DOI: 10.5769/C2013005 or http://dx.doi.org/10.5769/C2013005

Cybercrime Investigation Challenges for Gulf Cooperation Council Governments: A Survey

Nasser Alalwan, Ahmed Alzahrani, Mohamed Sarrab

Abstract—***Computer crimes are criminal activities that involve the use of information technology. Modern life is increasingly relying on information technology; however, the more sensitive the information, such as government intelligence, credit card information or personal information the more important it is to improve the systems of computer crime investigation. Crime investigation helps detect illegal access to computer systems with the intent of deleting, modifying, damaging or stealing the data and information. Such activities may cause financial damages and may also result in publishing or destroying secret or confidential information. This survey study focuses mainly on highlighting the main challenges of the Gulf Cooperation Council (GCC) cybercrime investigation system and the need of information security laws in these particular countries. To achieve that personal knowledge, literature review and case study are used to complement and maintain the authors' statement about the challenges of cybercrime Investigation in GCC.***

Keywords- *Cybercrime; Computer Crime; Cybercrime investigation procedure.*

I. Introduction

The revolution of information technology and communication has increased the use of computer systems and networks. The marriage between the information technology and communication has increased the rate of the computer crime all over the world. In addition, with the increase of web applications, the sensitive and critical information become uncontrolled and more vulnerable. Computer crimes or any other digital crimes are criminal activities that involve the use of modern information technology. All aspects of our life have become increasingly relying on modern information technology. The more important the information, such as government intelligence, credit card information and any other private information the more important it is to improve the systems of computer crime investigation to detect any unauthorized access to a computer system with intent of deleting, changing or damaging computer data and information. An illegal access to the data or information in computer systems more potentially causes a financial damage in case of the manipulation or destroy of confidential information and secret or critical information. Computer crimes involve different types of activities such as machine misuse, digital frauds, system interference as well as unauthorized access and they might not necessary include any type of physical damage. Therefore, these different types of computer crimes and the rapid increase on the use of information technology make the work of computer crime investigator became very hard to detect and prevent any type of computer crimes. The issue is that the Arab gulf countries are in different stages of implementing electronic management such as E-government, E-commerce and E-business. For example, 51 cases of cyber-attacks were recorded in 2009 by the Telecommunications Regulatory Authority (TRA) targeting the UAE's information technology infrastructure which warranted the agency to issue the "devastating" effect [1]. The research value is raised from the rapid increase of the cybercrimes all over the world. Some countries have a good progress in the investigation procedures as well as in the law of cybercrime. Their investigators have a good experience in different types of computer crimes and the law in these countries protects the personal and government information. In each of these countries, the law provides criminal penalties for any identifying of the cybercrimes. This may cause other countries as a worth area for the criminal to steal or destroy any type of information. The purpose of this paper is to survey the cybercrime investigation challenges for GCC governments. To achieve that personal knowledge, literature review and case study are used to complement and maintain the authors' statement. The reminder of the paper is structured as follows. Sections II and III provide brief background about cybercrimes and introduce the cybercrime concept. Section IV discusses the state of information security in GCC. Section V and VI provide case study and its discussion respectively. In section VII the paper highlights the cchallenges of GCC cybercrime investigation system.

II. Backgroung

The advent of telecommunication and computer technologies has increased the number of users leading to an increase in cybercrimes such as hacking that causes a lot of damage via the computer. To protect data and information from cybercrimes, it is necessary to create a database to prevent unauthorized use based on confidentiality [2]. Cybercrime investigation is mostly similar to traditional crime investigation. Both have similar investigation procedure including (inspection, collecting evidences, investigations and analysing evidences). Moreover, in both types of crimes the investigators seek to answer the following key questions [3]. *What, When, Where, How, Who and Why?* However, cybercrimes have specific areas to deal with, such as computer machines, network, storage devices and other communication Medias. In addition, in computer crimes a huge record is very necessary to discover any available devices' manuals or any logging files [4, 5]. The most important step in cybercrimes is the strategic plan which is a long term plan that is concerned with national data network infrastructure [6]. Another important factor in cybercrimes investigation is the investigation team.

