On Cyber Crimes and Cyber Security

Chapter · January 2019

DOI: 10.4018/978-1-5225-8304-2.ch001

3 authors, including:

Mariam M. H. Alansari
Kuwait University
1 PUBLICATION **2** CITATIONS

SEE PROFILE

Muhammad Sarfraz
Kuwait University
320 PUBLICATIONS **3,508** CITATIONS

SEE PROFILE

The paper should be cited as:

Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber Security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.

On Cyber Crimes and Cyber Security

Mariam M. H. Alansari, Zainab Aljazzaf, Muhammad Sarfraz

Department of Information Science
College of Computing Sciences and Engineering
P.O. Box 5969, Safat 13060, Kuwait University, Kuwait

Abstract

The world has become more advanced in communication, especially after the invention of the Internet. A key issue facing today's society is the increase in cybercrime or e-crimes (electronic crimes), another term for cybercrime. Thus, e-crimes pose threats to nations, organizations and individuals across the globe. It has become widespread in many parts of the world and millions of people are victims of e-crimes. Given the serious nature of e-crimes, its global nature and implications, it is clear that there is a crucial need for a common understanding of such criminal activity internationally to deal with it effectively. This research covers the definitions, types, and intrusions of e-crimes. It has also focused on the laws against e-crimes in different countries. Cybersecurity and searching methods to get secured are also part of the study.

Keywords: Cybercrime, e-crime, cyber security, computers, internet, social media, cyber laws

1. Introduction

The Internet is the global system of interconnected computer networks that use the internet protocol suite to link billions of devices worldwide. Today, the Internet is one of the most important parts in daily life. The information technology revolution has brought two main functions with internet. On one hand it has contributed positive values to the world. While, on the other hand, it has produced many problems that threaten the order of the society and also produce a new wave of crime in the world.

The internet is used for different purposes depending on user requirements such as communication, research, education, financial transactions, threading, etc. The internet has become an environment, where the most lucrative and safest crimes are conducted. This research focuses on cybercrime or e-crimes (electronic crimes), another term for cybercrime. It refers to criminal activity that involves the internet, a computer or other electronic devices (Alex Roney Mathew, Aayad Al Hajj, and Khalil Al Ruqeishi, 2010).

E-crimes are increasing in frequency and causing extensive damage to governments, companies, society, and individual (Broadhurst R. & Grabosky P., 2005). Moreover, cyber criminals are motivated in various ways, including (but not limited to) financial gains, emotional instability, societal norms, and lack of legislation and punishment.

There are different names of e-crimes such as: the high-tech crimes, white collar crimes, and cybercrimes (Majid, 2012). Every year there is an increase of e-crimes due to the development of information technology and software changes (Rekouche, 2011). Thus, e-crimes have become very common and spread via various methods including malicious programs, which specially prepared to break through personal computers (PCs) or enterprise systems for copying confidential information or destroying systems. The most famous of these methods are Hacking, Phishing, Spamming, Cyber stalking, Cyber defamation, Cyber terrorism, and Malware (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009) (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013).

Consequently, the first step to secure the information and deny access to anyone is security programs. So many people and organizations have security programs to protect their software from the hackers (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009). Besides, many countries trying to enforce e-crime laws pose danger to the society and the individuals. This is because of the spread and development of information technology and the ease acquisition of electronic appliances.

The purpose of this study is to have an overall survey concerning cybercrimes, social media, cyberlaws and cyber security. It will also look at the e-crimes factors and the influence of factors that make e-crimes spreading in society. Specifically, it examines the following points:

- Researching and reviewing the most common types of e-crimes.
- Study the existing literatures on the factors influencing e-crime.
- Finding out the concerns of the society in using the Internet.
- Identify the factors influencing e-crime in the Society. Especially, influence of demography and technology over different types of e-crimes.
- Measurement and analysis of perceptions, experiences, and attitudes toward e-crimes.
- Determining the relationship between social media and e-crimes.
- Recommend the measures to reduce the e-crime by the policy makers and awareness programs so that cyber security is made certain.

The rest of the chapter is organized as follows. Section 2 presents the detailed study on cybercrimes. Section 3 highlights some of the common e-crime methods. Section 4 elaborates the factors of committing e-crimes. Cybercrimes in various countries are explored in Section 5. Section 6 discusses social media, cybercrimes and cyber laws. A survey of influencing factors towards e-crimes is given in Section 7. The issue of cyber security is considered in Section 8 whereas Section 9 concludes the chapter.

2. Cyber Crimes

As mentioned in Section 1, the purpose of this chapter is to determine e-crimes factors and examine the influence of the factors that make e-crimes spreading in society. Specifically, it examines the following: researching and reviewing the most common types of e-crimes, study the existing literatures on the factors influencing e-crime, finding out the concerns of the Kuwait society in using the Internet, identify the factors influencing e-crime in Kuwait Society. Especially, Influence of demography and technology over different types of e-crimes, determining the measurement and analysis of perceptions, experiences, and attitudes toward e- crimes, determining the relationship between social media and e-crimes, finally, recommend the measures to reduce the e-crime by the policy makers and awareness programs.

For the purposes of this research, this chapter is arranged in the following manner: the impact of e-crimes, classifications of e-crimes, then review the beginning and the growth of e-crimes. Methods of e-crimes will then be reviewed, which will be followed by factors of e-crimes, protection and preservation of data, e-crimes in various countries, e-crimes in Kuwait. Finally, related work.

2.1 What is Cybercrime or e-crime?

Cybercrime or e-crimes are offenses that are committed against individuals or groups with a criminal motive of intentionally harming the reputation of the victim, causing physical or mental harm, and cause loss of money or information directly or indirectly by using the Internet and electronic devices (Johnson, 2013), (Broadhurst R. & Grabosky P., 2005), (Alex Roney Mathew, Aayad Al Hajj, and Khalil Al Ruqeishi, 2010).

2.1.1 Impact of e-crimes

E-crimes affect the community in many ways. This includes (Amber Stabek, Paul Watters, and Robert Layton , 2010) (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013) (Balkhi, 2013) (Brokenshire, 2013):

- Loss of online business and consumer confidence in the digital economy,
- The potential for critical infrastructure to be compromised affecting water supply, health services, national communications, energy distribution, financial services, and transport,
- Loss of personal financial resources and the subsequent emotional damage.
- Loss of business assets,
- Costs to government agencies and businesses in re-establishing credit histories, accounts and identities,
- Costs to businesses in improving cyber security measures,
- Stimulating other criminal activity, or
- Costs in time and resources for law enforcement agencies.

2.1.2 Classifications of e-crimes

- **Computer crime**: Using of direct electronic operation that can attack security to obtain data and information illegally (Kumar, 2009).
- **High-tech crime**: A broad range of criminal activities that penetrate computers, illegally in violation of country laws, or federal laws. These crimes are done by hacking, money laundering, malware, harassment, electronic, and identity theft (Broadhurst R. & Grabosky P., 2005).
- **White-collar crime**: A crime committed by a person of respectability and high social status in the course of his occupation to obtain money. The famous persons who were convicted of white-collar are Kenneth Lay, Bernard Madoff, and Bernard Embers. (Majid, 2012) (Rubino, 2014).
- **Cybercrime**: It is a criminal activity that is done by using computers and the internet including anything from illegal downloading of music files and games to stealing millions of dollars from online accounts (Gorazd Mesko, and Igor Bernik, 2011). Also non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on internet through music

and game files. (Schaeff B, Chan H., and Ogulnick S., 2009).

- **Cyber terrorism**: Premeditated and politically motivated attack against information, computer systems, computer programs, and data, which results in violence against civilian targets (Brokenshire, 2013). Possible cyber terrorism targets include the banking industry, military installations, power plants, air traffic control centers (Dogrul M.,Aslan A.&Celik E., 2011).

2.2 Beginning and growth of e-crimes

This section indicates several general trends, since 1960s, about how e-crimes began and grew. The summary is as follows:

- In the early decades of modern information technology (IT), computer crimes were largely committed by unsatisfied individuals and dishonest employees.
- Physical damage to computer systems was a prominent threat until the 1980s (Sterling, 1992).
- Criminals often used authorized access to subvert security systems as they modified data for financial gain or destroyed data for revenge (Louw C. , Von Solms S. , 2014).
- Early attacks on telecommunications systems in the 1960s led to sabotage of the long distance phone systems for amusement and for theft of services (Kabay, 2008).
- As telecommunications technology spread throughout the IT world, people with criminal tendencies learned to penetrate systems and networks for amusement (Kenefick, 2008).
- Programmers in the 1980s began writing malicious software, including self-replicating programs, to interfere with personal computers (Kabay, 2008).
- As the Internet increased access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for sabotage, political action and financial gain (Erbschloe, 2004).
- As the 1990s progressed, financial crime using penetration and destabilization of computer systems increased (Sterling, 1992).
- The types of malware shifted during the 1990s, taking advantage of new vulnerabilities as operating systems were strengthened, only to give way to new attack routes (Kenefick, 2008).
- Illegal applications of e-mail grew rapidly from the mid-1990s onward, generating plenty of unwanted commercial and fraudulent emails (Hussainat M. , 2013).
- Social networking has become an increasingly important tool for cyber criminals to recruit people to assist their money laundering operations around the globe (Erbschloe, 2004).
- Global mobile devices' penetration—from smart phones to tablet PCs—accessing the Internet by 2013 surpassed 1 billion, creating more opportunities for cybercrime (Rubino, 2014).

2.2.1 Specific e-crimes

The real beginning of e-crime started in 1960, when there were attacks in the United States on the telecommunication systems, it led to destroying long distance phone communications (Kabay, 2008). In 1971, wire fraud by communication was escalated in the United States when the rogue program called Creeper, which spread through early bulletin board networks. In the same year, a person called Draper built a blue box that allowed making long distance free

calls (Sterling, 1992).

Email spam was discovered in 1976, when it was sent out over the Advanced Research Projects Agency Network (ARPANET) (Sterling, 1992). ARPANET kernel led to the advent of modern Internet (Ping, 2011). The first criminal convicted on e- crimes was Ian Murphy in 1981. Murphy penetrated and altered the billing clock in American Telephone & Telegraphs (AT&T's) and people could get discounted rates during normal hours of business. In the early decades of the modern information technology the first virus on an Apple computer was detected in 1982 (Louw C. , Von Solms S. , 2014).

