sharing, and analysis centers, and private entities among its non-federal representatives.

**Cyber Security Enhancement Act:**

Cyber Security Enhancement Act (CSEA) was passed together with the Homeland Security Act in 2002, it granted sweeping powers to the law enforcement organizations and increased penalties that were set out in the Computer Fraud and Abuse Act. Electronic Communications Privacy Act, internet, Communications Assistance for Law Enforcement Act, internet, Cyber Security Enhancement Act, internet.

Prior to the passage of CSEA, ISPs were forbidden by the ECPA from knowingly divulging personal details of their customers, for example to gain the contents of an email stored on ISP’s servers the government needed a search warrant. CSEA reduced the amount of privacy of stored data, it allows an ISP to voluntarily hand over personal information about its customers to a government agent, not just law enforcement officials, if the ISP has a reason to believe that the information concerns a serious crime. Thus, allowing law enforcement to gain access to data
without a warrant that they would have previously required. CSEA also allows the ISPs to let the law enforcement to intercept electronic communications on its computers if the ISP believes that they belong to a trespasser who is not authorized by the ISP to be on their computer. Thus completely bypassing any need for a warrant as was previously required. The Act also authorizes harsher sentences for individuals who knowingly or recklessly commit a computer crime that results in death or serious bodily injury. The sentences can range from 20 years to life. In addition, CSEA increases penalties for first time interceptors of cellular phone traffic, thus removing a safety measure enjoyed by radio enthusiasts.

**Digital Millennium Copyright Act:**

The Digital Millennium Copyright Act (DMCA) was enacted in 1998. The basic purpose of the DMCA is to amend Title 17 of the United States Code and to implement the World Intellectual Property Organization (WIPO) Copyright Treaty and Performances and Phonograms Treaty, which were designed to update world copyright laws to deal with the new technology. The DMCA prohibits “circumventing a technological measure” designed to protect a copyright. By technological measure DMCA means an access control technology which can take many forms, such as copy protection on CDs, requiring cd-keys or product codes in order to use installed software and so on. As such anyone attempting to disable or bypass such a technological measure would be in violation of the law. DMCA also prohibits the manufacture or sale of devices or

---

[https://www.copyright.gov/legislation/dmca.pdf](https://www.copyright.gov/legislation/dmca.pdf)

68 [https://www.copyright.gov/legislation/dmca.pdf](https://www.copyright.gov/legislation/dmca.pdf)
programs whose primary purpose is to circumvent access control technology. In addition, DMCA prohibits the removal or alteration of information identifying the author, copyright holder, performer, or director of a work, and terms and conditions for use of a work for the purpose of facilitating copyright infringement. The Act provides civil remedies as well as criminal penalties for violating the copyright protection. DMCA grants several exceptions from its prohibition on circumventing access control measures. It allows reverse engineering for the purpose of achieving interoperability among computer programs, but this only comes into effect if there is no other way to achieve interoperability and if it is otherwise allowed, and most software licenses usually forbid it. Legitimate research regarding encryption is also exempt from the prohibition as long as the copyrighted work is lawfully obtained, a good faith effort was made to get the owner’s permission to break the access control measure, it is necessary for research that is being done and is not forbidden by any other law. The Act of course provides an exemption for the law enforcement and government agencies. The Act also provides an exemption in cases where the security measures are being legitimately checked. In addition, DMCA specifically permits the manufacture and sale of technology whose sole purpose is to help parents to control what their children view on the Internet. The Act includes provisions that provide broad immunity from liability for the ISPs. There is no liability for the ISPs if infringing material is transmitted through their network and computers, so long as the ISP has no control over the content of the materials on its network, and no copy is maintained on the service provider’s system. In addition, ISPs cannot be held liable for infringement for copies of material automatically made for the purpose of temporary storage, i.e., caching. ISPs are also made immune from liability if the infringing materials are stored on their systems, or for links to infringing materials if the ISP has no actual knowledge of the infringing activity, does not receive a financial benefit that can be attributed to
the infringing activity in cases where ISP has the right and the ability to control such an activity, and acts expeditiously to disable or remove any infringing material when notified in writing of such activity. Other Laws Used to Prosecute Computer Crimes in addition to laws specifically tailored to deal with computer crimes, traditional laws can also be used to prosecute crimes involving computers.

For example, the Economic Espionage Act (EEA) was passed in 1996 and was created in order to put a stop to trade secret misappropriation makes a crime to knowingly commit an offense that benefits a foreign government or a foreign agent. The Act also contains provisions that make it a crime to knowingly steal trade secrets or attempt to do so with the intent of benefiting someone other than the owner of the trade secrets. EEA defines stealing of trade secrets as copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying trade secrets without authorization. The Act, while not specifically targeted at computer crimes, nonetheless covers the use of computers.

Other federal criminal statutes that are used to prosecute computer crimes are the criminal copyright infringement statute, National Stolen Property Act and Economic Espionage Act of 1996 National Stolen Property Act, internet, - as I already mentioned the wire fraud statute. In addition to the federal government, many states have also passed computer crime laws. For example, in 1999, Virginia passed the Virginia Internet Policy Act, composed of seven bills: Virginia Computer Crimes Act; Encryption Used in Criminal Activity; Encryption Technology; Virginia Computer Crimes Act, Penalties; Freedom of Information; Privacy Protection; and Child Pornography and Indecent Liberties with Children
According to the EU directive and its restriction on trans-border transferring the data, they are allowed to transfer data outside the EU only if that countries are approved by the EU policy or having the similar restriction on privacy regulation.

This regulation was implemented in 1998 and around ten countries have approved to this regulation, which includes Israel, Isle of Man, Jersey, Faroe Islands, Canada, Switzerland, Argentina, Guernsey and Andorra.

However, US didn’t approved the directive trans-border transfer policy, but EU and US initiated a program named as safe harbour which specifies that individual entities of US should do self-certify and permit that they apply the principles to submit to jurisdiction of FTC if they are violated the directive.

Countries that mostly composed is the EU top ten countries, and it is important to follow and maintain the minimum threshold of the regulation but practically it was not possible that every member would agree to the directive trans-border policy which was introduces in the EU.

For example, UK is very weak in privacy approach as compared with France or Germany. Currently EU is in process to implement the directive and to form a centralized platform by adopting the enforcement framework and regulation

---

During this process UK has presented some more highly restriction and some terms and policies were not agreed by the other EU countries and looks like UK will not be in the regulation top ten list of EU. In place of UK, they would include other non-EU countries that agrees to the directive policy and followed the EU model such as Argentina, Canada and Israel.

This does not mean that US lacks in strong privacy and protection comparatively US is highly segmented in regulation and enforcement framework. Any organization is not following the regulation and not practising the standard security policy they get fines from the FTC.

The Children's online privacy act (COPPA) which applies data collected on children under 13 and adopts the principles of OECD.

Educational and other health data is regulated (under FERPA, and HIPPA) and the way the banking industry handles the financial data (under Gramm-Leach-Bliley) which is a significant regulation but this approach in lack of data privacy and leaves loopholes in the market for this reason US fails to make in the top ten list of EU framework.

4.2. United Kingdom Cybersecurity Law

The Privacy and Electronic Regulations (EC Directive) 702003 were introduced to address the growing prevalence of spam mail and its use in the transmission of spyware and adware. However, the regulations, which are not extra-territorial, only cover spam mail sent to private individual email accounts and not those transmitted to business accounts. In addition, the Information Commissioner alone decides if action is to be taken against offending organizations transmitting

---

70 https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/
the mail; and further the penalties which apply are limited in comparison to those imposed by the Computer Misuse Act.

4.2.1. United Kingdom - Computer Protection Law

The UK legislation takes a similar approach to that of the US enactments. The Computer Misuse Act 1990 provides for only three distinct areas of offending. Where the actions amount to unauthorized access to a system; where the access is unauthorized and occurs to facilitate or commit further offences; or where unauthorized modification of computer material occurs, an offence is committed.

4.2.3. United Kingdom - Online Theft Law

The Computer Misuse Act 1990 creates an offence where a person uses a computer to carry out a function which enables him to access data in an unauthorized manner. This access is secured by moving or copying the data to another location or storage medium for personal use. Whereas the Theft Act 1968 makes no provision for the theft of data, it appears that such actions are covered by section 1(1) above. In addition, Data Protection Act 1998 section 55 provides for an offence where a person ‘knowingly or recklessly, without the consent of the data controller, obtains or discloses personal data’ where such data relates to a living individual and can be used to identify that person. However, while the data is of a kind which may be copied or stolen, it does not include

71 [https://www.gracefulsecurity.com/uk-cyber-crime-law/](https://www.gracefulsecurity.com/uk-cyber-crime-law/)


data which is created by a user on his personal computer or held by a company on the internal network.

4.3. Privacy Law of the world

Below are top ten list of countries which maintain the similar level of privacy policy and protection. Some other countries are also based on the similar criteria and best privacy policy includes countries like Norway, Spain, Slovenia and the Czech Republic.

