Network Security Challenges of CyberCrime Investigation in Oman

Nasim Al Balushi
Information Technology Department, Ibri College of Technology, Ibri, Sultanate of Oman
Email: Nasim.albalushi@ibrict.edu.om

Abstract— It is becoming increasingly difficult to imagine our life without the Internet. Despite the importance and benefits of the Internet, Internet connections are vulnerable to many threats; the number of phishing sites, spoofing of social networking sites and other attacks has increased annually. Therefore, the cybercrimes increase and the investigations for the crimes become a challenges for the investigators. It is a very necessary to figure out the difficulties of the investigation and to improve them, as cybercrimes can cause many damages or loss of sensitive information. Thus this paper focuses on the Challenges of Cyber Crime Investigation in Oman.

Keywords—Cybercrime, investigation, computer crime, network security

I. INTRODUCTION

In these years, there has been growing concern about computer crime investigation. The importance of network security has risen recently [1]. In one analysis, Al- Shaer (2006) argues that, because of the size and number of network users, attacks have dramatically increased; as a consequence, the challenges in investigating computer crime have raised [1]. computer crime means unauthorized access to computers to getting access to information available on the computer to browse or steal them. Sometimes, the purpose of the access may be to install malicious attacks such as worms, viruses, Trojan horse and etc. The person who do any one of the previous actions is called as a hacker [3].

II. AIMS AND OBJECTIVES

The topic of this research paper was selected for the following purposes: as the number of computer crimes is rising, a considerable amount of challenges faces to investigate the crimes and to design of an effective tool to parse the electronic crimes. Although the global electronic crimes index indicates that the Sultanate is the first among Arab countries in the field of cyber security and third globally, the number of blackmail cases are constantly increasing [2]. The main goal for this paper is to explore, analyze and understand the challenges of computer crime investigation in Oman. There are some challenges facing the investigation of computer crimes in Oman including the growth of IT users in Oman, lack of awareness and regulations relating to computer crimes and the awareness between the people about the security.

III. LITERATURE REVIEW

A. Threat Environment

A considerable amount of literature has been published on computer crime investigation. The newness of technology means that safety is also new, so the continuously growing demand in employing computer networks means that those machines will also be under a growing threat. Computers are prone to many types of threats at any time. Hackers and attackers are motivated to compromise computers. In addition, attackers have lots of methods and tools at their disposal to accomplish their purposes. The threat will be more serious if the goal is to attack critical information, for example, military or financial data.

B. Threat Environment in Oman

Recently, literature has emerged that offers lots of surveys, reports and statistics relating to information security in the Sultanate of Oman. Oman is exposed to a number of threats every year. The government of Oman and the Information Technology Authority play important roles in tracking these threats. The goal of the Information Technology Authority is to convert the Sultanate of Oman into a possible knowledge society by activating the role of information technology to enhance government and business services (Information Technology Authority report 2012). The figure below illustrates the types of IT security incidents that Oman is exposed to.

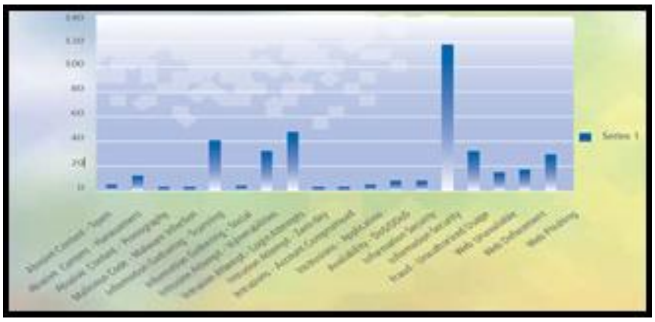


Fig. 1. Types of IT security incidents that Oman is exposed to

C.Information Security and computer Crimes in Oman Surveys such as that conducted by Information Technology Authority have shown that information security is vital. Oman National Center CERT's (OCERT) has discovered about 8,713 gaps in 2014.Also, they found about 537 seriously and real damaging malware infections and malware spreading targeting to and generated from Oman's cyber space. Furthermore, OCERT discovered about 288 digital forensics evidences in the same year. In addition; More than 269 blackmail incidents were noted in the Oman CERT since 2011 and 161 of which are occurred in 2016 only [7].