In 1986, the oldest virus called 'Pakistani Brain' was created by unauthorized circumstances, which attacked the computers of International Business Machines (IBM) Corporation (Kenefick, 2008). And then, in 1988, Kevin Mitnick was sentenced for spying on e-mails for Microwave Communications Inc. (MCI) and Digital Equipment Corporation (DEC) (Kabay, 2008).

At the same year, the first worm of ARPANET surfaced on the government systems and got out control, which caused the closure of universities and government systems as it spread over 6000 networked computers. This was done by a graduate student at Cornell University called Robert T. Morris, who was dismissed from Cornell University and sentenced to three years' probation with $10K fine (Sterling, 1992). After that, criminal activities began to make malicious software including self-replicating programs to interfere with personal computers (Kabay, 2008).

With the increasing of internet use, criminals started using malicious programs to get their goals. By mid-1990, e-crimes had gone too advanced and used software systems to computer breakthroughs and frauds spread by email (Hussainat M. , 2013). As that in 1992, the first virus called 'Dark Avenger', was released (Sterling, 1992). In the late Nineties, the famous malware named 'Melissa' appeared. As well as the other famous virus 'Chen Ing-Hau' (CIH) was sent to the internet users around the world (Kenefick, 2008).

At the beginning of the millennium, the technological developments of e-crimes increased significantly. In 2000, Denial of Service (DOS) was sent to corrupt websites such as Yahoo, eBay, CNN, Amazon, Buy, etc. The famous virus in that period 'I LOVE YOU', was spread by forwarding itself and sent to all contacts on the mail lists from their accounts (Erbschloe, 2004).

The most famous e-crimes took place in 2001, when Microsoft was attacked and corrupted from a new Domain Name Server (DNS), which blocked Microsoft's Web sites for two days (Erbschloe, 2004). In addition, more new worms were discovered in the millennium. These include The L10n worm, Code Red, Sadmind, Nimda memory-only, the Klez. H, Multiple variants of the MyDoom worm, and Storm Worm (Erbschloe, 2004).

One of the most dangerous cyber-attacks is the Structured Query Language (SQL) - injection attack, launched through the web browsers, that leaves a lot of doors widely open for the attackers to exploit these and gaining access to confidential Information that resides in the website server databases. In 2008, attackers used SQL injection techniques to create malicious iFrame blocks on legitimate Web sites (Totarotech, 2013).

In recent years, countries had begun to absorb the gravity of e-crimes to society and the

individuals because of electronic-attacks, as experienced by hackers in 2010. According to Spanish investigators, there were over 13 million infected computers around the world, including PCs, affecting thousands of organizations, and above forty major banks (Tabuchi, 2011).

The important historical event of e-crimes was exposed by associated press in 2013 about theft on Twitter account. The criminal wrote tweets about attacks in the White House that left President Obama injured. This tweet had led to a drop in Dow Jones by 130 points and withdrawal of 136 billion dollars from stock markets in the United States of America (Rubino, 2014).

3. Methods of e-crimes

The routine uses of the internet such as downloading songs, games, and free music from insecure sites as well as opening an unknown sender`s message lead to the possibility of a threat via the internet (Fawn T. & Paternoster R., 2011)**.** Cybercrimes are escalating by various methods such as: malicious programs, which facilitated in penetrating devices (Dixon, 2005). These programs are progressing year after year with highest techniques that can help hackers to be hidden (Oweis N., Owais S., Alrababa M., Alansari M., 2014). This section explains methods of e-crimes by using some of famous malicious programs such as: Hacking, Phishing, Spam, Cyber stalking, Cyber terrorism, Cyber defamation, and Malware as follows (WD Kearney & HA Kruger, 2014).

3.1 Hacking

Hacking developed by a highly skills programmer (Hacker) that enters a computer system and network in an illegal way (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013). Hackers have easy targets and objectives, by hacking over websites' security to take and manage the theft data, such as edit, delete, install any file in any user's directory (Erbschloe, 2004). However, there are experts in machine code and operating systems and well-known in latest bugs, latest patches, latest bugs in the patches, etc. (Oweis N., Owais S., Alrababa M., Alansari M., 2014). Finally, hackers are able to increasingly rely upon the community to identify bugs and create programs that can adapt for their specific purpose (Rekouche, 2011). Table 1 shows highest targets of e-crimes by hacking (Saini Das, Arunabha Mukhopadhyay, and Girja.K. Shukla, 2013) (Balkhi, 2013) (Barnes B. and Perlroth N., 2014).

Table 1: Highest targets of e-crimes by hacking from 2011 to 2014**.**

Date	**Target**	**Type of attack**	**Loss**
2011	Citigroup	Hacking the system of the company	2.7 million Dollar
			Theft over 200,000 customer sensitive information
2011	Citi Bank	Individual hackers	Over 2.7 million Dollar
			Customer data loss
2012		Hacking website	Website downtime

	USDJ[1], FBI[2], RIAA[3],	Defacement	Loss of reputation
2014	Sony	Attacked by hackers called Guardians of Peace	Caused companywide shutdown of computers
			Leak of corporate information such as: salaries and bonus of executives and the security numbers of employees

3.2 Phishing

Phishing is defined as a way to get sensitive information illegally such as passwords, user name, credit card details, and electronic signature through online networks, websites, and online payment (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013). Another definition of phishing "is a method of stealing personal data whereby an authentic-looking e-mail is made to appear as if it is coming from a real company or institution, the idea is to trick the recipient into sending secret information such as account information or login data to the scammer" (Schaeff B, Chan H., and Ogulnick S., 2009). The process of phishing is through the illusion users to enter personal data, which is almost identical to the legitimate site with makes recorded use of phishing described in detail was in 1987 and the first used in phishing meaning was in 1996 (Rekouche, 2011).

Phishing scams are increasing day after day under the evolution of technology; the United States faced the problem of phishing in 1995, when passwords were stolen from a large number of people online through the use of software piracy (Johnson, 2013).

3.3 Spam

Spam is the irrelevant or unwanted e-mails/messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc. (Erbschloe, 2004).

The most common form recognized on a large scale is the spam e-mail. This term is applied to similar abuses in other media like: instant messaging spam, Usenet newsgroup spam, web search engine spam, spam in blogs, wiki spam, online classified ads, spam, mobile phone messaging spam, internet forum spam, and social networking spam (Rekouche, 2011). Furthermore, the size of a spam email has become very high, because many spammers enter process easily, even after preventing senders to sending spam through emails. The amount cost of spam in 2011 about seven trillion dollars paid by the client and Internet service providers (Louw C. , Von Solms S. , 2014).

Countries have different views on how to deal with spam. For example, in South Africa, Electronic Communications and Transactions Act stipulates that any person who sends unsolicited commercial communications named spam to consumers is required to provide the consumer option of stopping their subscription from the mailing list (Sterling, 1992).

1 United States Department of Justice

2 Federal Bureau of Investigation

[3] Recording Industry Association of America
[4] Motion Picture Association of America
[5] International Federation of the Phonographic Industry

In December 2014, the Symantec's Brightmail operations carried out by monitors to categorize spam, which are coming into the network. Figure 1 shows the latest seven types of spam trends (Symantec Enterprise, 2014).

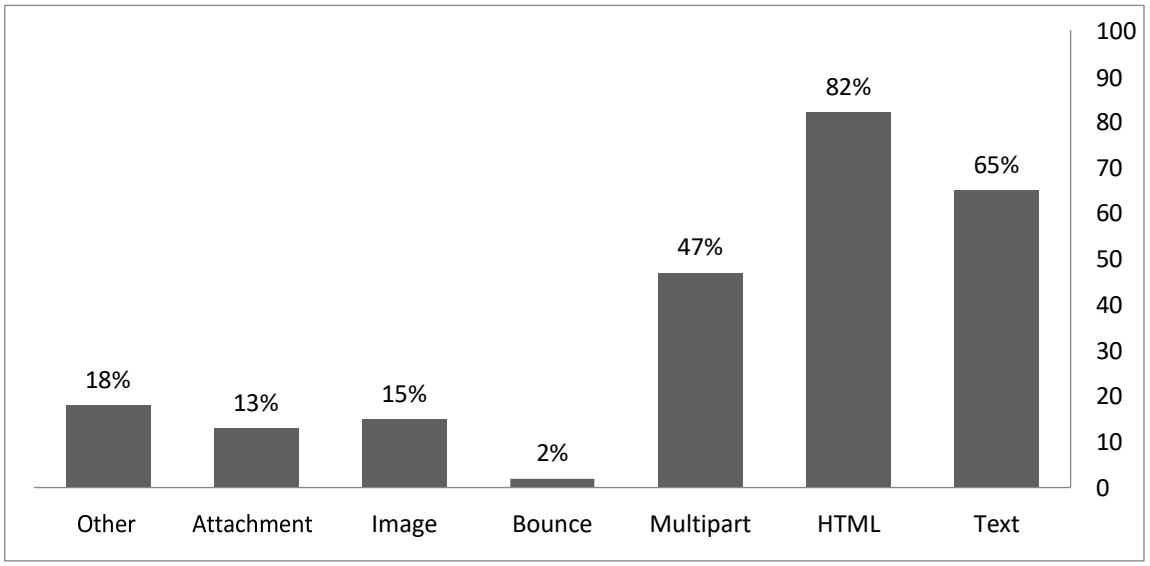

Figure 1: Latest seven types of spam trends in 2014.

3.4 Cyber Stalking

Cyber stalking is defined as using the internet or other electronic means with a view to harass or threaten any individual, group of individuals, or an organization. It includes monitoring, false accusations, identity theft, making threats, damage to data or equipment, the request of minors for sex, or gathering information that may be used to threaten or harass (Bhatt S. & Pant D., 2011).

Table 2: Three ways of cyber stalking.

Cyber stalking categories	
Email Stalking	Send e-mails to user for harassment and extortion. In some cases send viruses to intimidate the user.
Internet Stalking	Takes on public through internet such as a chat room, social network, and Web sites by sending personal data, pictures, and video to several locations to meet their demand, which is often physical.
Computer Stalking	Computer-to-computer connection, the activities of stalker is working through the Internet and the Windows operating system in order to assume control over the computer of the targeted victim. The defensive option for the victim is to get disconnected and reassign their current address of internet.

Lambert Royakkers (Royakkers, 2000) defined stalking crime as follows: "Any person is guilty of the stalking crime who: willfully, maliciously, trace another person with the intent of placing that person in reasonable fear of death, sexual assault, or great bodily injury to that person, any member of that person's family, or anyone with whom that person has a sexual or intimate relationship".