(1) Canada
(2) Switzerland
(3) Portugal
(4) Israel
(5) Germany
(6) France
(7) Sweden
(8) Greece
(9) Argentina
(10) Finland

75 https://www.quora.com/What-10-countries-have-the-toughest-Internet-privacy-laws
Figure 13: The Privacy Score Board

https://www.uktech.news/news/these-5-countries-were-ranked-best-for-privacy-infographic-20131015
4.4. Privacy Law of Spain.76

Among the EU countries, Spain has some of the strictest legislation on personal data protection. It has transposed all of the EU Directives related to this matter. Spanish law has even been successfully challenged before the European Court of Justice (ECJ) for imposing additional requirements in its domestic legislation regarding the release of personal data without the consent of the data subject. Spain’s data protection agency has been very active and responsive to citizens’ complaints and imposes heavy fines on violators of data protection laws.

Spain has recently been engaged in “right to be forgotten” litigation with Google. Although Google obtained a positive ruling from a Spanish court on jurisdictional grounds, the court did not address the right to be forgotten. That issue went to the ECJ for an advisory opinion, which will be binding on all EU Member countries when issued.

4.5. Legal Framework

The 1978 Spanish Constitution provides for the protection of personal and family privacy, stating that the law must set limitations on the use of information technology in order to guarantee the honor as well as the personal and family privacy of individuals and the full exercise of their rights. This provision constitutes the framework and basis for Spanish legislation on data protection, which in 1978 was a novel concept unlikely to be found in a constitutional norm.

In 1999, Spain enacted an Organic Law on the Protection of Personal Data (LOPDP) to transpose the European Union (EU) Data Privacy Directive (Directive 95/46). The LOPDP governs personal and family privacy, and guarantees and protects fundamental rights and freedoms with respect to the processing of personal information. In 2007, Spain enacted an implementing regulation to the LOPDP that also serves to transpose Directive 95/46: The Regulation on the Development of the Organic Law on the Protection of Data (RLOPDP), which aims to bring more legal certainty to the

76 https://www.loc.gov/law/help/online-privacy-law/spain.php#_ftn1
https://www.loc.gov/law/help/online-privacy-law/spain.php#_ftn1
data protection regime, particularly on issues that over the years have proven to be in need of further regulatory implementation.

In 2007, Spain enacted Law 25/2007 on the Retention of Data Generated or Processed in Connection with Electronic or Public Communications Networks, to transpose European Directive 2006/24/EC, on Telecommunications Data Retention. On March 30, 2012, Spain transposed Directive 2002/58/CE (the E-Privacy Directive) as amended by Directive 2009/136, when it passed Royal Decree 13/2012, introducing the European regulation of “cookies” into domestic law, as discussed further in section II(B) of this report.

4.6. Council of Europe – Cybercrime Convention

This Convention is the very first international treaty on crimes committed using the Internet services and other computer networks, dealing specifically with computer related fraud, infringement of copyright, breach of network security and child pornography. It also has a sequence of capabilities and procedures such as the search of computer networks and interception.

Its principal purpose, set out in the preamble, is to gain a common criminal policy aiming the security of society resisting cybercrime, chiefly by adopting suitable legislation and advance international co-operation. The Budapest Convention is supplemented also by an added custom to the Convention which has been embraced in the year 2003.

4.7. Legal Divergences

- The fleeting growth of the Internet and sophistication of cybercrime remains to surpass the potential of the legal system to respond and react accordingly. The attribution problem leaves policing and accountability especially uneasy.

- Cyber virtues are scattered between the private sector and public sector, and the private sector contains of a broad range of different bodies.

---

• Deficiency of international coordination on cyber issues do exist, resulting in no centralized international cyber threat data sharing or frequent computer incident response teams.

• Different values among countries; different levels of preparedness; different degrees of interest and risks.

Chapter-5

5.Cases of Cyber Crime in UAE.

5.1.UAE: A target of 5 per cent of global cyber attacks

UAE takes a significant chunk of attacks, with 5% overall and if an expert is to be believed there is a YOY increase of about 500% in this activity. Rabih Dabbousi, an expert from a reputed cyber security firm ‘Dark Matter’, has cited the finance sector to be the most vulnerable in the UAE amongst other disciplines.

“The ever-increasing adoption of technology potentially increases UAE’s attack surface which is rapidly expanding by the day. Typically, cybercrime is motivated by monetary gains. The never stopping volume of money related exchanges in the UAE, the foundations of monetary free zones and the wider interest of investing resources into the nation are just a part of the reasons why banks and other budgetary establishments are always being targeted,” he said.

Dabbousi further explained, “The oil and gas industry is the second most visible and targeted in the UAE. “Intruders who infiltrate these immense organisations do so in order to gain the credibility of others in their fraternity. As this division further digitizes, gets proficiency, efficiency and upgrade to the general plan of action, it likewise offers chances to assailants to utilize normal instruments,” he included.

As UAE encourages leveraging newer technology, innovation and differentiation to make one’s life easy, the country’s visibility and profile is also expanding across the planet. “The fact that we

are constantly prone to attack day in and out is something we have to agree in our lives. Cyber security in UAE has emerged as proactive force. Hence we are expanding in global arena establishing economy socially and competitively and visible in several ways we are expanding in global arena establishing economy socially and competitively and visible in several ways” Dabbousi said. “However, these are merely growing pains,” he added. Dark Matter is working to set up a cyber-security academy in UAE to develop local talent in the field.

5.2. Face book Ghost allegedly selling drugs arrested by Abu Dhabi Police

On the 27th of September 2016, the Abu Dhabi police had reportedly arrested three men caught for allegedly dealing in drugs on social media, concealing their identity.

Impersonating as ‘Facebook Ghost’, the three accomplices of Arab nationality were using Facebook to reach naïve customers in an attempt of making money without disclosing their origins. Several other accused of committing such crime where nabbed by the Criminal investigations teams for selling drugs.

5.3. Hacker Holds UAE Bank to Ransom, demands 3m$  

An evil digital criminal has hacked into a Sharjah bank and is currently holding it to emancipate by releasing private information of customers on person to person communication and microblogging website Twitter like clockwork, XPRESS can uncover.

The criminal who passes by the moniker Hacker Buba and utilizizations a stolen photo of a bank staff says he won't stop until the point that the bank pays him an undisclosed measure of payoff cash in the computerized money Bitcoin (clarified beneath) by this end of the week.

Consistent with his oath, he has been posting the record proclamations of government elements and scores of UAE firms and people every day since November 18 2015.


80 http://gulfnews.com/xpress/courts-crime/hacker-holds-uae-bank-to-ransom-demands-3m-1.1626394
On November 23, the bank inspired Twitter to suspend Programmer Buba's record yet the relief was brief. The next day, he made another character and was back with a retaliation, transferring account proclamations of 500 bank clients in only one tweet connection.

Prior, Programmer Buba had sent cautioning instant messages and messages to a few bank clients, saying their records were under his "control" and that they should pay him straightforwardly or get their bank to do as such falling flat which he would discharge their bank proclamations on the web.

Hours after the fact he completed the danger, making alarm among clients.

The bank conceded the digital assault and affirmed they have been sent a payoff note.

"Truly, there was an information break and we have been reached by Programmer Buba. He is requesting cash however I can't uncover how much. This is shakedown. We have revealed the issue to UAE National Bank. The Telecom Administrative Specialist's (TRA) PC Crisis Reaction Group (aeCERT) is researching," the bank's boss money related and working officer told XPRESS.

"We won't offer in to any coercion danger. Regardless there has been no money related misfortune. All what this man has is some client data and he's endeavoring to utilize it as a negotiating advantage," he included.

Nonetheless, clients influenced by the break, perhaps the most exceedingly terrible in UAE's history are shocked and irate. "This is significantly more genuine than what it's made out to show up. I feel stripped as my whole organization stands uncovered. Our money related exchanges, customer subtle elements, everything is on an open stage," said the fund officer of a speculation firm in Dubai.

The proprietor of an Abu Dhabi based contracting organization said the harm to his business was "irreversible" while the chief of a Sharjah-based nourishment enterprises firm reprimanded the bank for remiss digital security.

"Digital assaults are winding up progressively well-known due to the vulnerabilities in the framework planner. Banks need to put resources into frameworks that discussion to each other cleverly. The watchword here is reconciliation. A framework that is incorporated from the security viewpoint averts hacking and enables one to act progressively if there should arise an occurrence of a digital assault," said Hamed Diab, territorial chief MENA, Intel Security.
Another digital security master said it's almost difficult to follow such programmers as they are specialists in covering their advanced impressions and making counterfeit trails. "Programmer Buba's Twitter area focuses to a region in Hungary, his past posts are in Indonesian dialect while the SMS sent to clients were from a cellphone with a UK number," the master said.

Many organizations and people didn't know their own points of interest had been posted online until the point that XPRESS called them.

"I am stunned past mistrust. At any rate the bank could have educated us," said the originator of a land firm in Dubai.

It's not clear how the programmer broke into the bank's PCs. In an immediate message to this columnist by means of Twitter, Programmer Buba asserted he is looking for $3 million and approaches the bank database and go down records from every one of its servers.