Creating investigation team with a good experience in computer machines, a data network and software tool is very hard to have one team with all these skills. The investigations team involves the team leader and the team members. The team leader should have a good experience in forensic and cybercrimes investigation [2]. Digital Forensics is the science of identifying, collecting, preserving, documenting, examining, analyzing and presenting evidence from computers, networks, and other electronic devices. It generally classifies and considers the digital evidence in a way that is officially acceptable by courts. Digital evidence contains the collection of several procedures of digital data [6, 7, 8]. Besides the strategic planning, the investigation team and the team leader are the cybercrimes' digital evidence. The digital evidence is an important part of the cybercrime investigation procedure which might include hardware, software, manuals, or phone numbers [9, 10, 11]. Many works have been done on the cybercrimes investigation [12, 13, 14] but to the best of our knowledge no work has been done in this particular area generally Gulf Cooperation Council countries.

III. Conceptualizing Cybercrime

Computer crimes can be defined as any criminal activities that are committed against a computer hardware machine. In computer crimes, the computer machine is used as a target of any type of criminal activities. The types of crimes are not only related to the data, information, software or any other program applications. The criminal activities in computer context is often refers to the computer functions; such as electronic mail and instant messaging services, social media applications, file transfer facilities and audio or visual conferencing programs, … etc. However, cybercrimes are any criminal activities committed using the computer, Internet or other electronic machines as the medium, in violation of existing laws. In other words cybercrimes can be defined as a type of crime that involves the use of computer technology, and for which penalties already exists under existing legislation. Fundamentally, there are no difference between generic individual crimes such as extortion, forgery, fraud, theft, impersonation and their cyber analogues. The cybercrime can also include the use of digital resources to commit any type of traditional crimes such as theft of identifiable card information and other forms of proprietary information or property in both digital and physical form [3, 5, 13, 15].

IV. State of information security In GCC

The state of cybercrime in the GCC is different from other countries all over the world, in which the state of information technology security in GCC and all Middle East regions is affected by many factors such as growth of IT user, IT infrastructure, and poor IT security system, lack of regulation and training of law enforcements.

- **Growth of IT user.**

With decrease cost of the broadband services in the region, the number of new IT users are growing daily and faster than other countries all over the world. According to Internet World Stats, Internet use in the Middle East had reached 2.5% of the total worldwide use by December 2007. Middle East use from 2000 to 2007 increased by 920.2% compared to 259.6% for rest of the world! [17, 18]. Internet World Stats 2013 shows that he growth rate of internet users in Middle East from 2000 to 2012 is 2,639.9%. Table 1 shows the world internet usage and population statistics in June 2012.

Table. 1. World Internet Usage And Population Statistics June 30, 2012

World Regions	Population (2012 Est.)	Internet Users Dec. 2000	Internet Users Latest Data	Growth 2000-2012
Africa	1,073,380,925	4,514,400	167,335,676	3,606.7 %
Asia	3,922,066,987	114,304,000	1,076,681,059	841.9 %
Europe	820,918,446	105,096,093	518,512,109	393.4 %
Middle East	223,608,203	3,284,800	90,000,455	2,639.9 %
North America	348,280,154	108,096,800	273,785,413	153.3 %
Latin America / Caribbean	593,688,638	18,068,919	254,915,745	1,310.8 %
Oceania / Australia	35,903,569	7,620,480	24,287,919	218.7 %
WORLD TOTAL	**7,017,846,922**	**360,985,492**	**2,405,518,376**	**566.4%**

This huge growth of number of users in Middle East has made the Internet more popular, supports the meaning of communication and opens a new online business opportunities. However, this growth in the number of users has increase the potential for IT abuse. Due to the lack of IT security policy enforcement, many Internet users have become victims of cybercrime attacks.

- **Information Technology infrastructure.**

The growth of overall investment in IT infrastructure in the Middle East is extensive, especially in GCC; but this IT infrastructure investment needs to do more in securing IT network infrastructure. In fact, over the past few years banks in the region have invest considerable budget to control the cybercrimes and securing online banking transactions. But, most banks in the region are still vulnerable to phishing attacks and hackers, which indicate that the GCC should invest more in IT security enforcement.

- Poor IT security system.

In all countries in Middle East region, especially in GCC there is a significant lack of security awareness and security policy enforcement among IT and online users. Comparing security awareness and security policy enforcement in the GCC to the other major players such as USA, Europe, China and Russia, there is a big gap between them in the less effort being made to raise awareness and security policy enforcement among IT users in GCC.