Moreover, cyber stalking has three ways dependent upon the particular use of the Internet, which are email stalking, internet stalking, and computer stalking as shown in Table 2 (Ogilvie, 2000).

3.5 Cyber defamation

Cyber defamation is a crime taking place in cyberspace through the internet to libel and damage the reputation of the victim (Berg, 2013). Defamation can be categorized as libel and slander. Table 3 shows categories of cyber defamation (Linda L. Edwards, J. Stanley Edwards, Patricia Kirtley Wells, 2008). Frequently, it occurs during the elections or while taking senior positions in the country. Also, some persons defame others through publication across online networks (Bhatt S. & Pant D., 2011).

With the advancement of internet technology, people have a large area to search and transfer the information. It also allows people to express their opinions where anyone can leave comments that can be libel, whether intentionally or unintentionally (Berg, 2013).

People comment on the internet by using the following:

- Public comments on media like newspapers, magazines, and web sites.
- Comments on social media such as Blogs, Twitter, Facebook, Instagram, and Chat Room (Berg, 2013).

Table 3: Cyber defamation categories.

Cyber defamation categories	
Libel	Words or pictures that are written, printed, and copied in internet
Slander	Spoken words or sounds, sign language, and gesticulations

3.6 Cyber terrorism

Cyber terrorism is defined as the act of Internet terrorism in terrorist activities online. It includes deliberate disruption of computer networks connected to the internet, by the means of tools such as viruses and malware to security sites, official sites, or commercial sites (Neff, 1994). Terrorism in cyberspace can be as follows:

- Physical destruction of machinery and IT infrastructure.
- Penetration of computer networks.
- Disruption of government networks.
- Disruption of financial networks or social media networks.

Therefore, cyber terrorism has been used by terrorist groups to get their goals. It carries out attacks against the computer systems, communications, infrastructure, and to launch electronic threats (Brokenshire, 2013).

3.7 Malware

Malware is the name of the programs that are permitted in a way that they are hidden under the useful programs. The term of malware generally covers viruses, worms and Trojans (Schaeff B, Chan H., and Ogulnick S., 2009) (Erbschloe, 2004).

The viruses are programs having the ability to self-replicate and attach themselves to other executable programs. Viruses spread on the infected computer and it is difficult to remove them, which leads to data loss (Schaeff B, Chan H., and Ogulnick S., 2009). Table 4 shows the different forms of viruses (Swain, 2009).

Table 4: Virus categories**.**

Virus categories	
Resident Virus	A virus that is implanted in the memory on a target system. It becomes active whenever the system starts to operate. It implements specific action on the work every time.
Non-resident Virus	A virus that transmits infection on network location, removable, and local systems. It does not remain in the system for a long time.
Boot sector Virus	A virus that targets a boot sector on the hard drive. It is being loaded into memory each time when an attempt is being made to boot from the infected drive.
Macro Virus	A virus that has written especially in macro language in Word, Outlook, Excel, Etc. It is being executed as soon as the documents are contained and automatically open.

The worm is one of the programs that distribute full function or parts of them to computers (Erbschloe, 2004). Worms are famous in reproduction and publishing, it is often used for the transfer of viruses from computers to break through barriers (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009). Table 5 shows worms categorize (Sebastian, 2013).

Table 5: Worms categorizes**.**

Worms categorize	
Email worms	Spread through email messages, especially with attachments.
Internet worms	Spread directly over the internet by abusing access to open system weaknesses.

Network worms	Spread over open, unprotected network shares
Multi vector worms	Spread over two or more various capabilities

In the world of computers, it is infiltrating across malware and hidden under the useful programs. Table 6 shows some of the most common Trojan categories (Sebastian, 2013). The name of the original Trojan is changing and activated every time you open the computer, so it is difficult to detect the damage and determine the place of attack (Schaeff B, Chan H., and Ogulnick S., 2009).

Table 6: Trojan categories**.**

Trojan categories	
Proxy Trojan	Designed to use a target computer through proxy server, which can attach to perform a multitude of operations anonymously.
Password Stealer Trojan	Designed to steal passwords from the targeted systems. This Trojan will very often first drop a key logging component into infected device
IM Trojan	Designed to steal account information or data through instant messaging programs such as Skype, MSN, and etc.
Dropper Trojan	Designed to install other malware on target systems. It is usually used in the beginning of a malware attack.
Game Thief Trojan	Designed to steal information through online gaming account.
Trojan-Banker	Designed to steal online banking information that allows hackers to access bank account or credit card information.

4. Factors of committing e-crimes

The previous section mentions methods that help committing of e-crimes, in which a person can steal personal data and confidential data. Foremost among the causes of e-crimes that are often infringed on information systems, this section explains the factors that lead to the commission of e-crimes, which are: Financial, Cultural, Political, and Sexual crimes as follows.

4.1 Financial e-crimes

Financial e-crimes, also often referred to as white-collar crime, which are committed via the Internet and have a major impact on the international banking and financial sectors.

Moreover, financial e-crimes affect private individuals, companies, organizations, and even nations. It has a negative influence on the entire economic and social system through the significant loss of money incurred (Alex Antoniou and Gauri Sinha, 2012).

Hiding behind a network, the perception of low risk and very high financial reward prompts many cyber criminals to engage in malware, phishing, identity theft and fraudulent money request attacks (Hussainat M. , 2013). Business week estimates that cybercrimes targeting online banking account nearly 700 million dollars per year globally (Nadiah Salman, 2014). Few examples of financial crimes are as follows:

- Using phishing to create a page similar to the official homepage. For example, they make a fake web page of the bank and asking the customer to enter the card number and PIN with intent to copy personal data and steal bank account (Rekouche, 2011).
- The false e-mails sent by criminals as in money laundering with promise to giving a high commission in the event of conversion, not to mention some of the fake emails sent by winning lottery or an award, where people are asked to send a bank account number to deposit the amount (Erbschloe, 2004) (Alex Antoniou and Gauri Sinha, 2012).
- Theft Automated Teller Machine (ATM) from bank and copied the credit card number of the machine. These cases were common in African countries, especially South Africa (Warner, 2010).

4.2 Cultural e-crimes

The method of cultural e-crimes refers to the theft of intellectual property rights or a person exercises one of the exclusive rights of the copyright holder without authorization and attribute them to oneself without mentioning the name of the source/author. It can be one of the following forms: (Broadhurst R. & Grabosky P., 2005) (Diane Lending & Sandra A. Slaughter, 1999)

- Copying software or movies on digital video discs (DVDs) from any international companies and selling them to the people at the lowest cost.
- Decoding private satellite channels, which are encrypted and have subscription fees. It is done by technology like Soft copy.
- Copying scientific literature electronically.

4.3 Political e-crimes

The spread of bad habits and cultures through internet network, which are alien to our society. The most widely spreads of political e-crimes are: terrorism, addiction, adultery and theft of money, which lead to the corruption of countries politically in the first place (Schaeff B, Chan H., and Ogulnick S., 2009).

- Theft of government websites, critical information and spread of viruses, as happened

in the United States in 1997, when teenagers broken through a system of air traffic control and disrupted air navigation system

- Information Technology is easier for terrorist groups to make communication because they are using the latest tools to convey their thoughts to the world (Neff, 1994). There are many reasons why terrorist using internet such as (Dogrul M.,Aslan A.&Celik E., 2011):
    - Limited money, they have considered them online from cheap materials that acquires the largest segment in the world.
    - The internet facilitates them to stay Unknown; these groups often choose countries with weak governments.
    - Their goals are easy to access, especially if the sites are not protected and secured.
    - There are no security barriers that hinder their movement.
    - Speed in the formation of attacks by internet communications.

4.4 Sexual e-crimes

Sexual e-crimes offenders have associated through the internet. Offenders have become active creators and distributors to distribute abusive content through online or offline by saving data (Riccardo Satta, Javier Galbally, and Laurent Beslay, 2014). Sexual e-crimes are summarized as follows:

- Flattering: When there is a relationship between a young man and a girl through chatting and developing this relationship with exchanging words of love until the trust becomes strong, then the young man exploits this relationship and threatens to blackmail the girl through her recorded calls, or saved chats for purpose of meeting his demands (Broadhurst R. & Grabosky P., 2005).
- Extortion: the most famous is a breakthrough personal computer of girls to take images and personal data, then threatening to expose the material online (Alex Antoniou and Gauri Sinha, 2012).
- Corrupting thoughts and weakening the faith of young minds through the dissemination of pornographic images and videos via the Internet (Alex Antoniou and Gauri Sinha, 2012).
- Pornographic websites: is one of the most prevalent ways through the Internet have been the dissemination of sexual images and movies, which is not limited to a particular age group, but sex can also enter these sites if unsupervised (Broadhurst R. & Grabosky P., 2005).
- Child abuse can occur in a child's home, organizations, schools, or communities the child interacts with. Each year, too many children fall prey to sexual predators and all too often, these heinous acts are recorded in photos and on video and released on the Internet (Oweis N., Owais S., Alrababa M., Alansari M., 2014). For example, in 2010, the largest sexual e-crime in the United States was detected and prosecution was made to 52 members of pedophile international child pornography for distributing up to 16,000 DVDs of child pornography (Sterling, 1992).

5. Cybercrimes in Various Countries

As mentioned before, there are many types of e-crimes involved to breach human and information privacy, theft, and illegal alteration of system critical information (Ping,

2011). Every year there are increasing of e-crimes in the world, due to the development of information technology and software changes (Rekouche, 2011).

With this spreading, countries are trying to protect the society from e-crimes. Different types of e-crimes have necessitated the introduction and use of newer effective security measures in many countries (Ilyin, 2013).

Recently, many countries carried out e-crime laws to limit their spread, especially after the expansion of communication networks using social media that resulted in adoption and implementation of these laws to reduce the e-crimes (Sharma, 2013). Figure 2 shows the top twenty countries exposed to external attacks from malicious programs in 2014. Each country lists 6 contributing tools mentioned in each subsection of countries (Symantec, 2014).