**5.4 Australian Women Deported from UAE over Facebook post:**

A 39-year-old Australian woman was sentenced imprisonment on 12 July, Sunday in UAE’s capital for charges of cybercrime. The woman, Magi, a graphic designer moved to Abu-Dhabi from Perth in 2012. On face book she posted picture of a car parked along two No parking zones outside her apartment. Australian Broadcasting Corporation (ABC news) reported that Magi didn’t disclose the name plate, owner and other details of the vehicle.

A complaint was lodged to the Abu-Dhabi police and Magi was found guilty for “using offensive words on social media” as reported by ABC news. Magi attended court on Sunday to pay her penalty and was detained until deportation formalities had been done.

DFAT emphasized that anyone who is visiting, working or living overseas must be aware of the rules and regulations of that particular country.

---

5.5 Dubai football coach accused of cyber-blackmailing boy\textsuperscript{82}

His warning comes in light of referring a 35-year-old Asian football coach to the Dubai Court of First Instance where he will be tried for blackmailing, molesting and sexually abusing a 15-year-old boy through the use of social media.

Prosecution records said the coach lured the boy to his car where he coerced the 15-year-old to strip naked and filmed him [still images and video], then used the indecent images for blackmail purposes. The suspect abused him sexually and molested him as well.

Cyber-blackmail is the act of threatening to share someone’s confidential and private information or material [audios, photos or videos] with others against personal gain and demands or for money.

“We are cautioning the parents in advance to watch out for their kids’ safety and well-being while using social media in order not to fall victims of cyber-blackmailers. There is increase in such a crime and it is still marginal … we are sending this warning from the beginning to keep it under control. Any crime starts small, then becomes viral and trendy. We call on parents to monitor their children while using social media in a moderate manner … because if they monitor them strictly, then that might push the children to use social media at places where they are unmonitored and unattended,” Rustom told Gulf News yesterday.

Cyber-blackmail is a crime that targets children and adults, according to Rustom, who said the Family and Juveniles Prosecution (FJP) of Dubai Public Prosecution recently investigated a few cases in which minors [under 18] were abused and exploited by cyber-blackmailers.

5.6. Hacker who leaked details of 1,300 people to Islamic State gets 20 years in jail

1. In September 2016, a computer hacker revealed the identity of 1000 US government and military employees as potential targets to Islamic state. He was convicted and sentenced to 20 years’ imprisonment.

2. The defence had argued for a mere 6-years term claiming that their client Ardit Ferizi intended no harms nor was an active supporter of the Islamic State,

3. “He was a nonsensical, misguided teenager who did not know what he was doing,” said public defender Elizabeth Mullin. “He has never embraced ISIL’s ideology.”

4. Ferizi, 20, a native of Kosovo who was arrested last year in Malaysia, is the first person convicted in the US of both computer hacking and terrorism charges. He affirmed hacking and extracting details like names, passwords and phone numbers of about 1300 people with government and military addresses. The Islamic State published the names to threaten them.

5. On Fridays hearing the US district judge Leonie Brinkema demanded an explanation from Ferizi who struggled to maintain that it all happened rather rapidly.


7. Prosecutors asked for the maximum sentence of 25 years.

8. “The defendant’s conduct has indefinitely put the lives of 1,300 military members and government workers at risk,” said Assistant U.S. Attorney Brandon Van Grack.

9. He disputed the idea that Ferizi’s crime was a whim. Last year he operated a website devoted to propagation of the Islamic states agenda before supplying the names to Islamic state hacking

---

division. During online conversations Ferizi defended the Islamic state and was fully aware of the high risk he was putting them at, Von Grack said.

10. “This was a hit list. The objective was to find and “Strike at their necks”, Von Grack said mimicking language of the Islamic state used while publishing the names.

11. Mullin countered that nobody on the list has been harmed, and said that much of the information Ferizi helped disseminate was publicly available anyway.

12. Court papers describe a difficult life for Ferizi, who was nominally raised as a Muslim and was just 4 years old when NATO airstrikes forced Serbian forces to withdraw from the territory, which subsequently became independent. Ferizi’s uncle was murdered and his father was kidnapped during the war, as per letters written by Ferizi’s family.

13. As a teenager, Ferizi got in trouble for hacking into Kosovar government databases, but he avoided jail. Ferizi went to Malaysia to study cybersecurity, but continued his hacking activities and developed worsening mental health problems, defence lawyers said.

5.6. Hack of Saudi Arabia Exposes Middle East Cybersecurity Flaws

A rare use of offensive cyber weapons targeted at erasing data massively on Saudi Arabia in Dec,2016. The strike used some malware that was used in 2012 assault on Saudi Aramco which destroyed 35,000 computers.

The Middle East, home to almost half of global oil reserves and much of its natural gas, is also a magnet for some of the world’s costliest cyberattacks, PricewaterhouseCoopers LLP said in a March 2016 report. The threat is set to grow as online activity mushrooms amid the region’s myriad geopolitical conflicts and tensions.

“For the last couple of years, the U.S. Department of Defence has been trying to get the Gulf states to harden their defences,” said James Lewis, senior vice president at the Centre for Strategic and International Studies in Washington, D.C. “Some of them are in appropriate shape. Saudi Arabia is not.”

The central bank, known as the Saudi Arabian Monetary Authority, denied that its systems were breached. The country’s General Authority of Civil Aviation said damage to its networks was limited to some office systems and employee e-mails.

While the assault was like the one that hit Saudi Aramco four years ago, the impact was “much smaller” and did not disrupt transportation or aviation services, said Abbad Al Abbad, executive director for Strategic Development and Communication at the Riyadh-based National Cyber Security Centre.

“We will always have a race between those who are exploiting security vulnerabilities and those who are defending against them,” said Wael Fattouh, a Saudi-based PwC partner specializing in technology risk assurance.

Public and government facility are more affected by cyberattacks in the Middle East. A unified regional online market could expand to include 160 million users by 2025 and add about $95 billion to gross domestic product, according to consultant McKinsey & Co. Saudi Arabia, the United Arab Emirates and other Arab states in the Gulf are leading this growth.

“The rapid adoption of digitization in the U.A.E. and Gulf Cooperation Council countries has made the region an attractive target for a wide array of security breaches,” Mohit Shrivastava, a senior analyst for information security at consultant Markets and Markets, said in an e-mail.

---

85 Kaspersky Lab Report By GREAT
FROM SHAMOON TO STONEDRILL “Wipers attacking Saudi organizations and beyond”

69
According to Kaspersky Lab’s Q1 malware report, the company’s experts detected 2,900 new ransomware modifications during the quarter, an increase of 14 percent on the previous quarter. There is an increase in number of ransomware modification in the database of Kaspersky lab which already includes 15000.

Kaspersky lab security solution in 2016 were successful averting 372,602 ransomware attacks.17%of these targets corporate sector. The number of victimised users increased by 30% compared to Q4, 2015.

One of the most noticed and widespread ransomware in Q1, 2016 was Lucky. Kaspersky Lab products traced consistent attempts to infect users with this Trojan in about 114 countries, and as of early May 2016, it was reported to be active. One other such ransomware called Petya was interesting from a technical perspective thanks to its not confined to encrypt data stored on the computer, but also to overwrite the hard disk drives master boot record (MBR), leaving infected computers with booting problems. As per the findings of Kaspersky lab the three-popular ransomware families in Q1 were teslacrypt (58.4%), CTB-Locker (23.5%), and Crypto wall (3.4%). All these spread through spam emails containing malicious content or links to infected pages.

“One of the primary reasons why ransomware has gained popularity is due to the simplicity of the business model deployed by cybercriminals. Once the ransomware obtains entry into the users’ machine, there is hardly any hope of getting rid of it without compromising personal data. As if that is not enough, they demand to pay the ransom in Bitcoins that makes the payment process anonymous and almost untraceable which is very attractive tool for fraudsters. Another trend causing trouble is the Ransomware-as-a-Service (RaaS) business model where cybercriminals pay a fee for the propagation of malware or promise a percentage of the ransom paid by an infected

user,” says Aleks Gostev, chief security expert in the Global Research and Analysis Team (GReAT).

There are many more reasons for the steady rise in ransomware attacks: users believe the threat is inevitable, businesses and individuals are not aware of the technology countermeasures that could help to prevent infection and the locking of files or systems; and by neglecting basic IT Security rules they allow cybercriminals to gain.

Kaspersky Security Network statistics for January-March 2016 shows that in the Middle East, Turkey and Africa (META region) an average of 45% of users had faced security incidents relating to local in META region local networks and detachable media faced 45% of security threats, 15% users encountered web-related threats. Kaspersky labs detection in the first quarter of 2016 then 2015.

Apart from an overview of ransomware outbreaks Kaspersky lab has summed up the cyber threats forced globally in Q1 2016. The security network data of lab gave the following as malware landscape in Q1 2016.

Close by an outline of the major ransomware flare-ups, Kaspersky Lab has checked the general level of digital dangers in Q1 2016 comprehensively. As indicated by Kaspersky Security Network data, the malware scene in Q1 2016 was the following:

- 21.2 percent of Internet users had gone through web-based attacks at least once, which is 1.5 percentage points lower than in Q4, 2015.