Table 1 shows the number of cyber security attacks that Oman has been exposed to during 2013. From the data given in Table 1, it is obvious that the months of May and June months witnessed the highest figures of attacks (about 2485 cases). The rate of security attack cases was more in July (1772 cases) than in November (1339 cases). In January, 1062 security attack cases were recorded. There were about 1661 cases in

April, compared to about 1733 cases in December. The lowest occurrences were recorded in November (about 149 cases) [8]. (OCERT) also discovered a noticeable increase in the number of security incidents in 2011 as compared to 2010, as Table 2 illustrates.

Table 1: Number of Cyber Security Attacks in 2013 (ITA 2013)

Month	Occurrences
Jan	1062
Feb	1078
Mar	1076
Apr	1661
May	2548
Jun	2548
Jul	1772
Aug	1484
Sep	969
Oct	1339
Nov	149
Dec	1733
Total	**17419**

Table 2: Statistics of Security Incidents during 2011(ITA 2013)

	Incidents Handled	Incidents Resolved	Inquiries/Helpdesk calls Handled
Q1	69	69	23
Q2	88	88	38
Q3	63	62	20
Q4	40	40	16

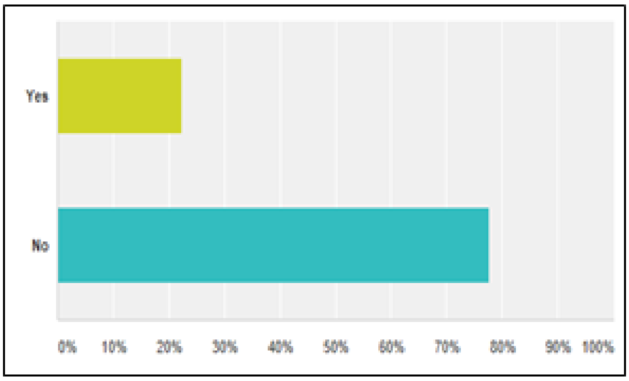


Fig. 2. Average hours the respondents spend on the internet every day

IV. RESEACH METHODOLOGY

There are a number of challenges need to be address in order to improve the level of the investigation for any cybercrime that face Sultanate of Oman. For this paper, quantitative research is implemented, online questionnaire about internet usage and security was distributed for about 60 persons. As the result of the questionnaire the following challenges for cybercrime investigation in Oman are extracted: Growth in IT users, lack of awareness and training about network security and about Oman cybercrime laws and regulations

A. *Growth in IT users*

Internet service entered to Oman in 1997, from that year the number of subscribers for internet services increased. During 2012, the penetration rate of the fixed internet subscribers increased by a 7.6%, bringing the total number of fixed internet subscribers close to 120,000[6]. Thus as number of users of the internet increase and the number of hours spend on the internet increase means the cybercrimes increase. As the result of the questionnaire, the graph shows most of the respondents spend more than 4 hours per day on the internet.

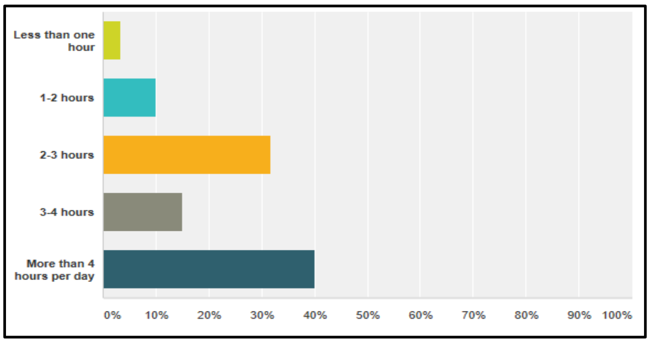
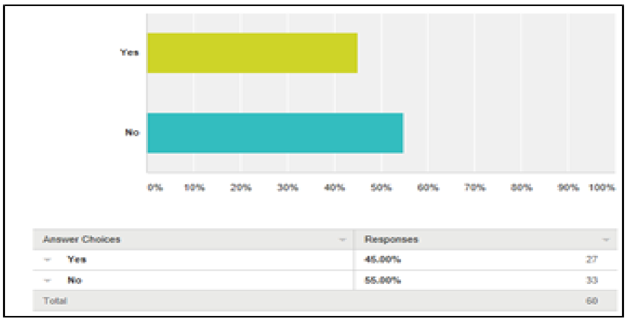