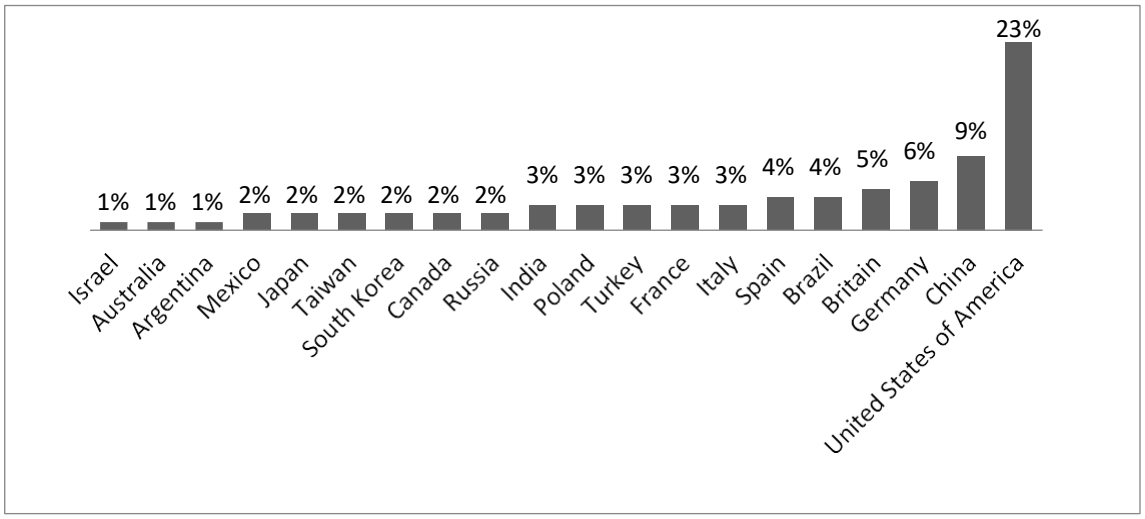

Figure 2: Top 20 countries exposed to external attacks from malicious programs in 2014.

This section explains and clarifies the spread of e-crimes and the applicable laws in various countries, which are: Malaysia, Mexico, Taiwan, Brazil, India, Japan, United Kingdom, United States of America as follows.

5.1 Malaysia

Malaysia aims to achieve the democratic potentials of technology. The government is committed to provide best practices, cyber security of information, training, and awareness programs. Among several forms of e-crimes, the Royal Malaysian Police reported that the top three types of e-crimes are:

1. e-commerce fraud-online purchase.
2. Parcel scam.
3. Voice-over-Internet Protocol (VOIP) scam across border syndicates. (Majid, 2012)

After confrontations, Malaysia amended the copyright Act in 1990 that came into force initially in 1987 as per accession to the Berne Convention, which provides explicit protection for literary and Artistic works viewed on computers (Neff, 1994).

After a few years, in 1997 the act was passed to computer crime, digital signature, and

copyright. Also in 1998, an act was passed to the communications and multimedia (CMA) (Kumar, 2009). At the beginning of the millennium an act was passed to optical disc, and in 2006 an act was passed to electronic transactions (Chang Yew, Wong, 2002). In addition, the Malaysian police have given statistical data on e-crimes from 2007 to 2012 on the number of issues and losses year wise as shown in Table 7 (Majid, 2012).

Table 7: Statistics of e-crimes from 2007 to 2011in Malaysia.

Year	Total cases	Losses (RM million)
2007	1139	11.4
2008	1821	12.9
2009	3863	22.3
2010	6167	63.0
2011	6586	8.5
2012	4738	96.1

5.2 Mexico

Mexico faced different types of e-crimes; the first type discovered was in copyright infringement. In 1991, Mexico made amendments and additions to the Federal law of copyright. These amendments feature the restriction of copying by users of a file or backup copy. It also improved the protection of computer programs (Neff, 1994).

Mexico took commendable effort to reduce the e-crimes by the Cybercrime Police Unit called Cybercrime-Mexico (DC Mexico) (Velasco, 2007). Table 8 shows the tools of e-crimes in Mexico (Symantec, 2014).

Table 8: Tools of e-crimes in Mexico**.**

Factors	Rank
Share of malicious computer activity	2
Malicious code	6
Spam zombies	18
A phishing web site hosts	31

DC Mexico was formed by the Ministry of Public Security in 2002, and headed by the Cybercrime Police Unit as the technical secretariat, and it is formed by government entities of

the Legislature, Federal Executive, and Judicial Power through representatives of the Chamber of Deputies, state governments, telecommunications companies, the Senate, the computer security services, industry chambers, academic institutions, and associations with civil society groups (Velasco, 2007).

5.3 Taiwan

The large number of counterfeiting industries in Taiwan is impacting economically the outside community that became a necessary intervention of outside parties to reduce these industries, which is considered by many countries as e-crimes. Republic of China, where Taiwan is a part of it, has issued a law in 1985, as amended due to the influence and pressure from the United States, which explicitly protects computer programs (Neff, 1994).

In 1992, Taiwan has protected the rights of authors through the adoption of new measures limiting the export of computer programs that contain software. They also inspect and control all related products and software that require the presence of a copyright or a valid license for the export of these software products (Neff, 1994).

The largest historical operations that were carried out by Taiwan regards to e- crimes after the signing of a joint agreement between the Chinese authorities and the officials of Taiwan in 2010, which resulted in 450 scammers arrested in all parts of Taiwan and the Chinese provinces. They carried out more than 16 joint raids, which lead to more than 1,000 arrests (Warner, 2010).

In this case, the activity initially focused on telephone fraud and auction fraud on the internet. Also, they had been doing ATM fraud through hacking into foreign banks and using ATM card readers to steal from more than 200 foreign financial institutions and bank accounts. In addition, money laundering, online shopping scams, and impersonation of public and agencies for fraud are parts of financial e-crimes (Sharma, 2013). Table 9 shows the tools of e-crimes in Taiwan by Symantec in 2014 (Symantec, 2014).

Table 9: Tools of e-crimes in Taiwan**.**

Factors	Rank
Share of malicious computer activity	2
Malicious code	11
Spam zombies	21
Attack origin	15
Bot	11
A phishing web site hosts	12

5.4 Brazil

Brazil is one of the countries keen to protect society from the e-crimes. In 1987, Brazil issued law No. 7646 that provides protection of copyright and establishes penalties for

exceeding the law. The software also focused on the law to protect the Brazilian market (Neff, 1994). Law No.8248 was passed in 1992 to provide protection of a patent relating to the technical nature of computer programs.

After that Brazil imposes a similarity test, as well as restrictions on the foreign origin of the software market (Neff, 1994). The Brazilian Senate Substitute passed acts to the House Bill No.89 of 2003 draft law, which provides no guarantees for freedom of expression or information. The purposes of the draft law created new provisions that would transform private companies responsible for delivering Internet services into an online police force to punish and detection of crimes committed using the Internet (Articl19 Group, 2012).

It is possible that the draft law would require same provisions for mass surveillance and data retention of all online communications by same unaccountable private bodies with few restrictions on the circumstances, which a court could order the disclosure of that data (Articl19 Group, 2012). Table 10 shows the tools of e-crimes in Brazil by Symantec in 2014 (Symantec, 2014).

Table 10: Tools of e-crimes in Brazil**.**

Factors	Rank
Share of malicious computer activity	4
Malicious code	16
Spam zombies	1
Attack origin	9
Bot	5
A phishing web site hosts	16

As well, in 2009 the federal government established the 'Critical Infrastructure Protection Information Security Working Group' (CIPISWG), which works in information security and incident response plans under Department of Information and Communications (DIC) (Sterling, 1992).

5.5 India

India is the country faced e-crimes in the ancient times; the beginning of laws in information technology was passed in 1951 for the rules of Indian Telegraph (Kumar, 2009). But the real beginning for e-crimes in India was in 2000, when the law of information technology was passed (Rekouche, 2011). India formed the Ministry of Information Technology in 1999, which have sought proposals to amend the law in 1998 after undergoing a huge change (Kumar, 2009).

Ministry of Information Technology had proposed to assist find offender by forcing Net cafe

owners to register the names and addresses of all persons who visit the café and also a list of sites they surfed. The Information Technology Act has been implemented in the year 2000. However, with the growth of information technology they need to amend some of the provisions of this IT Act and inclusion new types of e- crimes were found necessary and the amended Act was made effective in 2009 (Resercher, 2007).

The study in India on different types of e-crimes between 2001- 2011 is shown in Table 11. The study had tried to find out the cause of the rapid changes in the occurrence of crimes and its impact on the individuals in society. All data were collected from the media as well as from various electronic gates. (Bhatt S. & Pant D., 2011)

In the early years, the growth rate of reported cases was very high because people did not realize this type of crime, but after 2005 the rate of reported cases increased suddenly making it evident that individuals are starting to be aware of these crimes. This study is on the basis of data collected during ten years that growth is increasing rapidly year after year and these new types of crime affecting the community in a different ways (Bhatt S. & Pant D., 2011)**.**

Table 11: Report of e-crimes factors between 2001 and 2011in India.

Variants	**2001**	**2002**	**2003**	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**
Hacking	12	25	20	35	45	39	75	87	123	145	109
Phishing	08	14	26	54	40	58	103	92	97	109	74
Spam	04	17	19	29	43	67	86	94	89	105	57
Stalking	02	08	06	15	19	27	34	29	47	58	36
Defamation	03	11	09	13	17	24	32	37	59	46	45
Pornography	Nil	Nil	02	07	03	23	27	15	35	42	31

5.6 Japan

The Japanese government has created a vast network of regulatory bodies, institutions that operate under the umbrella of Center for Information Security, the National Secretariat of Council of Ministers, which was founded in 2005, after the cyber-attacks on the websites of many government ministries and agencies in 2000 (Shimbun, 2011). The Japanese government tried to stem any cyber-attacks through the formation of cyber security forces, which consist of four categories (Russell, 2011):

1. Policies to protect the industry led by the Ministry of Economy Trade and Industry.
2. Initiatives to combat cybercrime, led by the National Police Agency.
3. The Ministry of Internal Affairs and Communications.
4. 4- Security measures coordinated by the Ministry of National Defense.

In addition, Japan depends on the self-regulation in the private sector to protect personal data. Japan approved a law to protect personal information in 2005 on the protection of privacy and data at the companies. Failure to comply law, it is punishable by a fine of up to about 30.000 USD or imprisoned for up to six months (Warner, 2010). Table 12 shows the tools of e-crimes in Japan by Symantec in 2014 (Symantec, 2014).

Table 12: Tools of e-crimes in Japan**.**

Factors	Rank
Share of malicious computer activity	2
Malicious code	7
Spam zombies	29
Attack origin	11
Bot	22
A phishing web site hosts	11

Mitsubishi industries exposed to cyber-attacks in 2011 that resulted in the burning of 83 PCs in 11 locations including headquarters in Tokyo, research and development center, and many factories. As well as, Parliament and Kawasaki Heavy Industries were exposed to cyber-attacks at the same time (Bhatt S. & Pant D., 2011).