- 44.5 percent of Kaspersky Lab solutions users faced a malicious threat at least once, which accounts to 0.8 percentage point increase on Q4, 2015.

- Kaspersky lab solutions averted the danger inflicted up to 459,970 users by cyber offender’s malicious attempts to access bank details and steal their money.
• Adware amounts to 42.7 percent of mobile threats which makes it the leading one. 4,416 new mobile Trojans were detected which is 1.7 times more statistically than the earlier quarter.

• The number of new mobile ransomware has increased 1.4 times, from 1,984 in Q4, 2015 to 2,895 in Q1, 2016. Eight of ten UAE firms are vulnerable to cybercrime and hacking.

On the 14th of February, 2015, it was reported that formidable IT authorities of UAE unanimously agreed that cybersecurity threats were potentially increasing across the region. F5 Networks; a global application delivery networking leader conducted a survey which reported that most of IT decision makers acknowledged their more vulnerability than ever to cyber threats. The findings come ahead of the months IDC CIO summit in Dubai.

Common cybersecurity threats include distributed denial of service (DDoS) attacks, phishing/spear-phishing emails, data theft, “zero-day” software assaults, web application exploits, and website defacement. “Traditional security methods such as next generation firewalls and other reactive measures are losing the fight against a new breed of attacks,” said Garth Braithwaite, Middle East Sales Director, F5 Networks.

“Security is now very much about the protection of the application, the enforcement of encryption, and the protection of user identity. Increasingly, it is less about the supporting network infrastructure. Organisations need a security strategy that is flexible and comprehensive, with the ability to combine Domain Name System (DNS) security, DDoS protection, network firewalls, access management, and application security with intelligent traffic management.”

‘Markets and Markets’ suggests that the Middle East cybersecurity market is on course to grow from $5.17 billion in 2014 to $9.56 billion in 2019 at a CAGR of 13.0%. In its 2014 Global Economic Crime Survey, ‘PricewaterhouseCoopers’ identified cybercrime as the second most common form of economic crime reported in the Middle East.
The top cybersecurity challenges listed in F5 Networks’ survey include changing motivations for hacking (33% of respondents), the virtualization of server desktops and networks (31%), difficulty in managing a variety of security tools (29%), the increasing complexity of threats (29%), the shift from datacentre-focused infrastructure to the cloud (25%) and the move from traditional client-server applications to web-based applications (24%).

In order to adapt and cope, 57% of decision-makers wanted a better understanding of the different types of security threats, 24% called for consolidated management of their different security tools, and 20% wanted a stronger focus on security issues from management.

“With multi-dimensional or 'cocktail' style attacks - DDoS attacks combined with application layer attacks and Structured Query Language (SQL) vulnerabilities –organisations really need to look at a multi-stack security approach, combined with a process to handle internal control,” added Braithwaite.

5.8 Know UAE's law on cybercrime to stay on the right side of the law!87

Social media is like a double-edged sword. It's a powerful tool to connect millions and send your views across, and share updates of your day to day life. But, at the same time, it has its risks. Whatever you post online becomes public information at once. You unknowingly share your life events with strangers, who may use that information to their advantage.

Thankfully, the UAE government has put in place laws that protect the individual's privacy, and ensure miscreants are brought to justice. Here are some rules you should keep in mind:

Posting photographs: Care needs to be taken when posting pictures of others online, including via social media sites since the Cyber Crimes Law (Federal Law No. 5 of 2012) makes it an offence

87 (Legal pointers by Dubai-based law firm Al Tamimi & Co.)
to use any IT means to breach someone else's privacy, including by taking pictures of others, or publishing or displaying those pictures.

Privacy and confidentiality: Disclosing secrets relating to someone's private life, without that person's consent can attract liability. Similarly, disclosure of confidential information, such as information belonging to an employer, can also attract legal liability in the UAE.

Defamatory statements: The Penal Code makes it an offence to publish information that exposes another person to public hatred or contempt, or to make a false accusation which dishonors or discredits another person.

Content contrary to morality, social cohesion: It is an offence to use any IT means for activities which are inconsistent with public morals and good conduct including content that is un-Islamic, blasphemous, lewd, that encourages sinful activity, or that is aimed at corrupting minors, etc.

Online monitoring: UAE TRA monitors online content available and prohibits content for hacking and malicious codes, Internet content providing unlicensed VoIP services and other illegal Internet content.

Licensed service providers (du and Etisalat) can also block online content if required and subsequent to complaints of abuse or defamation, authorities can take legal action against those running the sites after verifying the validity and seriousness of the complaint.

5.10. UAE to get tough on IP address forgery

On the 18<sup>th</sup> of January 2016, The Federal National Council (FNC) decided to review a drafted law for proposing more than three years in prison and a fine up to 2 million AED for IP address forgery with criminal intent. The bill, which introduces changes in Federal Law No. 5 of 2012 on

---

combating cybercrimes, seeks to crack down on people using a fraudulent computer network protocol address.

Under the current law, IP address forgery is a minor offence punishable with a jail term of between 24 hours and three years; and a fine of up to AED 500,000. “The proposed amendment shows that the UAE authorities are keen to crack down on so-called IP spoofing by imposing harsher penalties for offenders,” said Dino Wilkinson, legal expert in Abu Dhabi. A relevant article states that it is an offence to use a fraudulent computer network protocol address by using a false or third party address for committing a crime or preventing its discovery. A prominent publisher sent out an article stating that it is an offense to utilize a fraudulent computer network protocol address by utilizing a false or external address for carrying out a wrongdoing or keeping under cover its whereabouts.

It is therefore important to note that there must be a crime committed or concealed, in addition to the IP address spoofing activity, for a person to be liable under this provision of the law. For example, this could be a hacking or denial of service attack, which are criminalised under other provisions of the cyber-crimes law.

CHAPTER 6

6. Conclusions and Recommendations:

6.1 Conclusion:

It is difficult to convict an offender due to the divergence of laws among other countries because the nature of internet creates a question of jurisdiction about from where the offence is committed and initiated every part of the world is connected over the internet and someone sitting in one part of the world can assaults target the globe.
The laws differ from country to country and it is difficult to arrest the attacker if he initiated the offence from a different country and its difficult to punish the offender if that country’s law is different in a given situation.

Standard law should provide protection on cybercrime acts and safeguard the information, national infrastructure and the rights on individual property. A convention on cyber law was commissioned by UAE as a signatory which agreed to inaugurate the convention.

Later jurisdiction decided to implement new law by seeing the growth in the cybercrime across the world where offenders were easily escaping after committing the offence. Hence eventually the jurisdiction was formed to implement a law to monitor such acts. Thereby US and UK have implemented a common law and others are following suit.

After UAE introduced the cyber-law for other vulnerabilities caused to the national infrastructure, damage to the premises or theft, this criminality was focused in the law. Apart from this they have no rights to access to the unauthorised system or data. If the access is achieved to the intruder, they can destruct the data or can create denial of service.

As mentioned above jurisdictions which have decided to implement a law against the offender were United Kingdom and United States of America they have agreed to prosecute the criminal of cybercrime and also develop new rules them from re-attempting the crimes.

6.1.1 GCC Cybercrime Center like ECC (European Cybercrime Center)

The establishment of the GCC Cybercrime Centre will strengthen the fight against cybercrime. The GCC help the Union member governments, businesses and citizens to have the tools to tackle cybercrime and make the GCC Nations cleverer and stronger in its fight against cybercrime and efficient in solving any problem. The GCC Cybercrime Centre will have information on cybercrime. The center will support investigation, building capacity to struggle on cybercrime through working out, creating awareness and providing best practice on cybercrime. Moreover, the Centre will build experts community for all sectors of society to battle and stop cybercrime and online child sexual exploitation.
GCC will collaborate with companies involved in internet security like the financial sector, academic experts, civil society organizations and National Computer Emergency Response Teams forming a safer Communication information around the world by improving and maintaining the high security of information infrastructures and combating any computer activities related crimes. The GCC Union set four principal points which should be included in any cybercrime policy are:

1. The adoption of adequate, substantiates, and procedural legislative provisions to deal with both domestic and transnational criminal activities.

2. The availability of a sufficient number of well-trained and well-equipped law enforcement personnel’s.

3. The improvement of the cooperation between all stakeholders, users and consumers, industry, and law enforcement.

4. The need for ongoing industry and community-led initiatives.

- Awareness Campaign should be launched by the ISPs, Mobile Operators and Government Bodies.

- (Rodriguez-Ferrand, 2012) **UAE Should Follow PRIVACY LAW like Spain** which is currently awaiting the advisory opinion of the ECJ (European Court of Justice) to clarify the scope of the **right to be forgotten**. At the same time, the EU has been drafting stricter rules on data privacy, putting greater responsibility on companies such as Facebook to protect users’ information and threatening those who violate the rules with heavy fines, of up to 2% of the company’s yearly income. Once these rules are adopted, companies that are already processing data in Spain will not experience a great deal of change, because many of the new EU rules have already been in force in Spain under the LOPDP and RLOPDP. The EU proposal, which will become EU legislation in 2013 if approved by all EU Members and the European Parliament, aims to address new technologies that were developed after the current data protection legislation was adopted, in order to better protect consumers’ personal data and privacy.
6.1.2. Proposed Computer Crime Legislation Like USA.

