International Journal of Information and Communication Technology Research

http://www.esjournals.org

An Overview on Cyber Security Awareness in Muslim Countries

Saeed S. Basamh, Hani A. Qudaih, Jamaludin Bin Ibrahim
Faculty of Information and Communication Technology,
International Islamic University Malaysia

ABSTRACT

Various cases of security breaches and attacks has been experienced globally, and high-level cases of cyber-attacks that threaten security has been documented. Attacks from various hacking groups have been conducted on organizations like the LuzSec, Stuxnet and many others that caused various levels of damages. Recent years have even seen groups that are anonymous in nature, targeting businesses that are highly profiled and other organizations. Some attacks have been conducted with much ease, thereby exposing the existing weaker systems of handling cybercrimes and some breaches have brought along very highly costs incurred on security. Countries have become very vulnerable in particular with the escalating levels of economy and the essential needs of improving infrastructure, in which has made them rely on technology and computer networks. Cyber threats can be categorized into two, and briefly they've been explained. This paper evaluates some instances of cyber-attacks in some of the Muslim countries like The Kingdom of Saudi Arabia (KSA), and the United Arab Emirates (UAE), the potential impacts and the possible recommendations that is implemented by governments, can help in raising awareness on cyber-attack issues.

Keywords: *Cyber Security, Awareness, Muslim Countries, Saudi Arabia, UAE.*

1. INTRODUCTION

1.1. Background Information

The global arena has experienced various cases of security breaches and attacks of malware over the last years. History has documented high level cases of cyber-attacks that threaten security conducted by malicious hacking groups like the LulzSec that attacked Sony Pictures where they took data that includes names, passwords, e-mail addresses, home addresses and dates of birth for thousands of people (Pepitone, 2011). There have also been cases of attacks on services of foreign intelligence where 24,000 files, stolen from the Pentagon defense contractor (Purewal, 2011). Recently, have even seen groups that are anonymous in nature, targeting businesses that are highly profiled and other organizations for cyber-attacks (Sindi, 2006).

Worth noting is that some of the attacks have been conducted with much ease, thus exposing the existing weaker systems of handling cybercrimes and the need to increase awareness on cases of cyber security. Such breaches in technology have brought along very high costs incurred on security by the relevant stakeholders, governments included. For instance, Sony Company experienced a consequent business loss of up to $171 million after the attack on the PlayStation (Hachman, 2011). In the United States, to be particular, cases of cyber security are on the rise due to the rapidly changing nature of technology (Battah & Hussain, 2011). This implies that those involved are advancing their cyber-attack tools quite in line with advanced technologies. As a result, countries, have become very vulnerable, especially with the escalating levels of the economy and the essential need to improve infrastructures. This has made them heavily rely on technology and computer networks through accessing the World Wide Web (WWW); hence any attempts to attack such massive computer networks have damaging results.

There is an increase in IT security incidents globally, mainly because of the Increase in electronic data, mobile devices, increase of organized cybercrime groups, of intelligent external and internal IT security threats, difficulty of tracing the attackers, and lack of adequate IT security knowledge among internet users. Furthermore, hackers are motivated by various reasons and some of these reasons are; to spread a political message, to gain financially (i.e. Theft), to steal information, to cause harm and disturbance, and to achieve self-satisfaction and esteem.

Cyber threats can be categorized into two groups; those that affect national whose emergence were as a result of the internet technology and the traditional activities of crime. Those from Internet Technology Development, include cases of cyber terrorism that are highly rampant in Muslim countries and the cyber theft of highly sensitive data. The traditional criminal activities, are those enhanced by computers like stealing intellectual property and sexual exploitation of young children online. This implies that both foreign and local organizations that deal with terrorists in Muslim countries are becoming encrypted to the use of technology so as to promote their communication and controlling the operations of the people (Ministry of Communication and Technology, 2007).

The Federal Bureau of Investigation must have the capacity to recognize and infiltrate the change and control components of these organizations and performers. The Stuxnet infection, for instance, pointed to modern control framework issues that hit the Iranian atomic program, affecting its uranium improvement program (Ahmad, 2011). On a more particular level, the cases of spying on the people's cellular telephones, voice-mails and their email accounts by journalists from a News International distribution have exposed the risk in cyber-attack on personal privacy.

1.2. Terms Definition

For long periods of time, the word, cyber security has often been perceived as a new concept with the components that are quite familiar with issues that deal with information security which has been utilized for many decades (Schreier *et al.*, 2013). Price

Water House Coopers, observe that the definitions of information security are highly variable due to the nature of wanting to protect the levels of confidentiality, high percentages of integrity and the consistent nature of available information, irrespective of the global status of the cyber security of information (2011). This paper analyze cyber security in two broad perspectives. The first is that cyber security includes the development of products and services for security applications. These are largely designed for government and military use, and are often referred to as cyber weapons or cyber defense. The second is the perception that cyber security is not only limited to the IT sector, but also deals with telecom's equipment.