As part of initiative, an information technology forum established working groups in 2012. The report of the group released in May 2013 recommended using intermediary organizations to provide information that assist in building a relationship based on trust between businesses and consumers to use the personal data. Also, it stated that companies use, which set of personal information for any of their services instead of asking consumers to identify their data. As well as the need to provide different levels of service based on the type of consumers (Andreasson, 2011).

5.7 United Kingdom

United Kingdom is interested in information technology, copyright in databases, regulations and the code of advertising. In 2000 an Act was passed for electronic communications and the consumer protection regulation (Obrien A. & Marakas G., 2007). Table 13 shows the tools of e-crimes in the United Kingdom by Symantec in 2014 (Symantec, 2014).

According to a study carried out by cyber security experts at the University of Kent in 2011, more than 9 million adults in Britain were victims of hacked, and 8% of the population say they have lost money in the last year due to e-crimes, Also it stated that 2.3% of the population reported a loss of more than 10,000 pounds to online predators (Hernandez-Castro E.,Boiten E., 2013). In addition, the study found that 18.3% of those surveyed have seen attempts to break into one or more of their accounts on the Internet, including online banking, e-mail,

games, and social media.

Finally, the researchers found that people aged between 55 and 64 are less successfully targeted by cyber criminals. The figure for this group, 11.4%, said the study, which may be because they are more cautious or spend less time on the Internet. More than one out of every four people aged from 18 to 24 (27.3%) has been subjected to privacy attack (Hernandez-Castro E.,Boiten E., 2013).

Dr. Julio Hernandez-Castro and Dr. Eerke Boiten, from the University of Kent, the Cyber Security research center said that "it seems the crime on the Internet has a clear impact on the lives of citizens in the United Kingdom, with their account credentials being compromised significantly, and in some cases several times" (Hernandez-Castro E.,Boiten E., 2013).

According to the British government report in the same year, the total economic cost was 27 million British pounds per year, with identity theft of 1.7 billion pounds, online frauds and rip-offs of more than 1.4 billion pounds. The report found that the main loser was a British businessman, who took a blow of 21 billion pounds. British people suffer high levels of intellectual property theft and industrial espionage (Brokenshire, 2013).

Table 13: Tools of e-crimes in UK**.**

Factors	**Rank**
Share of malicious computer activity	5%
Malicious code	4
Spam zombies	10
Attack origin	3
Bot	9
A phishing web site hosts	5

5.8 United States of America

In 1986, a law was passed to the Electronic Communications Privacy (ECPA), which provides for identification judgments to protect the privacy of electronic communications and access third-party project for computers. (Neff, 1994).

In addition, the laws that are specifically designed to deal with e- crimes and traditional laws can also be used to prosecute crimes involving computers. For instance, Economic Espionage Act (EEA) passed in 1996 and established in order to put an end to trade secret misappropriation. EEA law includes provisions that make steal trade secrets aware of or try to do so in order to benefit someone other than the owner of trade secrets, as a crime (May, 2004).

A law of the digital millennium copyright was passed in 1998. The main purpose is to update copyright laws for dealing with the global information technology. Law No.17 was amended and implementation of the World Intellectual Property Organization, which provides for copyright treaty and the Performances and Phonograms Treaty (Lynch, 2002). Also, at the same year United State passed acts of Children`s online privacy protection (Kumar, 2009).

In 2003, an Act was passed for Controlling the Assault of Non Solicited Pornography And Marketing (CAN-SPAM). In 2006, Adam Walsh child protection and safety Act to protect children from sexual exploitation and violent crime, to prevent child abuse and child pornography thereby to promote internet safety. (Kumar, 2009).

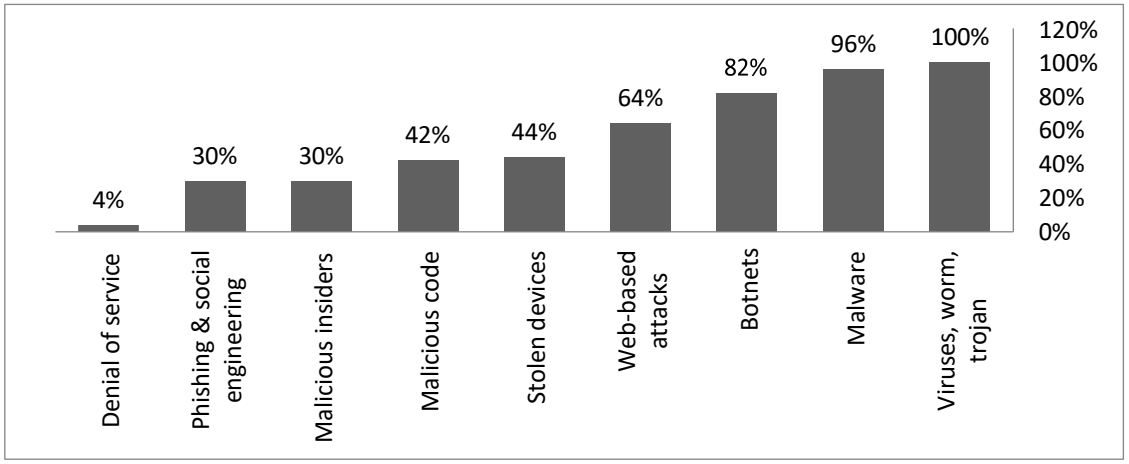

Figure 3: Attacks to companies in USA by benchmark sample**.**

Furthermore, the United States focused on Federal Trade Commission's (FTC`s) Guidelines for internet advertising, uniform domain name dispute resolution policy, computer fraud and abuse act and wire (May, 2004). Table 14 shows the tools of e- crimes in the United States (Symantec, 2014). The Figure 3 explains attacks to companies in the United States by benchmark sample (Paganini, 2012).

Table 14: Tools of e-crimes in USA.

Factors	**Rank**
Share of malicious computer activity	23
Malicious code	1
Spam zombies	3
Attack origin	1
Bot	2
A phishing web site hosts	1

5.9 Cybercrimes in Middle East

Like other countries, middle east is also not free of e-crimes. Various countries including Kingdom of Saudi Arabia (KSA), United Arab of Emirates (UAE), Egypt, Lebanon, Bahrain, Qatar, Syria, and etc., have been found to suffer through e-crimes. Figure 4 demonstrates the summary of nine countries in the middle east. This section describes specially about KSA and UAE in details.

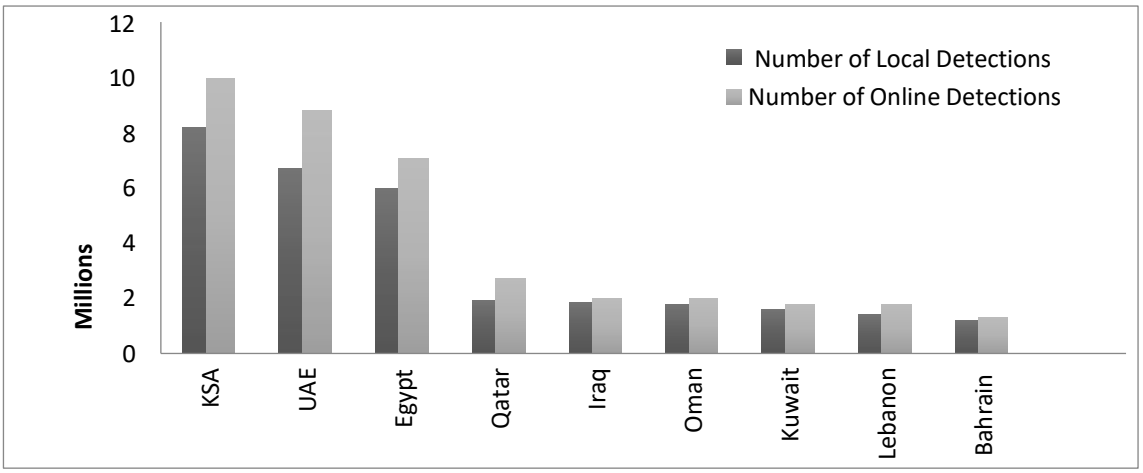

Figure 4: Kaspersky Lab presented statistics for the Middle East in 2014.

5.10 Kingdom of Saudi Arabia

Saudi Arabia is at the forefront of countries in using social networking, official statistics in 2013 (see Figure 6) revealed the results of using the Internet in the Arab world that Saudi Arabia has the highest rate among the Arab countries in terms of mobile usage of up to 63% and the number of connected Internet more than 8 million, as shown in Figure 5. Saudi Arabia also ranked first in the highest percentage of watching TV channels on the Internet up to 25% (Abdulaziz Alarifi, Holly Tootell, and Peter Hyland, 2012).

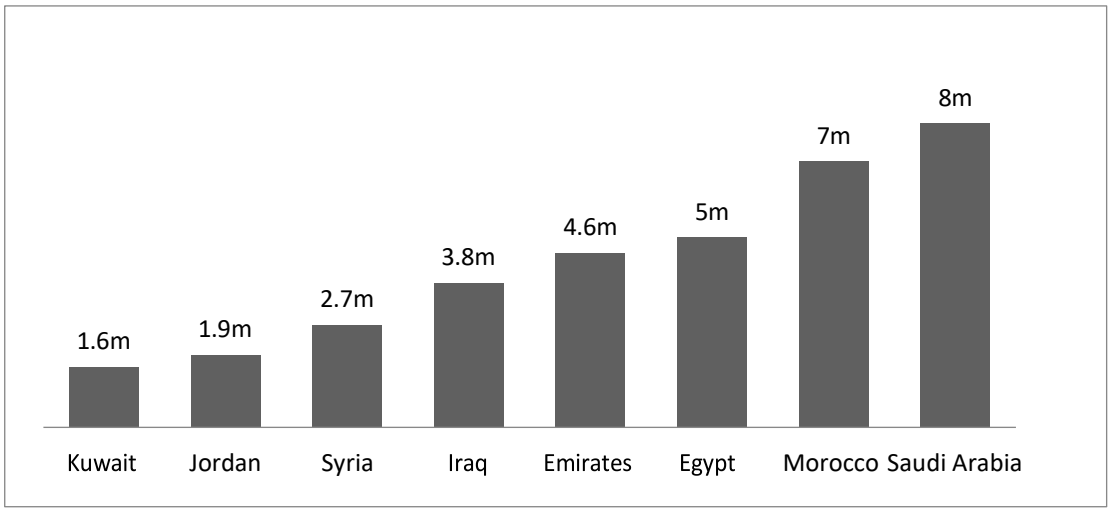

Figure 5: Number of people connected to the Internet in 2013.