- **Lack of regulations and training of law enforcements.**

From the previous mentioned points, it becomes obvious that the GCC lack of regulations and training of law enforcements. These countries need strong security awareness training, targeting native speakers to educate users,

employees and law enforcers to understand the dangers and risks of attacks and hackers [17].

V. Case Study

The case study is about Saudi Arabian Oil Company (Saudi Aramco) where it confirmed the attack of its network occurred due to virus infection. Saudi Aramco is one of the largest energy and petroleum companies all ov ` e r the world. This virus attack could lead information stealing, destroy or any other financial damage. In that time, Symantec announced the discovery of a new malware called "W32. Disttrack" or "Shamoon". The malware infects a PC, steals certain data, send the data to another infected PC inside the compromised network and then overwrites the PC's Master Boot Record, which makes the system useless. The way this malware works might be linked to the Wiper malware which infected Iranian oil terminals in April 2012. The Wiper malware is also considered new variant of Flame as the investigation of the Wiper led to the discovery of Flame, according to Kaspersky Lab.

Kaspersky also provides new analysis of how Shamoon is coded. This type of malware might be used to physically access to a computer device that is connected to Saudi Aramco network then data and information propagation started. The infected device might not be inside Aramco but it can be connected with the company remotely from any other place. In this situation, Aramco needs to conduct thorough investigation to figure out from where this malware accessed their network not only focusing on the recovery from that attack. To identify the identity of the attacker a lot of work and collaboration needs to be done between GCC together and with other countries over the world specially the major players of the dangerous game such as USA, Europe, China and Russia [17, 19]. However, the important question after this Aramco attack is: Are we as GCC ready for the 21st century threats?

VI. Discussion

The paper focusses in this case of Saudi Aramco were the company's machines are infected with the Shamoon virus which requires Saudi Arabia to co-ordinate typical of state-sponsored attacks, and the targeting of critical infrastructure shortens the list of suspects. Another example of hacker attach in the region is the UAE's e-government sites that have been attacked by hackers, which caused financial loss and propagation of secret and confidential information to the public; Moreover, the famous channel news Al-Jazeera website is another example of a big name that has been hacked in the region.

In fact the investments in IT infrastructure have increased the value of e-business and e-governments and have increased and created great opportunities for small and medium businesses in the GCC, which helps with the unemployment problem. This lack of security awareness and security policy enforcement is one of the biggest problems inside IT companies in the GCC. Further, IT users and decision makers in GCC are not aware of the growth of the cybercrime problems. Poor security policy enforcement means that investments and chance to fight in the level of cybercrime are minimal which leaves the business across the GCC vulnerable to cybercrime or online attacks.

VII. Challenges Of GCC Cybercrime Investigation System

Despite the huge potential and many benefits that could be gained from improving cybercrime investigation system. There are still many challenges that face the improvement of cybercrime investigation including: Lack of comprehensive study on the main influencing factors of cybercrime investigation system in the GCC countries: to the best of our knowledge, there is no research study on the main factors/ barriers that influence the work of cybercrime investigators in GCC countries. One of the important factors is the cultural and social considerations such as user behaviors and the lack of knowledge in exchanging cybercrime between the gulf countries. Moreover, these countries are still in the earlier stages of their electronic management implementation, consequently, these countries might be seen by criminal to as a worth area to steal or destroy sensitive information. The following are the main challenges of the GCC cybercrime investigation system.

- Legislation, which may include the criminal offences, requirements to open an investigation, evidences, involvements of and shire knowledge with prosecutor and judge.
- Dedicated Units consist of legal framework, competence offices, field offices, trained and skilled officers, other necessary equipment and software applications.
- Criminal investigative procedures should allow computer access, internet interception, computer search, data preservation and supports procedure complaint and any other cybercrime related information and reports the case to the prosecutor. The procedure should support an investigation, surveillance, identifying IP and phone users and monitoring of phone conversation, internet data.
- Private sector cooperation should assist and exchange of information with the government related to cybercrime victim, evidence, knowledge, training, legislation, protocols, phone companies, banks, ... etc.
- International cooperation, countries all over the world should collaborate in exchanging of information related to cybercrime victims, evidence, public and private, mutual assistance request, contact points, joint investigation.
- Responsibility, In GCC there is big dilemma when discussing the cyberspace related laws. Due to the fact that there is no established cybercrime legislation in the region and there is absence of a government agency or department to be responsible for drafting or dealing with

