Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.3, No.12, 2013

Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future

Bushra Mohamed Elamin Elnaim (Assistant professor)
Department Of Computer Science and Information, College of Science and Humanity Studies-Alsulial
Salman Bin Abdulaziz University, Kingdom Of Saudi Arabia.
E-mail: bushra_moh@hotmail.com

Abstract
The world we are in today is all about Information Technology (IT) because we are in the age of Information Technology and the people with the right information, with proper way of disseminate this information and processing them is considered as the most successful. Computers have become the mainstay of business and government processes. Business has been using them for years and in most countries, there are drives towards electronic or joined up government. This is to allow the people to access government services from their desktop in their own home . A rapid growth of computer crimes and formation of laws in different countries addresses the severity of problem. This paper discusses the stand of Saudi Arabian government against cyber crime and its IT act. It analyzes the cybercrime in the Kingdom and the anti-cyber crime law.
Keywords: Cyber Crime, Anti-Cyber crime law, Cyber Terrorism

1. Introduction

The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet.

This rapid growth and widespread use of the Internet, fueled the need for better methods of protecting the computers and the information they store, process and transmit.

The U.S. National Information Systems Security Glossary defines "Information Systems Security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats (University of Nevada, 2012).

"Computer crime" refers to any crime that involves a computer and a network (Moore.R. ,2005). The computer may have been used in the commission of a crime, or it may be the target (Warren G. Kruse, Jay G. Heiser ,2002). Netcrime refers to criminal exploitation of the Internet. Dr. Debarati Halder and Dr. K. Jaishankar defines Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" (Halder, D., & Jaishankar, K. ,2011).

2- Types of Cyber Crimes

Cybercrime continues to diverge down different paths with each new year that passes. In 2013, cybercriminals are changing the way they organize and targeting new users and new platforms, online transaction-based activities continue to be exploited, and hacktivism-related attacks continue to rise as a way to commit corporate espionage, push political agendas or cause reputational damage. In this section let us explaining various variants of technology that are used for cyber crime.

A. Hacking

Hacking is the gaining of access(wanted or unwanted) to a computer and viewing, copying, or creating data(leaving a trace) without the intention of destroying data or maliciously harming the computer (Urban Dictionary, 2013).

Hacking and hackers are commonly mistaken to be the bad guys most of the time. Crackers are the ones who screw things over as far as creating virus, cracks, spyware, and destroying data. A hacker first attacks an easy target, and then uses it to hide his or her traces for launching attacks at more secure sites.

B. Virus Dissemination

A computer virus is a program that can 'infect' other legitimate programs by modifying them to include a possibly 'evolved' copy of itself.. Viruses can spread themselves, without the knowledge or permission of the users, to potentially large numbers of programs on many machines. Computer viruses currently cause billions of dollars worth of economic damage each year (Syemantic.com, 2008) due to causing systems failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. The Internet gives viruses a particularly efficient new path for global infection. The following figure show families and habitats of viruses.

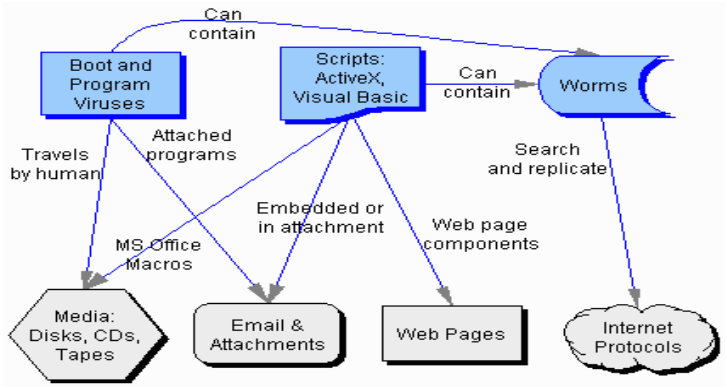

Figure (1): Viruses - Families and Habitats

C. Denial of service Attack

A DoS attack or distributed DoS (DDoS) attack is a crime that renders computers or network resources inaccessible to their intended users or customers. Although DoS attacks may be via different means, motives, and targets, they generally include the concerted, malevolent efforts of a person or persons to make an Internet site or service unable to perform normally or even at all (Yuval F and others, 2010) .A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. There are two general forms of DoS attacks: those that crash services and those that flood services.