The Ministry of Interior in collaboration with the Communications and Information Technology Commission declared strict punishments for computer crimes, including identity theft, defamation, hacking, theft of e-mail, and other**.** They issued combat system for e-crimes by cabinet decision No.79 dated 07/03/1428 AH, and was approved by the Royal Decree No. M/17 dated 03/08/1428 AH in 2014. This Law aims to reduce the occurrence of computer crime, by identifying these crimes and determining penalties for each of them to ensure the following:

1. Enhancement of information security.
2. Protection of rights relating to the lawful use of computers and information networks.
3. Protection of public interest, ethics, and morals.
4. Protection of national economy.

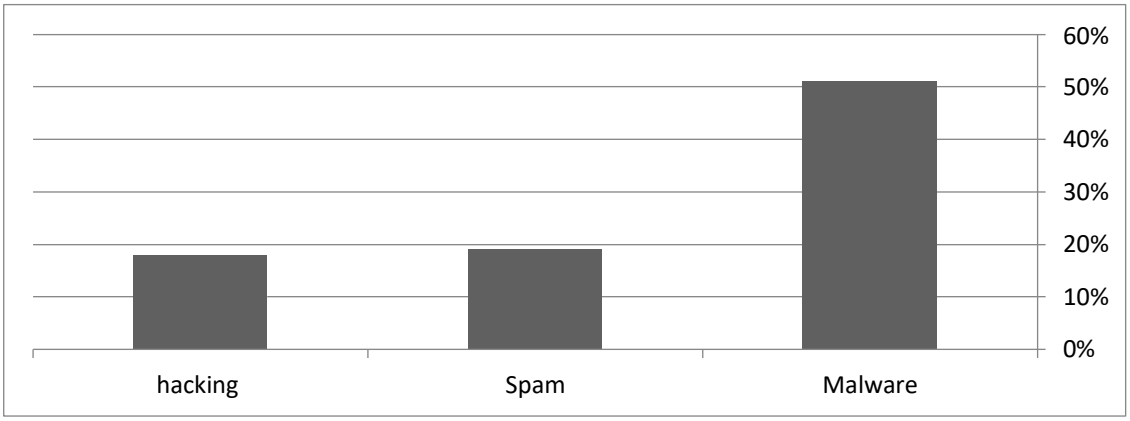

Figure 6: Tools prevalent of e-crimes in the United Arab Emirates**.**

5.11 United Arab Emirates

In United Arab Emirates (UAE), the perpetrators of-crimes have stepped up their activity in recent times in varied styles and age groups. According to statistics issued by Dubai Police in 2013, email fraud, extortion to get money and unethical goals up to 25% of total cases.

In 2012, the Norton Company submitted a study on e-crimes factors in UAE. It turns out that during every two minutes there is victim to e-crimes. The report revealed the tools prevalent of e-crimes in UAE, as shown in Figure 6 (Norton, 2012).

As per the report, experts warned of e-crimes activity in the UAE, where nearly 20% of the intrusions aimed at mobile devices, because the mobile internet use were approximately 56% of the total mobile users. The study also showed that the measures taken by the internet users to protect themselves are still not enough, that they cannot keep pace with the steady increase in e-crime ~~s~~-activities (Norton, 2012).

UAE President Sheikh Khalifa bin Zayed Al Nahyan issued a decree (Federal Law No. 5 of 2012) regarding the fight against crimes of Information Technology; some of these laws are:

- Punish by imprisonment of any person using electronic sites or any information

technology means to engage in the unauthorized use of, or provide unauthorized facilities for others to use, communication services or audio and video channels.

- Punish anyone who uses the Internet or an information technology device to defame sanctuaries or Muslim rites or holy people such as apostles and prophets, as well as offend sanctuaries or rites prescribed in other religions or insulting a heavenly recognized religion.
- Punish by imprisonment those who use the Internet or an information technology device for trafficking or the promotion of drugs or psychotropic substances of abuse or facilitate the deal of drugs.
- Punish anyone who uses the Internet or an information technology device in with the money transfer or deposit with the intention of concealing or disguising the illicit origin, as well as to hide or disguise the fact that the source of the money is illegal. Also use illegal money with the prior knowledge of its illegal source.

Table 15: Increasing of e-crimes in Kuwait.

Years	**Number of e-crime**
2010	**371**
2011	**300**
2012	**563**
2013	**997**
2014	**1206**
2015	**1461**
Total	**4904**

5.12 Kuwait

The e-crimes rate has increased recently in Kuwait because the deployment methods and techniques by criminals have become more complex and difficult to identify the offender, this is shown in Table 15. It is based on the studies of Kuwait General Department of Criminal Investigations (Kuwait General Department of Criminal Investigation, 2018). This section focuses on social media, e-crimes and law on e- crimes in Kuwait.

The director general of the General Department of Criminal Investigation in Kuwait, said that "the e-crimes rate in the State of Kuwait is evolving significantly". The goals of such e-crimes are: spreading destructive ideas, stealing money using fake internet cards, and destroying the information that has become difficult to be substantiated and tracked. He also added that "the e-crimes rate in the State of Kuwait is evolving significantly". The goals of such e-crimes are: spreading destructive ideas, stealing money using fake internet cards, and destroying the information that has become difficult to be substantiated and tracked. Table 16 shows the highest e-crimes activity until 2015 by the Kuwait General Department of Criminal Investigations (Kuwait General Department of Criminal Investigation, 2018).

Table 16: Types of e-crimes in Kuwait.

Activity	Number of crimes
Defamation	305
Abuse reputation	65
Fraud in the bank Editor	9
Libel and slander	37
copyright	1
stalking	49
Incitement to hatred of a category of society	7
Child pornography	150
Impersonate	40
Abuse means of communication	301
Incitement to immorality and debauchery	114
Threat and blackmail	55
Contempt of religions	3
The establishment of communities without a license	1
Theft	21
Compromising the very princely	-
Hacking	14
Insulting a public official	-
Fraud	27
Death threats	5
False news	2
Forgery	-
Divine insults	-
Total	**1206**

The Kuwait Ministry of Interior has established a special department called 'Fight against Electronic Crime' to handle e-crimes. It is able to make achievements in the detection of e-crimes with the following tasks (Directorate General of criminal Investigations, 2018):

- Supervising the detection of e-crimes such as theft of data, information, and identity of individuals and institutions.
- Follow-up on the infringement of copyright.
- Supervise the development of strategies to prevent hackers luring citizens to financial transactions or personal relationships in an illegal way.
- Providing all the necessary work in area such as technological software, human resources, and hardware technology.
- Supervise the criminal lab for photographic film and pictures for the Directorate General of criminal Investigations.

- Providing photographers to portray the e-crimes issues.

After viewing the factors of e-crimes in Kuwait, and measures taken by the Ministry of Interior in Kuwait to reduce this type of crimes, it is important to explain the relation between social media and e-crimes, and law of e-crimes in Kuwait.

6. Social media, Cybercrimes and Cyber Laws

Social media programs via the Internet swept a big part of our daily life due to the user friendliness of mobile phones. Here comes the decision of the individual in the use of this latest technology either beneficial or harming to himself or others. The uses of social media are on the rise of all age groups, with the vast majority being adults and young people. The arrival of smart phones has made it easier to access social media. Besides, the most prominent social media programs at the present time are Twitter, Facebook, and Instagram, which have become forums for religious and political debates. This is threatening the security of communities through the broadcasts and chats, which may undermine the harmony of the world. These thoughts may also lead to rifts among the communities and nations worldwide.

Kuwait News Agency (KUNA) published that Kuwait is one among the five Arab countries in using Twitter and Facebook extensively among its residents. A recent study revealed the majority of young population used Facebook and that it will rise further in coming years. Many countries relate e-crimes with social network, including social media because contact with different societies through internet led to the creation of e-crimes and social media laws (Louw C. , Von Solms S. , 2014). In recent years, many Arab countries witnessed political turmoil using social media, which led to civil unrest and street protests.

With the present social media, there is an increase of e-crimes in societies across the globe. There is a need for stringent laws to be emphasized by notaries and dignitaries. At present, in many of the countries (specially under developed countries) cyber laws are under the framework of the general laws and carry lenient or no punishments.

As an example, it is surprising that, Kuwait did not have special e-crime laws until 2015; they were applying sanctions under the audiovisual law only. But it turns out later that they started making e-crime laws and also initiated applying in the beginning of the year 2016. The Kuwait government aggressively enforced the audio-visual Law during 2013, also prosecuting citizens for internet-related offenses on social media platforms, and often pursuing these cases in conjunction with other criminal charges. The lowest penalty under the audiovisual law is a six-month jail term and a fine of up to KD 2,000 for those who illegally use computers that belong to others. The penalty increases if the misuse involves damaging or altering data or information stored in the computer. But the main penalty is a jail sentence of up to 10 years and a fine ranging between KD 20,000 and KD 50,000 for those who set up a website for terror groups or publish news about them that could be used for raising donations. At that, The Kuwait National Assembly passed a law to combat electronic crimes, stipulating a jail term of up to 10 years for providing online assistance to terror groups and for money laundering. (Kuwait Times, 2016). The safety of intellectual property is governed by the law No 64 of 1999 provides copyright protection and penalties for copyright infringement. Also the copyright of the press and publishing is protected under the Press and Publications Law, which was issued in 2006.

7. Influencing factors towards e-crimes

Various authors, in the recent years, have worked towards finding out influencing factors towards the e-crimes. The study of Hussainat (Hussainat M., 2013) has shown that the most important influencing factors are: financial, political, and cultural. Menshawi (Menshawi, 2003) showed that the highest e-crimes are breakthroughs, financial crimes, and crimes create or frequenting sites hostile and crimes piracy.

Ping (Ping, 2011) concluded that the network crime mainly focused on the financial system with the intent of making fraud, theft, defamation, sex, and intellectual property crime. Ping showed that the crime areas cover nearly all sides of social life, and the criminal activity will become more complex. Lesisko and Lee (Lesisko, Lee James, 2003) focused on copyright policy where the authors suggested raising awareness among teachers and students to reduce the unauthorized copyright.

Kearney and Kruger (WD Kearney & HA Kruger, 2014) were interested in their study if users have a trust in the corporation's ICT systems and infrastructure. Result showed that demographic factors play significant role in the protection of information and information assets.