UAE can adopt the two most significant proposed legislations in the U.S. Congress namely the **Fraudulent Online Identity Sanctions Act (FOISA)** and **Computer Software Privacy and Control Act (CSPCA)**. FOISA attempts to tackle the problem of criminals registering online domains under false identification, it includes a provision that would increase jail term for people who provide false contact information to a domain name registrar and then use that domain to commit copyright and trademark infringement crimes. The law, if passed, would not make providing false contact information to domain name registrars a crime by itself only if that domain is then used in committing a crime would FOISA be used against the criminal.

CSPCA is meant to deal with the problem of spyware and adware that has plagued so many people. The Act, if passed, would prohibit transmission of software that collects and transmits personal information about the owner or operator of the computer, monitors and transmits web pages accessed by the owner or the operator or modifies default computer settings such as home page, unless the owner or the operator give their consent there can be no activity. The software has an uninstall option also built into it.

- Lack of IP Telephony Transparency Law and VPN Guidelines are vague for Inter country and Intra Country.

- As a whole, the vision of this recommendation is that this region and its population, should be aware of Cybercrime and the laws pertaining to it just as in other cases like murder, theft etc. Speaking metaphorically, there are no two thoughts that the Networking field is ‘running’ so fast in this region that the feet of this region are finding it difficult to handle. It is here that the organizers of this region need to make sure that it has enough protection, medication and nutrition, to check that crime cannot overcome it and win the race.

6.2. Recommendations:

Every national government in the region is striving to create a secure digital environment, but too often these efforts are fragmented, tactical, and reactive. Moreover, they do not include the
participation of all essential stakeholders. Consequently, governmental responses often lag behind the ever-evolving threat landscape, and the defensive measures taken are circumvented or exploited. A strategic approach to national cyber security is needed that follows a “CCC” framework — comprehensive in nature, collaborative by intention, and capability-driven.

UAE government can apply the CCC framework in their own national cyber-security programs. First, they should establish a centralized national cyber-security body, with a clearly defined mandate. The established body should define a national cyber-security strategy and establish a national dialogue.

They should be capable of building cybersecurity capabilities both reactive and preventive with implementation of new capabilities government will also ensure that digitization of nation.

Adoption of new technology, digitization and amount of resources in Middle East countries made this region attractive target for cyber-attacks. In fact, the major organizations, government sectors and vital sectors have sustained the damage from cyber-attack.
Rapid increase in the technology will simultaneously increase the risk of cyber-attack, so parallel UAE should also improve and implement strong security policies itself to protect itself from the cyber threats. Therefore, as recommended best practice is to advance precaution and preparation of a backup plan for any kind of disaster recovery. It exceeds the global average by more than four-fold, a differential that has increased in recent years.

Due to the evolving nature of IT, the majority of organizations have had to respond by changing the way their company approaches security. In most of the countries surveyed, one of the greatest factors has been the change in IT operations, especially as firms move to cloud computing or implement new mobility strategies. Another significant driver of change in security approach is reports of security breaches at other firms. Furthermore, across all the companies surveyed, nearly three quarters report have at least one security breach/incident* in the past 12 months (73%).


Due to the evolving nature of IT, the majority of organizations have had to respond by changing the way their company approaches security. In most of the countries surveyed, one of the greatest factors has been the change in IT operations, especially as firms move to cloud computing or implement new mobility strategies. Another significant driver of change in security approach is reports of security breaches at other firms. Furthermore, across all the companies surveyed, nearly three quarters report have at least one security breach/incident* in the past 12 months (73%).

**Figure 14:** Number of virus-infected computing devices in the Middle East

**Figure 15:** Occurrence of security breaches in past 12 months
6.3. The State of Cybersecurity in the UAE

The counter risks many states have adopted cyber capability as an integral part of economic development plans. The challenge for UAE is that has real and compounding intensity of risky incursion to accessibility, integrity and resilience of its critical networking systems and infrastructure. Threats to their sector are distinctly on a rise. To counter balance this vulnerability UAE plans to launch a Military Cyber Command in Armed Forces Headquarters to run parallel to National Security Authority (NESA).

In order to improve efficiency of cyber defense force UAE needs to compound its human capital. This requires recruiting and hiring security professionals and training for cyber security sector. National Cyber Security Alliance’s (NCSA) and Raytheon survey on cyber career interest and the knowledge in educational preparedness. Schools sectors will not provide much awareness about the cybercrime and activities or about the cyber career information and also they don’t encourage
developing the cyber skills, schools need to conduct seminars and arrange cyber career awareness programs. Cyber defense is lacking due to insufficient cyber talent which is considered as a gap in cyber knowledge. According to a research private sectors offer more cyber security plan to government sector and leave the public sectors with insufficient manpower.

6.4. Cyber-wellness profile of UAE.

6.4.1 Cyber Security and legal measures.

Following are the specific legislations on cybercrime.

- Cyber-crime Decree No.5 of 2012 is introduced by the Federal Law.
- To prevent the technology crime federal law no.2 of 2006.
- Electronic commerce and transaction regulation related to legislation and cybersecurity federal law no.1 of 2006 was introduced.

6.4.2 Technical Measures and Certifications.

CIRT also known as aeCERT is a UAE official recognized security standard. For implementing standard cyber security framework internationally UAE doesn’t have recognized cybersecurity standards. UAE also doesn’t have any cybersecurity framework certifications and accreditation of national agencies and professionals.

6.4.3 Recommended Security measures for Organization sectors.

- **Policy**- Adopt the officially recognized policy of telecommunication sector.
- **Road-map** –According to the further study there is no cybersecurity for national governance There is need to improve such kind of activities.
- **Responsible agency**-TRA (Telecommunications Regulatory Authority) is responsible for implementing security policies and the cybersecurity strategies should improve security measures and perform penetrating testing.
6.4.4 Building the capacity, manpower development and certifications.

- **Standardization** - aeCERT is the only recognized and officially responsible body of research and analysis of cyber security standards.

- **Manpower** – Both recognized and standard TRA and aeCERT launched an awareness program for safety of cyber security where aeCERT is also a legal advisor of cybersecurity education and awareness.

- **Professional certifications** – Database which records all the public sector professionals under the aeCERT.

6.4.5 Child Online Protection.

- **Rights**- Article 12 .16,17(e) and 34(c) specifies the convention of child rights

- **Institution support** – there is no declaration and protection against the child online act, there is no agency responsible for children online protection

6.5. Practical Approach

- Building knowledge and promoting cybersecurity protection policies.
  - Conducting awareness programs in universities with support from government.
  - Certifying the programs.
  - Information about economic potential for investing in the cyber security programs and training.

- Professional training to promote competence
  - Training for state personnel’s.
  - Merging with professional certification
  - Private sector security improvement.
  - Professionalism in cybersecurity and knowledge framework.

- Capabilities and cybersecurity updates.
  - Updating the security policies.
  - Introducing a global and standard culture of cybersecurity.
  - Collaborating with national CERTs to strengthen the cooperation.
- Developing capabilities and strategies for ICT capacity-building.
- Promoting the actual behavior of cybersecurity.
  - Training programs to overcome the limitations.
  - Preparing cybersecurity international legal framework.

6.6. KEEPING CHILDREN SAFE ONLINE: TIPS FOR PARENTS

An RIT study reveals that a high percentage of cybercrimes against children are committed by other children. The perpetrator is also significantly more likely to be a fellow student than an adult.

There are some basic steps parents can take to help protect their children against Internet dangers. The Cyber Safety and Ethics Initiative offer the following tips for parents to help keep their children safe online:

- Keep your computer in a common area of your home, such as the family room.
- Monitor your children's Internet habits and ask them to show you websites they visit.
- Talk to your children about cyber ethics. Remind them that bullying, cheating and illegally downloading music, movies and software are wrong.
- Develop an "Internet usage contract" for your children and sign it.
- Review your children's instant messenger profiles and messages, in addition to their social networking profiles on sites such as Facebook and Myspace. Periodically take a look at the profiles of their friends as well.
- Set time limits on Internet usage.
- Know your children's friends — online as well as in person.
- Stress Internet "stranger danger."
- Do a Google search for your children's names to make sure that their personal information and photos are not easily searchable on the Internet.