cyber laws. It can be found that there are many agencies in the government might be involved in cyber related laws such as copyright, E-commerce, E-government, domain name registration and cybercrime. For example more than one government departments can involve in such situation like: Ministry of Interior, Ministry of ICT, Ministry of Justice, Ministry of Interior, Central Bank and even Intelligence and Defense departments. The issue is that any of the above mentioned authorities could claim responsibility of such laws which in fact the big challenge for GCC governments when discussing and drafting cybercrime law. It is very important to establish dedicated department in the government structure to deal with cyber laws. The UAE for example just started and appointed dedicated courts for cybercrime cases.

In addition, the most important challenge in the cybercrime investigation procedure is to understand the criminal activity and prove it [16].

VIII. Conclusion

The GCC are still in the earlier stages of their electronic management implementation. For these reasons, these countries' governments and organizations are concerned about the quality of their investigators and the cybercrimes investigation procedure itself. There is no doubt that the concept of cybercrime is feasible but this paper discussed the main challenges of the GCC cybercrime investigation system and highlighted the need of information security laws in these particular countries. This paper also focuses in the lake of cybercrime investigation experiences exchange between GCC.Therefore, there is a need for a comprehensive study of cybercrime investigation to address all issues and improve the cybercrime investigators procedure. This study should include an exploration of the work of the cybercrime investigators and identifying the types of cybercrimes in GCC. Finally, identifying the skills needed to improve the procedure of cybercrime investigation in GCC and according to their local user behaviour. Finally the study should end up with single information security law in GCC.

References

[1] B. Jay and B. Lubna, Cyber gangs on the prowl in UAE, gulfnews.com Al Nisr Publishing LLC. Online 2011.

[2] E. Timothy, "The field guide for investigating computer crime, part eight: Information discovery," Symantec, 2001.

[3] A. Bahar, Computer crime investigation, Master's thesis, De Montfort University, 2010.

[4] J. Richter, N. Kuntze, and C. Rudolph, "Securing Digital Evidence," in the Fifth International Workshop on Systematic Approaches to Digital Forensic Engineering. 2010.

[5] I. David and S. Karl S, Computer Crime: A Crime fighter's Handbook, OReilly Associates, Inc, Sebastopol, CA, 1995.

[6] V. Loia, M. Mattiucci, S. Senatore, and M. Veniero, "Computer Crime Investigation by means of Fuzzy Semantic Maps," in IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies, IEEE, 2009.

[7] S. Simundic, S. Franjic, and T. Susic, "Databases and Computer Crime," *52nd International Symposium ELMAR-2010*, pp. 195-201, September 2010

[8] H. Yousef, and A. Iqbal, "Digital Forensics Education in UAE," in the 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, UAE, 2011.

[9] A. Sammes, and B. Jenkinson, Forensic computing a practitioners guide, Springer Verlag, 2000.

[10] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 1st edition, 2000.

[11] E. Casey, "Error, uncertainty, and loss in digital evidence," International Journal of Digital Evidence, vol. 1, no. 2, 2002.

[12] S. McLean, "Basic considerations in investigating computer crime, executing computer search warrants and seizing high technology equipment," 14th BILETA Conference: CYBERSPACE. Crime, Criminal Justice and the Internet. 1999.

[13] C. Prosise, and K. Mandia, Incident Response: Investigating Computer Crime, Mcgraw-Hill Osborne Media, 2001.

[14] P. Stephenson, Investigating Computer Related Crime, CRC Press, Boca Raton, Florida, 1999.

[15] Warren B. Chik., (2011) "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore", Available online at www.law.ed.ac.uk/ahrc/complaw/docs/chik.doc visited 28 October, 2011

[16] S. Kabay, Computer Security handbook, Wiley, 2002.

[17] M. El-Guindy, Saudi Aramco cyber attack, are we ready Net Safe. Middle East, 2012. Availbe from http://netsafe.me/2012/08/27/saudi-aramco-cyber-attack-are-we-ready/#more-535

[18] Miniwats Marketing Group, Internet Seven Year Growth, Second Quarter Stats, Internet World Stats News, no. 028 - July, 2007.

[19] C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco", Survival: Global Politics and Strategy, vol. 55, no. 2, pp. 81–96, April 2013.