D. Phishing

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication(Van der Merwe and others, 2005). Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users(Microsoft corporation, 2013) and exploits the poor usability of current web security technologies.

E. Spamming

Electronic spamming is the use of electronic messaging systems to send unsolicited bulk messages (spam), especially advertising, indiscriminately. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: 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, junk fax transmissions, social networking spam, social spam, television advertising and file sharing spam. Spamming remains economically viable because advertisers have no operating costs beyond the management of their mailing lists, and it is difficult to hold senders accountable for their mass mailings. Because the barrier to entry is so low, spammers are numerous, and the volume of unsolicited mail has become very high. In the year 2011, the estimated figure for spam messages is around seven trillion. The costs, such as lost productivity and fraud, are borne by the public and by Internet service providers, which have been forced to add extra capacity to cope with the deluge. Spamming has been the subject of legislation in many jurisdictions (Spamhaus.org,2013).

F. Cyber Stalking

Cyber stalking is the use of the Internet or other electronic means to stalk or harass an individual, a group of individuals, or an organization. It may include the making of false accusations or statements of fact, monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. The definition of "harassment" must meet the criterion that a reasonable person, in possession of the same information, would regard it as sufficient to cause another reasonable person distress(Bocij, Paul, 2004). Cyber stalking is different from spatial or offline stalking in that it occurs through the use of electronic communications technology such as the internet. However, it sometimes leads to it, or is accompanied by it (Spitzberg, Brian H.; Hoobler, Gregory (February 2002). Both are criminal offenses. Cyber stalking shares important characteristics with offline stalking; many stalkers – online or off – are motivated by a desire to control their victims.

A cyber stalker may be an online stranger or a person whom the target knows. A cyber stalker may be anonymous and may solicit involvement of other people online who do not even know the target.

G. Cyber Terrorism

Cyber terrorism is the use of Internet based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses. Cyber terrorism is a controversial term. Some authors choose a very narrow definition,

relating to deployments, by known terrorist organizations, of disruption attacks against information systems for the primary purpose of creating alarm and panic. By this narrow definition, it is difficult to identify any instances of cyber terrorism. Cyber terrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives (Matusitz, Jonathan (April 2005). Objectives may be political or ideological since this is a form of terrorism. Cyber terrorism can also include attacks on Internet business, but when this is done for economic motivations rather than ideological, it is typically regarded as cybercrime.

H. **Cyber Pornography**

Cyber pornography or Internet pornography is pornography that is accessible over the Internet, primarily via websites, peer-to-peer file sharing, or Usenet newsgroups. While pornography had been available over the Internet since the 1980s, it was the availability of widespread public access to the World Wide Web in 1991 that led to an expansion of Internet pornography. The Internet enables people to access pornography more or less anonymously and to view it in the comfort and privacy of their homes. It also allows access to pornography by people whose access is otherwise restricted for legal or social reasons, such as children.

3. The Current Situation of Cyber Crime in Saudi Arabia

Information Technology highly influenced the Arab world in the last decade which results in increase of Internet users day by day. There were about 15.8 million Internet users in the Kingdom at the end of 2012 representing a population penetration rate of about 54.1% compared to 5% in 2001 (CITC annual report, 2013). The Communications and Information Technology Commission in Saudi Arabia estimates and field surveys indicate that there are about three users per fixed broadband subscription, both residential and business. There is also more than one user per mobile broadband subscription. Further, a number of users have both fixed and mobile subscriptions.

It is expected that the demand for Internet services will increase significantly in the next few years due to the availability of fiber optic networks at very high speeds (especially in large cities), growing Internet content, and the spread of handheld smart devices and applications.

Cyber crime has cost the Kingdom SR 2.6 billion in year 2012, according to a report released by Symantec. Symantec released the findings of its annual Norton Cybercrime Report, one of the world's largest consumer cybercrime studies (arabnews,2012).