Fig. 3. Percentage of the respondents who have read and understood information security awareness

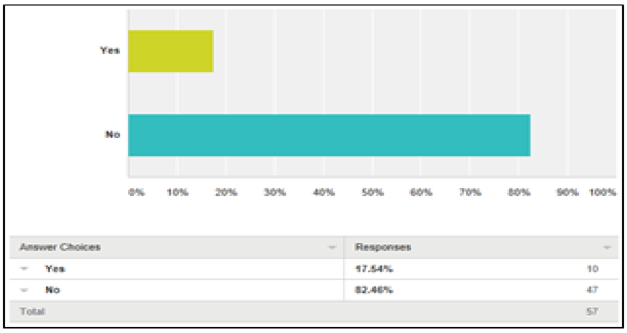
B. lack of awareness and training about network security

According to the following data that are taken from the questionnaire, it indicates that there is less awareness about network security, figure 3 shows that about 45.00% did not read any information about security. 55.00% of respondents did not receive any training that is related to information security as shown in figure 4.



Answer Choices	Responses	
Yes	45.00%	27
No	55.00%	33
Total		60

Fig. 4. Percentage of the respondents who received information security awareness training



Answer Choices	Responses	
Yes	17.54%	10
No	82.46%	47
Total		57

Fig. 5. Percentage of the respondents who have read and understood Oman cybercrime Laws and regulations

C. lack of awareness about Oman cybercrime laws and regulations According to the results of the questionnaire only 10 people out of 57 have read and understood Oman ybercrime Laws and regulations.

V. CONCLUSION

The aim of the present research was to examine the challenges of cybercrime investigations in Oman. This study has shown that there are three main challenges which are: growth in IT users, lack of awareness and training about network security and lack of awareness about Oman cybercrime laws and regulations. This research will serve as a base for future studies and more investigation about the topic of cybercrimes. In future also other paper about investigators skills can be publish. a Although the current study is based on a small sample of respondents, the findings suggest that beside the challenges the study has to focus the skills and knowledge that any computer crime investigator has to acquire; such as time management, critical thinking, concentration, and collecting and documenting evidence. A limitation of this study is that This research has thrown up many questions in need of further investigation.

References

[1] Al –Shaer, E. (2007) "Network security policies: verification, optimization and testing" IEEE/IFIP Operation and Management Conference.

[2] Hinson , 2016. Comments on "Security basics: definitions of threat, attack, andvulnerability". Available from: <http://peterhgregory.wordpress.com/2016/03/14/security-basics-definitions-of-threat attack-and-vulnerability> [Accessed 23 Febraruary 2017].

[3] Meier, J., Mackman, A., Dunner,M. and Vasireddy, S., 2003. Threat modeling. Available from: http://msdn.microsoft.com/en-us/library/ff648644.aspx [Accessed 23 Febraruary 2017].

[4] Wack, J., Cutler, K. and Pole, J., 2006. "*Guidelines on firewalls and firewall policy*". Available from: <http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf>[Accessed 22 Febraruary 2015].

[5] http://www.ita.gov.om/itaweb/CEO/CEO.aspx . [Accessed 24 Febraruary 2017].

[6] https://www.tra.gov.om/en/market/info/data-summary. [Accessed 24 November 2017].

[7] http://www.oman.om/wps/portal/ut/p/a0/04_Sj9CPykssy0xPLMnMz0vMAfGjDdwNDPwtPX1NnAJdDIy8jLxNgx2NjQyCTfSDE4v0C7IdFQHeH9ej/?WCM_GLOBAL_CONTEXT=/wps/wcm/connect/ar/site/home/gov/gov22/gov225[Accessed 24 Febraruary 2017].

[8] ITA, 2012. *Information and communication technology (ICT) survey results.* [Online] Available at: http://www.ita.gov.om/ITAPortal_AR/Media Center/ Document_Library.aspx > [24 Febraruary 2017].