The Cyber Safety and Ethics Initiative is a partnership between Rochester Institute of Technology, more than 20 Rochester area district school, Time Warner Cable, the National Centre for Missing and Exploited Children, the Information Systems Security Association and InfraGard Member Alliance of Rochester, a program of the Federal Bureau of Investigations.
Appendix 1:
A Federal Decree-Law no. (5) of 2012

Issued on 25 Ramadan 1433 AH Corresponding to 13 August 2012 AD On Combatting Cybercrimes Abrogating:


Law no. (1) of 2004 on Combating Terrorism Crimes, and Federal Law no. (1) of 2006 on Electronic Transactions and Commerce, and Federal Law no. (2) of 2006 on Combating Cybercrimes, and Federal Law no. (51) of 2006 on Combating Human Trafficking, and Federal Law no. (6) of 2008 on the Establishment of the National Council for Tourism and Archaeology, and Federal Law no. (3) of 2009 on Fire Weapons, Ammunitions and explosives, and Federal Decree-Law no. (3) of 2012 on the Establishment of the National Electronic Security Authority, and Upon the proposal of the Minister of Justice and the approval of the Council of Ministers, have promulgated the following Decree-Law:

**Article 1**

The following terms and phrases shall have the meanings assigned opposite to each of them unless the context indicates otherwise:

<table>
<thead>
<tr>
<th>The State</th>
<th>The United Arab Emirates State.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competent Authorities</td>
<td>Federal or local authorities concerned in the electronic security affairs in the State.</td>
</tr>
<tr>
<td>The Content</td>
<td>Information, data and electronic services.</td>
</tr>
<tr>
<td>Electronic Information</td>
<td>Any information which may be stored, processed, generated and transmitted through information technology means and in specific writings, images, sound, digits, letters, symbols, signals and others.</td>
</tr>
<tr>
<td><strong>Computer Program</strong></td>
<td>A set of data, instructions and orders which are enforceable through information technology means designed for a certain task.</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Electronic Information System</strong></td>
<td>A set of computer programs and information technology means designed for processing, managing and saving electronic information and the like.</td>
</tr>
<tr>
<td><strong>Computer Network</strong></td>
<td>Two or more computer programs and information technology means linked together to enable users to access and exchange information.</td>
</tr>
<tr>
<td><strong>Electronic Document</strong></td>
<td>A computer record or data to be established, stored, extracted, copied, sent, notified or received by electronic means through a medium.</td>
</tr>
<tr>
<td><strong>Website</strong></td>
<td>A place where the electronic information is made available on the computer network, including social communication sites, personal pages and blogs.</td>
</tr>
<tr>
<td><strong>Information Technology</strong></td>
<td>Any tool, whether electronic, magnetic, optical, electrochemical or any other tool which is used to process electronic data, perform logical and arithmetic operations or storage functions, and includes any directly related to or operating in conjunction with such means which enables such means to store electronic information or communicate them to others.</td>
</tr>
<tr>
<td><strong>Government Data</strong></td>
<td>Means electronic data or information whether private or relating to the federal government or local governments of the Emirates of the State, or to federal or local public authorities or public establishments.</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Financial, Commercial, or Economical Facilities:</strong></td>
<td>Any facility which acquires its financial, commercial or economical description pursuant to the license issued by the competent authority in the State.</td>
</tr>
<tr>
<td><strong>Electronic</strong></td>
<td>Whatever is related to electromagnetic, photoelectric, digital, credit, or light technology or the like.</td>
</tr>
<tr>
<td><strong>Pornography involving Juveniles</strong></td>
<td>Any photographing, recordings, drawings or others which arouses sex organs or any actual, virtual or simulated sexual acts with a juvenile under eighteen years of age.</td>
</tr>
<tr>
<td><strong>Internet Protocol address</strong></td>
<td>A numerical label assigned to any information technology means participating in a computer network which is used for communication purposes.</td>
</tr>
<tr>
<td><strong>Confidential</strong></td>
<td>Any information or data unauthorized to be disclosed or made available to third parties unless by a prior permission from the owner of this authorization.</td>
</tr>
<tr>
<td><strong>Reception</strong></td>
<td>Viewing or obtaining data or information.</td>
</tr>
</tbody>
</table>
Offense

Every deliberate expression against any person or entity deemed by an ordinary person as insulting or afflicts the dignity or honor of that person or entity.

**Article 2**

Shall be punished by imprisonment and a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand Dirhams or either of these two penalties whoever gains access to a website, an electronic information system, computer network or information technology means without authorization or in excess of authorization or unlawfully remains therein.

The punishment shall be imprisonment for a period of at least six months and a fine not less than one hundred and fifty thousand dirhams and not in excess of seven hundred and fifty thousand dirhams or either of these two penalties if any of the acts specified in paragraph (10) of this Article has resulted in deletion, omission, destruction, disclosure, deterioration, alteration, copying, publication or re-publishing of any data or information.

The punishment shall be imprisonment for a period of at least one year and a fine not less than two hundred and fifty thousand dirhams and not in excess of one million dirhams or either of these two penalties if the data or information objects of the acts mentioned in paragraph (2) of this Article are personal.

**Article 3**

Shall be punished by imprisonment for a period of at least one year and by a fine not less than two hundred and fifty thousand dirhams and not in excess of one million dirhams or either of these two penalties.
penalties whoever commits any of the crimes specified in sections (1) and (2) of Article (2) of this Decree-Law in the course of or because of his work.

**Article 4**

Shall be punished by temporary imprisonment and a fine not less than two hundred and fifty thousand dirhams and not in excess of one million five hundred thousand dirhams whoever accesses a website, electronic information system, computer network, or information technology means without authorization whether such access is intended to obtain government data, or confidential information relating to a financial, commercial or economical facility.

The punishment shall be imprisonment for a period of at least five years and a fine not less than five hundred thousand dirhams and not in excess of two million dirhams, if these data or information were deleted, omitted, deteriorated, destructed, disclosed, altered, copied, published or re-published.

**Article 5**

Shall be punished by imprisonment and by a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand dirhams or either of these two penalties whoever gains access to a website without authorization intending to change its designs, or delete, destroy or modify it, or occupy its address.

**Article 6**

Shall be punished by temporary imprisonment and a fine not less than one hundred and fifty thousand dirhams and not in excess of seven hundred and fifty thousand dirhams whoever commits
forgery of any electronic document of the federal or local government or authorities or federal or local public establishments.

The punishment shall be both imprisonment and a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand dirhams or either of these two penalties if the forged documents belong to an authority other than those mentioned in paragraph one of this Article.

Shall be punished by the same penalty decided for the crime of forgery, as the case may be, whoever uses this forged electronic document with his knowledge that the document is forged.

**Article 7**

Shall be punished by temporary imprisonment whoever obtains, possesses, modifies, destroys or discloses without authorization the data of any electronic document or electronic information through the computer network, a website, an electronic information system or information technology means where these data or information are related to medical examinations, medical diagnosis, medical treatment or care or medical records.

**Article 8**

Shall be punished by imprisonment and a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand dirhams or either of these two penalties whoever hinders or obstructs access to the computer network or to a website or an electronic information system.
**Article 9**

Shall be punished by imprisonment and a fine not less than one hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses a fraudulent computer network protocol address by using a false address or a third-party address by any other means for the purpose of committing a crime or preventing its discovery.

**Article 10**

Shall be punished by imprisonment for a period of at least five years and a fine not less than five hundred thousand dirhams and not in excess of three million dirhams or either of these two penalties whoever willfully and without authorization runs a software on the computer network or an electronic information system or any information technology means, and caused them to stop functioning or being impaired, or resulted in crashing, deletion, omission, destruction or alteration of the program, system, website, data or information.

The punishment shall be imprisonment and a fine not in excess of five hundred thousand dirhams or either of these two penalties if the result was not reached.

The punishment shall be imprisonment and a fine or either of these two penalties for any deliberate act which intends to flood the electronic mail with messages causing it to stop functioning, inactivate it or destroy its contents.

**Article 11**

Shall be punished by imprisonment for a period of at least one year and a fine not less than two hundred and fifty thousand dirhams and not in excess of one million dirhams or either of these two
penalties whoever takes over a personal property, benefit, deed or its signature whether for oneself or for other persons and without legal right, by resorting to any fraudulent method or by adopting a false name, or false personation through the computer network, or an electronic information system or any information technology means.

**Article 12**

Shall be punished by imprisonment and a fine or either of these two penalties whoever gains access, without legal right, to credit or electronic card numbers or data or to bank accounts numbers or data or any other electronic payment method by using the computer network or an electronic information system or any information technology means.

The punishment shall be imprisonment for a period of at least six months and a fine not less than one hundred thousand dirhams and not in excess of three hundred thousand dirhams or either of these two penalties, if it is intended to use these data and numbers to take over the funds of others or to benefit from the services which they provide.

If he has reached to take over the funds of others whether for himself or for others, he shall be punished by imprisonment for a period of at least one year, and a fine not less than two hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties.

Shall be punished with the same penalty specified in the preceding paragraph, whoever publishes or re-publishes credit or electronic card numbers or data or bank accounts numbers of data which belong to others or any other electronic payment method.
Article 13

Shall be punished by imprisonment and a fine not less than five hundred thousand dirhams and not in excess of two million dirhams or either of these two penalties whoever forges, counterfeits or reproduces a credit card or debit card or any other electronic payment method by using any information technology means or computer program.

Shall be punished by the same penalty whoever:

Manufactures or designs any information technology means or computer program for the purpose of facilitating any of the acts specified in paragraph 1 of this Article.

Uses, without authorization, a credit or electronic card or debit card or any other electronic payment method aiming to obtain, whether for himself or for others, the funds or properties of others or benefit from the services provided by third parties.

Accepts to deal with these forged, counterfeited, reproduced cards or other electronic payment method with his knowledge of its illegality.