2. THE GLOBAL MARKET SIZE AND FUTURE PROJECTED GROWTH OF CYBER SECURITY

Worldwide cyber security consumption was about $60 billion in 2011 and is required to develop approximately 10 per cent every year throughout the following Three-to-Five years (Europe, 2011). The US represents over 50 per cent of this sum total. The following biggest business sector is Japan, then the United Kingdom. In most nations, the private sectors represent the greater percentage of consumers of cyber security (Ahmad, 2011). The prominent special case is the US where government consumption is practically equivalent to that of the private sector. The fundamental drivers of the cyber security market are therefore geared towards: increasing the digital risks from cyber users, creating greater vulnerabilities because of the more pervasive utilization of engineering, especially versatile equipments and cloud computing. It also increases the cognizance value by which organizations and consumers are exposed to potential risks (Ministry of Communication and Technology, 2007).

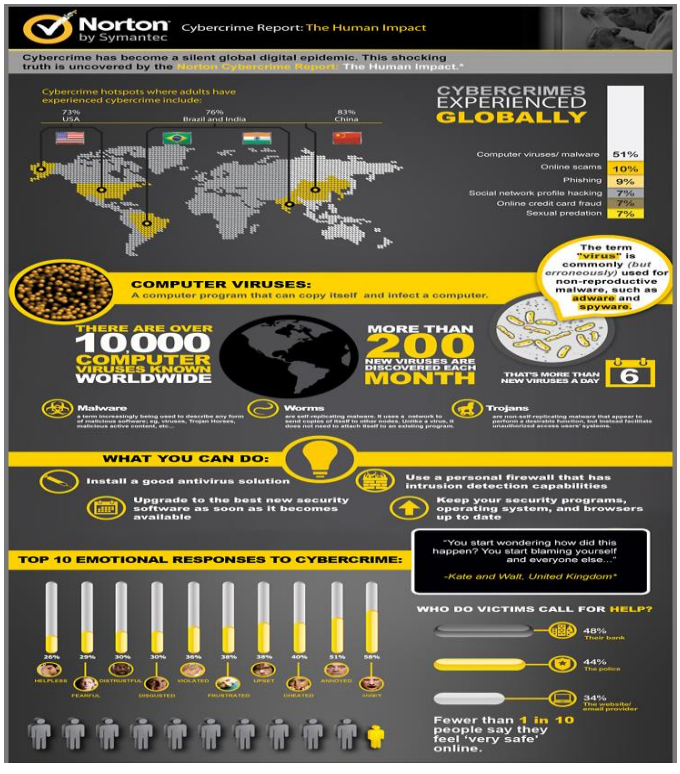

Figure: Cybercrime Report: The Human Impact (Norton by Symantec)

3. CASES OF REPORTED CYBER ATTACKS IN MUSLIM COUNTRIES

The regions within the Gulf and the Middle East have become the hotspots aimed for Internet crimes like cyber-attacks over recent years, in an era of computer-led warfare taking place all over the world. Cyber hackers who emanate from unspecified or unknown locations and countries have destroyed some of the most crucial data used in global security surveillance by countries. The data stolen is then used to plan attacks on financial institutions in countries (Sindi, 2006). Cases of cyber wars have been on higher end in Saudi Arabia and the UAE recently. The year 2009 marked one of the climaxes when a computer worm, Stuxnet was used to practice attacks on the Iranian nuclear facilities with the major goal of wanting to harm Iran's enrichment program of Uranium. Stuxnet nonetheless did not succeed in doing much damage as had been expected (SANs, 2013). Saudi Arabia was exposed to a similar situation when a series of its government websites were attacked including the interior ministry whose website crashed due to the massive requests of services received from an unidentified location (Reuters, 2013). Businesses, government agencies and critical infrastructure operators face unprecedented challenges from increasingly sophisticated cyber-attacks launched by criminals, hacker activists and foreign governments.

An attack had taken place in August 2012, which targeted the computer network of Saudi Aramco, the major company of oil and gas in Saudi Arabia. That attack used a computer virus known as Shamoon. A group named "Cutting Sword of Justice" claimed responsibility, said Saudi Aramco was the main source of income for the Saudi government. The virus channeled to this link caused an infection of about 30,000, workstations (Perlroff, 2012). Although this did not result in an oil spill, explosion or other manor fault in Aramco operations, the attack affected the business process of the company, and it is likely that some drilling and production data were lost, and causing the company to spend a week restoring their services (Bronk *et al.*, 2013).