Oweis et al., (Oweis N., Owais S., Alrababa M., Alansari M., 2014) used social engineering approach to find the most important human risk of e-crime. The study showed that the factors of committing e-crimes are young people, political interference, social experiences, and administrative restructuring of the networks.

Rekha and Radhakrishna (Rekha A. & Radhakrishna R., 2014) examined the relations between ethical awareness and the actual behaviors of individuals in real life situations. It was found that it is not enough to deter users from committing unethical actions related to information technology such as download of copyrighted content.

Another similar study in the field by Jeffery et al., (Jeffrey M. Stantona, Kathryn R. Stama, Paul Mastrangelob, Jeffrey Joltonb, 2004) develops taxonomy of end user security-related behaviors, tests the consistency of that taxonomy, and uses behaviors. The study found that people need training, awareness, knowledge of monitoring, and changing passwords more frequently and choosing good passwords.

Alexios et al., (Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis, 2012) built a prediction model to identify users who trust the application on repository. Results showed that the majority of users trusts the application repository, which is a clear lack of Smartphone users' security awareness.

In addition, Shahabuddin (Shahabuddin, 1987) stressed the need to the measures of securing computer data through legislation to help prevent computer crimes and should help deter the hackers from future attempts of breaching the security.

In the same field of cultural e-crimes, the study by Diane and Sandra (Diane Lending & Sandra A. Slaughter, 1999) focused to identify cultural factors that are associated with a variety of attitudes and behaviors regarding unauthorized software copying. This study reveals prominent differences in the behaviors and attitudes towards software copying in society.

Aloul (Aloul, 2010) found that users fall victims to phishing attacks. Researcher saw the need for security awareness programs in education, training, also in schools, universities, governments, and private organizations in the Middle East.

Alex et al., (Alex Roney Mathew, Aayad Al Hajj, and Khalil Al Ruqeishi, 2010) were Interested to explore some types of cybercrimes such as; phishing, spooting, and email. They discussed the ways to protect ourselves, and focus on solutions to users to be careful when using the internet, companies should secure themselves by firewalls and others programs and countries should implement special laws to counter e-crimes.

Amber et al., (Amber Stabek, Paul Watters, and Robert Layton , 2010) invented cybercrime classification framework (CCF), which determine what is needful for the development of a transnational, inter-jurisdictional, and global approach to identify and prosecute criminals othe internetet. This framework would improve the efficiency in identifying, and monitoring e-crimes.

A study by Bhanu et al., (Bhanu Sahu, Neeraj Sahu, Swatantra Kumar Sahu, and Priya Sahu, 2013) showed that, to give best judgments to criminals of e-crimes, society need special e-crimes laws, which make it easy to identify e-crimes types and how to deal with it.

The present study by Frances and Herman (Frances S. Grodzinsky and Herman T. Tavani, 2002) have considered about issues of cyber stalking that has relation with legal liability. Authors have seen that individuals and the internet Service Providers (ISPs) should assume responsibility to prevent harm of e-crimes.

Alex and Gauri (Alex Antoniou and Gauri Sinha, 2012) concentrated on sexual e- crimes, which encompass online publications or distribution of sexually explicit material. Also the study focused of financial e-crimes associated with money laundering via internet. Authors stressed that the countries need to take legal efforts against sexual pornography via Internet and anti-money laundering measures that enforce law to reach the criminals by tracing the path of their money.

In the same field of sexual e-crimes, Riccardo et al., (Riccardo Satta, Javier Galbally, and Laurent Beslay, 2014) focused on using demographic factors to monitor and investigate the offender by identifying facial features of the offender from the child victim by using law enforcement agencies. Also in the fight against online child sexual abuse (CSA).

In the light of the above mentioned studies, still there is a need to have extensive research about what are the factors which influencing e-crimes. Studying them well and them implementing the studies may be a step ahead towards cyber security as follows in Section 4.

8. Cyber Security

It is well known by now that cybercrime is a big threat worldwide. Cybercrime, no doubt, has made a big amount of damages everywhere in the world. As much as $6 trillion annually, by 2021, has been predicted to global damages (Cyber Security Ventures, (2018); Global Cybersecurity Index 2017 (2017); Aimee O'Driscoll (October 2, 2018)). Therefore, it is extremely important to get ready for potential threat cybercrime poses, the impact it is having, and what is being done about it. Cybersecurity, therefore, needs to be considered as a hot area to work on in order to avoid any future damages caused by cybercrimes. Some progress has been made in the recent years. Various countries, around the globe, have committed for

cybersecurity measures. Top ten most committed countries are Singapore, United States, Malaysia, Oman, Estonia, Mauritius, Australia, Georgia, France and Canada. For further information, the reader is referred to (Global Cybersecurity Index 2017 (2017)).

It has been noted that there is a need to fill big gaps in cyber preparedness around the globe. These gaps exist not only within and between countries, but they also exist between regions. Furthermore, cybersecurity related commitments, many of the times, are not equally distributed with countries performing well in some areas and less so in others. To make Cybersecurity more effective, it is mandatory that the factors like skills, cyber laws, international cooperation and technical implementation need to be given tremendous importance. Some additional concerns are that cybersecurity should not just be a worry of the governments, it should be given ample commitment by other sectors and communities. Hence, it is desired and vital to have a cybersecurity culture where people are aware of the give-n-take when using computers and networks.

Many organizations overlook the security aspect of the system information and monitoring to protect their original data. So, there are many data protection software such as: black ice defender, lockdown 2000, and anti-virus. One can also see how to protect data by using a firewall (Schaeff B, Chan H., and Ogulnick S., 2009). A firewall is a network security system that monitors and controls the incoming and outgoing network traffic (Mark Reith, Clint Carr, and Gregg Gunsch, 2002). This program filters data network to decide whether the devices are empty of viruses, not to forward it to their destination or to reject it. It has become important at this time to PCs to protect them from e-crimes and breakthroughs (Bruce S. Schaeffer, Henfree Chan, Henry Chan, and Susan Ogulnick, 2009).

Firewall contains a protection program for managing the information security such as: firewall logs, system logs, records of anti-virus, user profiles, viruses, records of physical access, etc.. It helps companies to collect and connect data securely and identify threats internally or externally (IIBF, 2012). The program includes monitoring successful practices such as:

- Strict security provided over form and layer helps identify security threat both from the internal network (more pressing) or foreign companies.
- Encrypt critical business data and record all changes to the audit minute and put strict controls to access the data.
- The application of the policy of 'least access privileges' to ensure not to allow access to all company information and records.
- Update the process of identity management from time to time to determine who has access to company information across the network by denying the access of employees who have completed their service from the institution.
- Providing Systems that reveal infiltration of the company's network to assist in the detection of suspicious or malignant activities. (Schaeff B, Chan H., and Ogulnick S., 2009).

The programs are generally created to protect information in computers, which can prevent the unauthorized request from external computer networks (Schaeff B, Chan H., and Ogulnick S., 2009). Firewall allows users to read email from different remote locations, but at the same time it does not allow running certain unknown program (Obrien A. & Marakas G., 2007). Firewall programs are not completely effective. There are some precautions to take as a user to ensure the survival of the system and have awareness to deception through online networks and educate ourselves of any developments that occur in the information technology (Obrien A. & Marakas G., 2007).

9. Conclusion

Technology has become an integral part of our daily life in the world of the internet and cannot be dispensed with. Although there are several advantages of the technology, but it has become a threat to our lives too. It became necessary to take caution when using any technology so as not to be trapped by e-crimes. Many of the countries do not have specific laws related to e-crimes until today, so it is imperative to enact new laws to combat the worldwide scourge, which has no boundaries. Many of the studies in the current literature have focused on factors that affecting e-crimes such as demography, sexual, financial, cultural, and political. There is a need to improve and validate these studies region vise and country vise. Thus, as future work, it desired to do the followings:

- Build new models to measure the influence of demography and technology over the factors of e-crimes leading political, cultural, financial, and sexual aspects in societies locally and globally.
- Create hypotheses for each factor to find the influence between factors.
- Collect data from significant sample sources, on country as well as region bases, to test on the build models and created hypothesis.
- Using suitable statistical measures for data analysis.
- Discuss the study finding and objectives.
- Drawing conclusions and set recommendations for future studies.
- Making necessary and needed measures for cybersecurity around.

References

Abdulaziz Alarifi, Holly Tootell, and Peter Hyland. (2012). A study of information security awareness and practices in Saudi Arabia. *International Conference on Communications and Information Technology (ICCIT)* (pp. 6-12). Hammamet: IEEE.

Alex Antoniou and Gauri Sinha. (2012). Laundering sexual deviance: Targeting online pornography through anti-money laundering. *European Intelligence and Security Informatics Conference* (pp. 91-98). Odense: IEEE.

Alex Roney Mathew , Aayad Al Hajj , and Khalil Al Ruqeishi. (2010). Cybercrimes: Threats and protection. *International Conference on Networking and Information Technology* (pp. 16-18). Manila: IEEE.

Alexios Mylonas, Anastasia Kastania, Dimitris Gritzalis. (2012). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security, 34*, 47-66.

Aloul, F. A. (2010). Information Security Awareness in UAE: A Survey Paper . *Internet Technology and Secured Transactions (ICITST), 2010 International Conference* (pp. 1-6). London: IEEE.

Amber Stabek, Paul Watters, and Robert Layton . (2010). The Seven Scam Types: Mapping the Terrain of Cybercrime . *Second Cybercrime and Trustworthy Computing Workshop* (pp. 41-51). Ballarat, VIC : IEEE.

Andreasson, K. (2011). *Cyber security : Puplic sector threats and responses.* U.S.A: CRC press.

Anti-phishing Working Group. (Sep,2013). *Phishing Activity Trends Report.* Phishing Activity Trends Report.

Articl19 Group. (2012, Feb 2). *Brazil: Draft Cybercrimes Law.* Brazil: www.artical19 . com.

Balkhi, S. (2013, MAY 6). 25 Biggest Cyber Attacks In History.

Barnes B. and Perlroth N. (2014, DEC 3). Sony Pictures and F.B.I. Widen Inquiry Into Hackers' Attack. *The New York Times*.

Berg, D. (2013). Social Media and Online Defamation. *NOLO law for all*.

Bhanu Sahu, Neeraj Sahu, Swatantra Kumar sahu, and Priya Sahu. (2013). Identify Uncertainty of Cyber Crime and Cyber Laws . *International Conference on Communication Systems and Network Technologies* (pp. 450 - 452). Gwalior : IEEE.