Article 14

Shall be punished by imprisonment and a fine not less than two hundred thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever obtains, without legal right, a secret number, code, password or any other means to have access to an information technology means, website, electronic information system, computer network or electronic information.
Shall be punished with the same penalty whoever prepares, designs, produces, sells, buys, imports, displays for sale or make available any computer program or any information technology means, or promotes by any means links to websites, computer program or any information technology means designed for the purposes of committing, facilitating or abetting in the commission of the crimes specified in this Decree-Law.

**Article 15**

Shall be punished by imprisonment and a fine not less than one hundred fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever, without authorization, deliberately receives or intercepts any communication through any computer network.

Whoever discloses the information which he has obtained through illegal reception or interception of communications shall be punished by imprisonment for a period of at least one year.

**Article 16**

Shall be punished by imprisonment for a period of two years at most and a fine not less than two hundred fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses a computer network or information technology means to extort or threaten another person to force him to engage in or prevent him from engaging in a certain act.

The punishment shall be imprisonment up to ten years if the subject of threat is to commit a felony or engage in matters against honor or morals.

**Article 17**
Shall be punished by imprisonment and a fine not less than two hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever establishes, manages or runs a website or transmits, sends, publishes or re-publishes through the computer network pornographic materials or gambling activities and whatever that may afflict the public morals.

Shall be punished by the same penalty whoever produces, draws up, prepares, sends or saves for exploitation, distribution, or display to others through the computer network, pornographic materials or gambling activities and whatever that may afflict the public morals.

If the subject of the pornographic content involves a juvenile under eighteen years of age, or if such content is designed to seduce juveniles, the principal shall be punished by imprisonment for a period of at least one year and a fine not less than fifty thousand dirhams and not in excess of one hundred and fifty thousand dirhams.

**Article 18**

Shall be punished by imprisonment for a period of at least six months and a fine not less than one hundred fifty thousand dirhams and not in excess of one million dirhams whoever has deliberately acquired pornographic materials involving juveniles by using an electronic information system or computer network or electronic website or any information technology means.

**Article 19**

Shall be punished by imprisonment and a fine not less than two hundred fifty thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever entices, aids or
abets another person, by using a computer network or any information technology means, to engage in prostitution or lewdness.

The punishment shall be imprisonment for a period of at least five years and a fine not in excess of one million dirhams if the victim is a juvenile under the age of eighteen years of age.

**Article 20**

Without prejudice to the crime of slander determined by the Islamic Sharia, shall be punished by imprisonment and a fine not less than two hundred fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever insults or accuses another person of a matter of which he shall be subject to punishment or being held in contempt by others, by using a computer network or an information technology means.

If a slander or insult is committed against a public official or servant in the course of or because of his work, this shall be considered an aggravating factor of the crime.

**Article 21**

Shall be punished by imprisonment of a period of at least six months and a fine not less than one hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses a computer network or and electronic information system or any information technology means for the invasion of privacy of another person in other than the cases allowed by the law and by any of the following ways:

Eavesdropping, interception, recording, transferring, transmitting or disclosure of conversations or communications, or audio or visual materials.
Photographing others or creating, transferring, disclosing, copying or saving electronic photos.

Publishing news, electronic photos or photographs, scenes, comments, statements or information even if true and correct.

Shall also be punished by imprisonment for a period of at least one year and a fine not less than two hundred and fifty thousand dirhams and not in excess of five hundred thousand dirhams or either of these two penalties whoever uses an electronic information system or any information technology means for amending or processing a record, photo or scene for the purpose of defamation of or offending another person or for attacking or invading his privacy.

**Article 22**

Shall be punished by imprisonment for a period of at least six months and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever uses, without authorization, any computer network, website or information technology means to disclose confidential information which he has obtained in the course of or because of his work.

**Article 23**

Shall be punished by temporary imprisonment and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever establishes, administer or runs a website or publishes information on a computer network or any
information technology means for the purpose of trafficking in humans or human organs or dealing in them illegally.

**Article 24**

Shall be punished by temporary imprisonment and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams whoever establishes or administer or runs a website or publishes on a computer network or any information technology means which would promote or praise any programs or ideas which would prompt riot, hatred, racism, sectarianism, or damage the national unity or social peace or prejudice the public order and public morals.

**Article 25**

Shall be punished by imprisonment for a period of at least one year and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever establishes, manages or runs a website or publishes information on a computer network or any information technology means for the purpose of trading or promoting fire weapons, ammunitions or explosives in instances other than those permitted by the law.

**Article 26**

Shall be punished by imprisonment for a period of at least five years and a fine not less than one million dirhams and not in excess of two million dirhams whoever establishes, manages or runs a website or publishes information on the computer network or information technology means for the interest of a terrorist group or any unauthorized group, association, organization, or body with the intent to facilitate communication with their leaders or members or attract new members, or to promote or praise their ideas, finance their activities or provide actual assistance thereof or for the
purpose of publishing methods for manufacturing incendiary devices or explosives or any other
devices used in terrorism acts.

**Article 27**

Shall be punished by imprisonment and a fine not less than two hundred thousand dirhams and not
in excess of five hundred thousand dirhams or either of these two penalties whoever establishes,
manages or runs a website or publishes information on the computer network or any information
technology means to call or promote for the collection of donations without a license accredited
by the competent authority.

**Article 28**

Shall be punished by temporary imprisonment and a fine not in excess of one million dirhams
whoever establishes, manages or runs a website or uses information on the computer network or
information technology means with intent to incite acts or publishes or transmits information, news
or cartoon drawings or any other pictures which may endanger the national security and the higher
interests of the State or afflicts its public order.

**Article 29**

Shall be punished by temporary imprisonment and a fine not in excess of one million dirhams
whoever publishes information, news, statements or rumor’s on a website or any computer network
or information technology means with intent to make sarcasm or damage the reputation, prestige
or stature of the State or any of its institutions or its president, vice-president, any of the rulers of
the Emirates, their crown princes, or the deputy rulers of the Emirates, the State flag, the national
peace, its logo, national anthem or any of its symbols.
**Article 30**

Shall be punished by life imprisonment whoever establishes, manages or runs a website, or publishes information on the Computer network or information technology means aiming or calling to overthrow, change the ruling system of the State, or seize it or to disrupt the provisions of the constitution or the laws applicable in the country or to oppose the basic principles which constitutes the foundations of the ruling system of the state.

Shall be punished by the same penalty whoever promotes to, incites or facilitates to others the commission of any of the aforementioned acts.

**Article 31**

Shall be punished by imprisonment and a fine not less than two hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever calls or incites to disobeying the laws and regulation in force in the State through publishing information on the Computer network or information technology means.

**Article 32**

Shall be punished by imprisonment and a fine not less than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever establishes, manages or runs a website or uses the Computer network or any information technology means for planning, organizing, promoting or calling for demonstrations or protests or the like without license from the competent authority.

**Article 33**
Shall be punished by imprisonment and a fine not than five hundred thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever establishes, manages or runs a website or uses the Computer network or information technology means for trafficking in antiquities or archaeological artefacts’ in instances other than those permitted by the law.

**Article 34**

Shall be punished by imprisonment of at least of one year and a fine not less than two hundred fifty thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever uses communication services, audio or video broadcasting channels without legal right or facilitates such use by others over the Computer network or information technology means.

**Article 35**

Without prejudice to the provisions of the Islamic Sharia, shall be punished by imprisonment and a fine not less than two hundred fifty thousand dirhams and not in excess of one million dirhams or either of these two penalties whoever commits through the computer network or any information technology means or a website any of the following crimes:

- Insult to any of the Islamic sanctities or rituals.
- Insult to any of the sanctities or rituals of other religions where these sanctities and rituals are inviolable pursuant to the provisions of Islamic Sharia.
- Insult to any of the recognized celestial religions.
- Condoning, provoking or promoting sin.
- If the crime contains any insult to the Divinity (Allah, God) or to the messengers and prophets or be against the religion of Islam or injures its basis and principles which constitute its foundation,
or whoever oppose or injures the well-known teachings and rituals of Islamic religion or prejudices
the religion of Islam or preaching another religion or calls for, praises or promotes a doctrine or a
notion which involves any of the aforementioned shall be punished by imprisonment up to seven
years.

**Article 36**

Shall be punished by temporary imprisonment and a fine not less than five hundred thousand
dirhams and not in excess of one million dirhams or either of these two penalties whoever
establishes, manages or runs a website or publishes information on the computer network or any
information technology means for trafficking in or promoting narcotics or psychotropic substances
and the like or the manner for their use or facilitates such dealing in instances other than those
permitted by the law.

**Article 37**

Without prejudice to the provisions specified in the Money Laundering Law, shall be punished by
imprisonment up to seven years and by a fine not less than five hundred thousand dirhams and not
in excess of two million dirhams whoever deliberately commits, by using a computer network, an
electronic information system or any information technology means, any of the acts mentioned
hereinafter:

Illegal transfer, transport or deposit of funds with intent to conceal or disguise the source of funds.