The study was aimed at understanding how cybercrime affects consumers, and how the adoption and evolution of new technologies impact people's security. With findings based on self-reported experiences of more than 13,000 adults across 24 countries.

In the Kingdom, it is estimated that more than 3.6 million people fell victim to cybercrime in year 2012, suffering an average of $ 195 (SR 730) in direct financial losses and 40 percent of the country's social networking users have fallen victim to cybercrime on social networking platforms. Of the social networking users, 20 percent have been victims of social or mobile cybercrime in the past 12 months in the Kingdom compared to 21 percent globally.

In addition, there was many online adults are unaware as to how some of the most common forms of cybercrime have evolved over the years, and thus have a difficult time recognizing how malware, such as viruses, act on their computer. In fact, the study found 40 percent of adults in KSA do not know that malware can operate in a discreet fashion, making it hard to know if a computer has been compromised, and more than half (55 percent) are not certain that their computer is currently clean and free of viruses.

3.1 Cases of cyber-attacks in Saudi Arabia

1- Cyber-attack against state-owned oil company Aramco. Over 30 000 computers at Saudi Arabian oil company Aramco were hit by a devastating virus in August 2012. The attack destroyed data and erased hard-drives of computers and is thought to have been aimed at stopping the production of oil (world exchange report,2013) .

2- The Official Website of King Saud University (KSU) Got hacked by some unknown Hacker . It is a public university located in Riyadh, Saudi Arabia. Database of 812 Users hacked from http://printpress.ksu.edu.sa/ and dumped on Internet by Hacker on a file sharing site including Mail address list, mobile phones and passwords (thehackernews.com, 2012) .

3- Several government websites in Saudi Arabia were sabotaged in a series of heavy cyber-attacks from abroad, disabling them briefly until the attacks were repelled (alarabiya.net, 2013).

4. THE ANTI-Cyber Crime Law in Saudi Arabia

The paramount body of law in KSA is the *Sharīʿah*. The *Sharīʿah* is comprised of a collection of fundamental principles derived from a number of different sources, which include the Holy *Qu'ran* and the *Sunnah*, which are the witnessed sayings and actions of the Prophet Mohammed.

Prohibited acts under *Sharīʿah* are punishable by specific penalties set out in the Holy *Qu'ran* or the *Sunnah*. However, where the Holy *Qu'ran* and the *Sunnah* are silent in that regard, a judge may use his discretion to

determine the appropriate penalty. Such penalties may include imprisonment, monetary compensation and/or deprivation of certain rights. In determining the severity of a penalty, a judge will take into consideration the damage suffered by a victim and whether such damage is actual or consequential. In general, however, only actual proven damages are awarded by Saudi Arabian adjudicatory bodies.

The new Arab Cybercrime Agreement (no. 126 of 2012) was approved in Saudi Arabia. This agreement will mainly address the rise in electronic crime which embraces such crimes as credit card frauds, internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, illegal access and interception, and so on. It aims as well at encouraging cooperation between Arab countries in combating cybercrimes. The Agreement stipulates also on the importance of enforcing the Copyrights Law. Penalties are imposed on the violators of the Agreement terms and regulations. By way of background, Saudi Arabia had previously issued a penal Law on cybercrimes which was comprised of 16 sections. The penal features of the law include the following: (sabaip.com, 2012)

Table I: Anti Cyber Crime Law 2007

Crime	**Fines**	**Imprisonment Term**
- Having knowingly accessed a government network without authorization, and by means of such conduct having obtained information that has been determined by the Saudi government to require protection against unauthorized disclosure for reasons of national security; - Using the internet in support of terrorism.	Up to 5 million Saudi Riyal (around US $1.3 million)	Not exceeding 10 years
- Creating websites that advocate drug use or that contain pornographic material; - Creating websites or programs that violate any of the Kingdom's general laws, Islamic values or public ethics.	Up to 3 million Saudi Riyals (around US $800,000)	Not exceeding 5 years
- Having accessed a network without authorization with the intention of changing or damaging its content.	Up to 3 million Saudi Riyals (around US $800,000)	Not exceeding 4 years
- Using websites to conduct fraudulent transactions	Up to 1 million Saudi Riyals (around US $260,000)	Not exceeding 3 years
- Having accessed a website without authorization with the intention of changing or damaging its content.	Up to 500,000 million Saudi Riyals (around US $130,000)	Not exceeding 1 year

5. Discussion

Saudi Arabia was ranked first as the most vulnerable of the Gulf countries to fall victim to cyber-crimes, such as website hacking, according to a statistics report recently. Cyber laws exist in the Kingdom since the year 2007, but its non awareness among youth has created potential imbalance between safe internet usage and vulnerability against crime. Most of the people know about cyber crime but very less is aware of the associated legislation to combat these crimes.