Bhatt S. & Pant D. (2011). Cyber Crime in India. *International Journal of Advanced Research in Computer Science*, Vol. 2 Issue 5, 153-156.

Box, J. F. (1987, Feb). Guinness, Gosset, Fisher, and Small Samples. *Institute of Mathematical Statistics*, Statistical Science, Vol. 2, No. 1, pp. 45-52.

Broadhurst R. & Grabosky P. (2005). *Cyber-crime.* Hong Kong: Hong Kong University Press.

Brokenshire, J. (2013, Mar 14). *UK government*. Retrieved Aug 1, 2014, from http://www.gov.uk.

Bruce S. Schaeffer, Henfree Chan Henry Chan and Susan Ogulnick. (2009). Cyber Crime and Cyber Security:A White Paper for Franchisors, Licensors, and Others. business.cch.com.

Chang Yew, Wong. (2002). *Malasian Law and Computer Crime* . Malaysia: SANS.

Diane Lending & Sandra A. Slaughter. (1999). Understanding differences in ethical beliefs and behaviors toward software copying: the effects of organization culture. *SIGCPR '99 Proceedings of the 1999 ACM SIGCPR conference on Computer personnel research* (pp. 253-260). NY, USA : ACM.

Dixon, P. D. (2005, December). An overview of computer forensics. *Potential, IEEE, 24*(5), 7-10.

Dogrul M.,Aslan A.&Celik E. (2011). Developing an international cooperation on cyber defense and deterrence againts cyber terrorism. *International conference on cyber conflict* (pp. 1-15). Istanbul: IEEE.

Erbschloe, M. (2004). *Trojans, Worms, and Spyware: A Computer Security Professional's Guide to Malicious Code.* Oxford: Butterworth-Heinemann.

Fawn T. & Paternoster R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*, 773-793.

Frances S. Grodzinsky and Herman T. Tavani. (2002). Cyberstalking: moral responsibility, and legal liability issues for Internet service providers. *International Symposium onTechnology and Society, 2002. (ISTAS'02).* (pp. 331
- 339). IEEE.

Gorazd Mesko,and Igor Bernik. (2011). Cybercrime: Awareness and Fear: Slovenian Perspectives. *European Intelligence and Security Informatics Conference (EISIC)* (pp. 28 - 33). Athens: IEEE.

Hamdi M. , Safran M. and Wen-Chi Hou . (2014). A Security Novel for a Networked Database . *Computational Science and Computational Intelligence* (pp. 279 - 284). Las Vegas, NV: IEEE .

Hernandez-Castro E.,Boiten E. (2013, Aug 23). *About Us: Kent University*. Retrieved Sep 22, 2014, from University of Kent website: http://www.cs.kent.ac.uk

Hussainat, M. (2013). Computer Crimes in the Jordanian Society: Ajloun/Empirical Study. *Asian Social Science, 9*, 85-93.

IIBF. (2012). IT Security . India : M/s TaxMann Publishers.

Ilyin, Y. (2013, AUG 15). *Kaspersky Lab Business Web site*. Retrieved MAY 22, 2014, from Kaspersky Lab Business Web site: http://business.kaspersky.com/threats- in-q2-2013.

Jeffrey M. Stantona, Kathryn R. Stama, Paul Mastrangelob, Jeffrey Joltonb. (2004). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Johnson, M. (2013). *Cybercrime : security and digital intellience.* U.S.A: Gower publishing LTD.

Kabay, M. E. (2008). A Brief History of Computer Crime. *An Introduction to Students conference.* Norwich University.

Kenefick, S. (2008). *Real World Software Configuration Management.* Newyork: Apress.

Kumar, A. P. (2009). *Cyber Crime.* Bangalore: The Banner of YFI & Anupa p Kumar.

Kuwait Times. (2016, 12 1). *Kuwait times*. Retrieved 1 25, 2016, from http://news.kuwaittimes.net/website/electronic-crimes-law-threatens-to-further-stifle-freedom-of-expression-amnesty-intl/.

Lesisko, Lee James. (2003). *Analyzing Software Piracy in Education.* ERIC.

Linda L. Edwards, J. Stanley Edwards, Patricia Kirtley Wells. (2008). *Tort Law for Legal Assistants.* Cengage Learning.

Louw C. , Von Solms S. . (2014). Online social networks to online social malworks. *The evolution an industry conference* (pp. 1-7). Africa: IEEE.

Lynch, J. (2002). *The United States: department of justice*. Retrieved Aug 3, 2014, from http://www.justice.gov.

Majid, M. D. (2012). *Cybercrime : Malaysia.* Malaysia: Royal Malaysia Police. May, M. (2004). *Federal computer crime law* . U.S.A.: SANS institute .

Menshawi, A. (2003). The size and style of the most common Internet crimes among Internet users in Saudi society, and a research paper.

Montgomery, D (2001). *Design and Analysis of Experiments (5th Edition).* NewYork: John Wiley & Sons.

Moon B., Mccluskey J., Mccluskey C. (2010). A general theory of crime and computer crime: An empirical test. *Journal of Criminal Justice, 38*(4), 767-772.

Neff, R. (1994). Software Piracy : International Copyright overview. *WESCON/94. Idea/Microelectronics. Conference Record* (pp. 190-195). Los Angeles, CA: IEEE.

Norton. (2012, April, 22). aitnews. Retrieved (2014, Dec 2) from http://aitnews.com.

Obrien A. & Marakas G. (2007). *Introduction to Information System.* Boston: McMagraw-Hill International irwin.

Ogilvie, E. (2000). Cyberstalking. *trends & issues in crime and criminal justice* (pp. 12- 19). Australia: Australian Institute of Criminology.

Oweis N., Owais S., Alrababa M., Alansari M. (2014). A Survey of Internet Security Risk Over Social network. *Computer Science and Information Technology* (pp. 1-4). Amman: IEEE.

Paganini, P. (2012, April 23). Analysis of cybercrime and its impact on private and military sectors. *PenTest Auditing & Standards*. Available: http://securityaffairs.co/wordpress/4631/cyber-crime/analysis-of-cybercrime- and-its-impact-on-private-and-military-sectors.html

Ping, Y. (2011). Study on the Main Form of Network Crime from the View of Criminology. *International Conference on Human Health and Biomedical Engineering* (pp. 1108-1111). China: IEEE.

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. *International Journal of Digital Evidence,*1(3),1-12.

Rekha A. & Radhakrishna R. (2014). Piracy in the digital age: Is ethical awareness turning into action? *Ethics in Science, Technology and Engineering*, (pp. 1-4). Chicago, IL: IEEE.

Rekouche, K. (2011). *Early phishing.* Available: http://arxiv.org/abs/1106.4692v1 .

Researcher. (2007). Retrieved Aug 2, 2014, from cyberlawsinindia: http://cyberlawsin india.net.

Riccardo Satta, Javier Galbally, and Laurent Beslay . (2014). Children Gender Recognition Under Unconstrained Conditions Based on Contextual Information. *International Conference on Pattern Recognition* (pp. 357 - 362). Stockholm: IEEE.

Richard Mankiewicz; Ian Stewart. (2001). *Story of Mathematics.* New Jersey, U.S.A: Princeton Univ Pr, Ewing.

Royakkers, L. (2000). The Dutch Approach to Stalking Laws. *Berkeley Journal of Criminal Law*, 3, 1-14.

Rubino, F. A. (2014). *Federal Criminal Defense Lawyer Frank A. Rubino*. Retrieved NOV 7, 2014, from http://www.frankrubino.com

Russell, J. (2011, OCT 25). Japanese government hit by Chinese Trojan horse attack.

Saini Das, Arunabha Mukhopadhyay, and Girja.K. Shukla. (2013). i-HOPE Framework for Predicting Cyber Breaches: A Logit Approach. *2013 46th Hawaii International Conference on System Sciences (HICSS)* (pp. 3008 - 3017). Wailea, HI, USA: IEEE.

Schaeff B,Chan H. and Ogulnick S. (2009). Cyber Crime and Cyber Security. *A wite paper for Franchisors licensors, and others*, p.1-15.

Sebastian. (2013, 25 DEC). Security 1:1 - Part 1 - Viruses and Worms. *Security, Symantec Protection Center (SPC)* .

Shahabuddin, S. (1987). Computer Crimes and The Current Legislation. *ACM SIGSAC Review, 5*(3), 1-8.

Sharma, D. (2013, 7 10). Retrieved Aug 2, 2014, from India largest cyber security solution: http://www.indiancybersecurity.com

Shimbun, T. A. (2011, Aug 20). Editorial: Japan should play active role against cyberattacks. *Adventure works weekley* .

Sterling, B. (1992). *The Hacker Crackedown.* Newyork: Bantam Books.

Swain, B. (2009, JUN 25). What are malware, viruses, Spyware, and cookies, and what differentiates them ? *Inside Symantec, Security, Endpoint Protection (AntiVirus)*.

Symantec. (2014). *List of Top 20 Countries with the highest rate of Cybercrime.* USA: Business Week/Symantec.

Symantec Enterprise. (2014, DEC 3). Retrieved DEC 5, 2014, from Symantec Corporation : http://www.symantec.com

Tabuchi, H. (2011, Sep 21). U.S. Express concern about new cyberattacks in Japan. *The NewYork Times*.

Totarotech. (2013, JAN 31). *TotaroTechBlog* . Retrieved OCT 10, 2015, from https:// totarotech.wordpress.com/2013/01/31/5-motivations-for-cybercriminals/

Velasco, C. (2007). *The Legal Framework on Cybercrime and Law Enforcement in Mexico.* mexico: Contribution to the Second WSIS Action Line C5 Facilitation Meeting.

Warner, G. (2010, Aug 26). Major Fraud Ring Busted in largest Chinese Cybercrime Operation. Malcovery, UAB.

WD Kearney & HA Kruger. (2014). Consodering the influence of human trust in practical social engineering exercises. *Information Security for South Africa (ISSA)* (pp. 1-6). Johannesburg : IEEE.

Cyber Security Ventures, (2018). https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Global Cybersecurity Index 2017, (2017). International Telecommunication Union (ITU), https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

Aimee O'Driscoll (October 2, 2018), 100+ Terrifying Cybercrime and Cybersecurity Statistics & Trends [2018 EDITION], https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/#Global.

Kuwait General Department of Criminal Investigation, (2018).

https://hmaconsulting.com/projects/kuwait-general-department-of-criminal-investigation/