Concealing or disguising the nature of the illicit funds, or its origin, movement, related rights or
ownership.
Illegal attainment, possession or use of funds with the knowledge of its illegal origin.

Shall be punished by the same punishment whoever establishes, manages or runs a website or publishes information on a computer network or information technology means to facilitate or incites the commission of any of the acts specified in paragraph 1 of this Article.

**Article 38**

Shall be punished by temporary imprisonment whoever provides any organizations, institutions, authorities or any other entities through the computer network or any information technology means any incorrect, inaccurate or misleading information which may damage the interests of the State or injures its reputation, prestige or stature.

**Article 39**

Shall be punished by imprisonment and a fine or any of these two penalties any owner or operator of a website or computer network who deliberately and knowingly saves or makes available any illicit content or if he fails to remove or blocks access to this illicit content within the period determined in the written notice addressed by the competent authorities indicating the illegal content and being available on the website or the computer network.

**Article 40**

Attempted misdemeanor’s specified in this Decree-Law shall be punished with half the penalty specified for the complete crime.

**Article 41**
Without prejudice to the right of bona fide third-party, shall be ordered, in all instances, the confiscation of devices, programs or means used in the commission of any of the crimes specified in this Decree-Law or the money accrued thereof, or deletion of the information and statements or their killing, as to the closure of the domain or site in which any of these crimes is committed whether permanent closure or for a specified period as determined by court.

**Article 42**

The court may decide deportation of a foreigner who is condemned in any of the crimes specified in this Decree Law upon execution of the punishment adjudged.

**Article 43**

Without prejudice to the provisions of the penalties specified in this Decree-Law, the court may order to put the condemned under surveillance or control or orders his deprivation from the right to use any computer network or electronic information system or any other information technology means or place him in a rehabilitation center for a period which the court may deem appropriate.

**Article 44**

The crimes mentioned in Articles (4, 24, 26, 28, 29, 30 and 38) of this Decree-Law shall be considered as crimes against the State security.

Shall also be deemed as crimes against State security any crime specified in this Decree-Law if committed to the account or benefit of a foreign country or any terrorist group or illegal group, association, organization or body.
Article 45

Mitigation of or exemption from punishment may be ordered by the court, at the request of the public prosecutor, regarding criminals who have provided the judicial or administrative authorities with information in respect of any of the crimes relating to the State security pursuant to the provisions of this Decree-Law, where such a matter has resulted in the discovery of the crime, or proving the case against them or arresting any of them.

Article 46

The use of the computer network, the Internet, any electronic information system, a website or any information technology means shall be considered an aggravating factor when committing any crime not specified by the present Decree-Law.

Shall also be considered as an aggravating factor the commission of a crime specified in this Decree-Law to the account or benefit of a foreign country or any terrorist group, or illegal group, association, organization or body.

Article 47

Without prejudice to the provisions of chapter two of part two of book one of the Penal Code, the provisions of this Decree-Law shall apply to any person who has committed any of the crimes mentioned therein outside the country, if its object is an electronic information system, computer network, website or information technology means relates to the federal government or any of the local governments of the Emirates of the State or any authority or public institution owned by any of them.
Article 48

The application of the penalties specified in this Decree-Law shall not prejudice any other greater penalty specified by the Penal Code or any other law.

Article 49

The officials determined by a decision from the Minister of Justice shall have the capacity of judicial officers for the ascertainment of acts committed in violation to the provisions of this Decree-Law, and the competent authorities in the Emirates are required to submit facilities necessary to those officials to enable them to perform their tasks.

Article 50

Federal Law no. (2) of 2006 on Combatting Cybercrimes shall be abrogated, and shall also be abrogated any provision contrary to or contradicting with the provisions of this Decree-Law.

Article 51

This Decree-Law shall be published in the official gazette and be put into effect on the next day of publication. Issued by Us, at the Presidential Palace in Abu Dhabi

On 25 Ramadan 1433 AH Corresponding to 13/08/2012 AD

Khalifa Bin Zayed Al Nahyan, President of the United Arab Emirates State the Present Federal Decree-Law was published in the Official Gazette, issue no. 540 (Addendum), p. 19.
REFERENCES:

- “Netgear” research Article
- “GulfNews.com”
- Check Point “Security Report”
- The Security Review
- The Cyber Security and Ethics Initiatives
- ITP. net IT Service Providers global
- Cybercrime out of obscurity and into reality:pwc global economic crime survey
- Computer News / Middle East www.comeonline.com
- “Look Out”
- UAE official gazette vol.:442
- Information Security - Best Practices to protect Data - Titus.com
- UBM. Tech Web White Paper
- RSA Cybercrime Trends Report
- Digital Persona white paper
- Security Middle East
- Checkpoint 3D Security Report
- Wolfpack information risk the South African Cyber Threat Baro Meter
• https://www.bloomberg.com/news/articles/2016-12-12/hack-of-saudi-arabia-exposes-middle-
east-cyber-security-flaws

• http://www.hindustantimes.com/india-news/3-indians-hackers-held-for-steal-dh-1-million-
from-dubai-businessman-s-account/story-tyonqw2yR4w7cCDUPyYb2H.html

• http://www.reuters.com/article/idUSLJ48901120080819
• http://www.slideshare.net/poonambhasin33/need-and-importance-of-cyber-law
• http://gulfnews.com/uaessentials/residents-guide/legal/uae-crimes-law-1.442016
• www.tra.gov.ae/legal_references.php
• https://www.strategyand.pwc.com/media/file/Cyber-security-in-the-Middle-East.pdf
• https://www.comptia.org/resources/international-trends-in-cybersecurity---uae
• http://www.gcsp.ch/download/6791/159595
• https://www.f-secure.com/en/web/labs_global/botnets
• www.opsi.gov.uk
• http://www.theregister.co.uk/2009/03/19/sumitomo_cyberheist_investigation/
• http://www.terramedia.co.uk/reference/law/UK_media_law/
  broadcasting_laws.htm
• http://www.datalossbarometer.com/docs/
• www.uaecert.gov.ae
• http://www.itp.net
• Http://www.sarbanes-oxley Act pertains to security - compliance audit report for SARBOX, PCI, HIPPA
  & GLB
• Http://www.gramm-Leach-Bliley Act pertaining to cyber security regulation compliance Demystified.
• Khaleej Times, April 8, 2011
• http://www.khaleejtimes.com/nation/general/uae-major-target-for-cyber-criminals
• http://www.khaleejtimes.com/nation/general/uae-major-target-for-cyber-criminals
• http://www.gadgetsnow.com/it-services/Cyber-war-talks-invade-CeBIT/articleshow/7620647.cms
• http://www.zawya.com/Story.cfm/sidZAWYA20100118085552/UAEToEstablishSpecialistCybercrimeCourts/
• http://www.crime-research.org/analytics/702/
• http://www.cybercrimejournal.com/ibrahimmarcusdec2009.htm
• https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/reports.pdf
• http://www.cybercrimejournal.com/ibrahimmarcusdec2009.htm
• http://www.zawya.com/Story.cfm/sidZAWYA20100118085552/UAEToEstablishSpecialistCybercrimeCourts/
• http://www.zawya.com/Story.cfm/sidZAWYA20100118085552/UAEToEstablishSpecialistCybercrimeCourts/
• http://www.hodgsonruss.com/media/publication/70_AA%20Security%202014.pdf
• https://books.google.ae/books?id=2jp0BgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
• https://books.google.ae/books?id=2jp0BgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
• https://books.google.ae/books?id=2jp0BgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
• https://books.google.ae/books?id=_gQEAAAAMBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false
• http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7249&context=jclc
• http://www.sei.cmu.edu/reports/12tr007.pdf
• http://www3.weforum.org/docs/GITR/2013/GITR_Chapter1.5_2013.pdf
• https://www.newscientist.com/article/dn7158-spies-infiltrate-zombie-computer-networks/
• http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers
• Townson P 2006 Call for legal steps to fight cybercrimes www.gulf-times.com [accessed on 3 March 2009]
• http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=4844&context=fss_papers
• http://www.cybercrimejournal.com/Leukfeldtetal2013janijcc.pdf
• https://books.google.ae/books?hl=en&lr=&id=aFJqtsfQhSkC&oi=fnd&pg=PR3&dq=Cybercrimes:+A+Multidisciplinary+Analysis&ots=CsVW70Pt7W&sig=cT5pHo2OXRmA7DVzOv1NTQgw5DI&redir_esc=y#v=onepage&q=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&f=false
• http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7456&context=jclc
• https://books.google.ae/books?hl=en&lr=&id=aFJqtsfQhSkC&oi=fnd&pg=PR3&dq=Cybercrimes:+A+Multidisciplinary+Analysis&ots=CsVW70Pt7W&sig=cT5pHo2OXRmA7DVzOv1NTQgw5DI&redir_esc=y#v=onepage&q=Cybercrimes%3A%20A%20Multidisciplinary%20Analysis&f=false
• Brown, I., 2010. Communications Data Retention in an Evolving Internet. International Journal of Law and Information Technology,
• http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1206&context=chtlj
• http://nials-nigeria.org/pub/lauraani.pdf
• Cybercrime Law in Ireland.