Therefore, in KSA it has been clear how computer crimes can affect people live especially for those financial crimes. Although, the information security is increased but also the unauthorized access for example were dramatically increased. Knowing the laws of computer crimes should be considered the first solution to reduce them.

6.Conclution

The Internet has presented a new challenge to humanity in facilitating crimes which have no boundaries and may be no evidence or trace. Muslims tend to relate to and adhere to Islamic teachings which instill the fear of God and hence the main conclusion of this research is to debate about non awareness of law and potential imbalance between Internet Usage & Awareness program in Kingdom. Cybercrime is on the rise across Saudi Arabia, and protecting against cyber threats is an ongoing management challenge for organizations in the country.

References

(alarabiya.net, 2013), Saudi Arabia says hackers sabotage government websites. Online available:

(arabnews,2012). Cybercrime costs Saudi Arabia SR 2.6 bn a year, online available: http://www.arabnews.com/saudi-arabia/cybercrime-costs-saudi-arabia-sr-26-bn-year (December 08-2013).

(sabaip.com, 2012), Saudi Arabia: Arab Cybercrime Agreement Approved, online available:

(symantic, 2oo8). Viruses that can cost you. Online Available: http://www.symantec.com/region/reg_eu/resources/virus_cost.html (November 12,2013).

(University of Nevada, 2012), Definition of Information Security. (online) Available: http://oit.unlv.edu/network-and-security/definition-information-security (november 10,2013)

(urnban dectionary, 2013), hacking. Online Available: http://www.urbandictionary.com/define.php?term=hacking (november 12,2013).

(CITC annual report, 2013). Annual report 2012, online available:

(Microsoft corporation, 2013). What is social engineering, online Available: http://www.microsoft.com/security/resources/socialengineering-whatis.aspx (November 17,2013).

(Spamhaus.org,2013) , "The Spamhaus Project - The Definition Of Spam". Online available: http://www.spamhaus.org/consumer/definition , (December 2,2013).

(thehackernews.com, 2012). Saudi Arabia king saud university database hacked, online available: http://thehackernews.com/2012/01/saudi-arabias-king-saud-university.html# (December 10,2013).

(worldexchangereport,2013).Onlineavailable[1])http://www.worldexchanges.org/files/statistics/pdf/IOSCO_WFE_Cybercrime%20report_Final_16July.pdf retrieved at December 07-2013.

Bocij, Paul (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. p. 14.

Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

http://english.alarabiya.net/en/media/2013/05/18/Saudi-Arabia-says-hackers-sabotage-government-websites.html (November 09 2013).

http://www.citc.gov.sa/English/MediaCenter/Annualreport/Documents/PR_REP_008Eng.pdf (December 07-2013).

http://www.sabaip.com/NewsArtDetails.aspx?ID=902., (December 11 2013).

In the proceeding of IEEE Security and Privacy, Los Alamitos, CA, USA: IEEE Computer Society; 8(2): 35‑44.

Matusitz, Jonathan (April 2005). "Cyberterrorism:". *American Foreign Policy Interests* **2**: 137–147.

Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Spitzberg, Brian H.; Hoobler, Gregory (February 2002). "Cyberstalking and the technologies of interpersonal terrorism". *New Media & Society*. 1 **4**: 71–92.

Van der Merwe, A J, Loock, M, Dabrowski, M. (2005), Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies, Cape Town, January 2005.

Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

Yuval F, Uri K, Yuval E, Shlomi D, and Chanan G. Google Android , (2010): A Comprehensive Security Assessment.