In the Middle East, cyber criminals are increasingly targeting UAE residents with advanced hacking methods, one of which are phishing scams (Ghazal, 2010). In January 2010, several UAE bank websites were a target of phishing attacks, were compromised as reported by ITP, Middle East security expert confirmed that there was not only a major attack against that one UAE bank but a minor one against another local. About 72 per cent of phishing attacks last year, targeted customers of local banks, according to statistics from aeCERT, a UAE cybercrime task force. In phishing, cyber criminals attempt to dupe bank clients with emails resembling official bank requests for user names and passwords.

In April 2010, it was reported that several users lost their UAE bank savings through Internet fraud attacks (Aloul, 2010). The gang hacked into the systems of several unnamed credit card processing companies, and used stolen card data to create counterfeit cards to withdraw cash from ATMs in as many as 27 countries, according to authorities in the US. The hackers increased the available balance and withdrawal limits on prepaid MasterCard debit cards issued by the Bank Muscat of Oman, and National Bank of Ras Al Khaimah (RAKBANK) of the United Arab Emirates. Card data was then distributed to

gangs in target countries, who used faked cards to withdraw large volumes of cash in two co-ordinated attacks. Causing theft about $45 million from the Muscat and RAK Banks (Sutton, 2013).

4. STATE OF CYBER SECURITY IN MUSLIM COUNTRIES

Individuals with hidden agenda or malicious intentions like promoting terrorism have sustained constant cyber-attacks in the Middle East and across the globe. This creates the need to further protect computer systems that often provide essential support for the management of operations and other infrastructures. Such concerns have been raised based on profound reasons that online cases of insecurities have been on the rise through hacking. Just like the other large organizations, government agencies heavily rely on systems that have been computerized to support electronic data. Likewise, the security of these frameworks and information is crucial to avoid operation disruptions, and help in preventing cases of information altering, deceiving, and indelicate revelation of highly sensitive data. Securing the machine frameworks that underpin the country's cyber security operations and foundations has never been more essential than it is in the modern day.

Telecommunications, power conveyance, water supply, the health of the public members, leadership and national defense, law authorization, the taxpayer supported organizations, and crisis responses are all hinged upon the security of their computer networks and operations. Yet with this reliance comes an expanding worry about ambushes from the people and anonymous groups that have malicious plans like wrongdoing, terrorism, intelligence information gathering from foreign countries and demonstrations of war (SANs, 2013). Such concerns are established based on various explanations, incorporating the cases of cyber securities that have been reported, accessibility to hacking tools, the simplicity of getting and utilizing hacking devices, the consistent development in the advancement of technology and innovation, and the impending warnings of new and more even more disastrous in attacks online.

The dramatic nature of increased inter-connectivity among personal computers, particularly in the utilization of the Internet, continues to alter the way the governments of the Muslim nations and a great part of the world impart and conduct business. The profits have been tremendous. Massive amounts of data are presently at our fingertips, thus expediting research on practically each theme that requires understanding; fiscal and different business transactions might be executed instantly and electronic mail permit us to communicate rapidly and effectively with an unrestricted number of people and groups within the Middle East region and across the countries.

5. CONCLUSION

The challenge of cyber security is here to stay put and thus governments in the Muslim nations must strive to develop policies and structures to encounter such threats. They could work to develop laboratories as done in the US' Iowa state to simulate, the investigation process of cyber-attacks via Internet. It is also worth noting that the nature of cyber security is becoming sophisticated compared to the traditional forms. This means that researchers must work to ensure they discover the actual complexities that pertain to cyber security through Internet.

6. RECOMMENDATIONS ON MEASURES TO INCREASE AWARENESS OF CYBER SECURITY IN MUSLIM COUNTRIES

Certain measures can be put in place by the governments of the Muslim nations to ensure that cases of cyber security are minimized and controlled in the near future (Jim, 2005):

i. Reviewing the existing legal systems of technology to determine whether they are criminalized in the appropriate way to qualify as a case of abuse made intentionally to the telecommunications systems and computer networks. This will eventually help towards the promotion of investigating cyber crimes.

ii. Countries should make considerations on issues that pertain to high-tech related crimes appropriately whenever conducting the negotiations of mutual agreements.

iii. The Islamic nations must continuously examine and make workable solutions that are in regards to; preserving evidence before executing a request for assistance. This can be achieved through conducting searches across borders and data searches from unknown data locations.

iv. Countries must develop the relevant protocols needed to obtain the traffic data brought forth from the channels of communications. Methods should be devised to ensure an expedition in the process of transferring the data internationally.

v. It is recommended that the appropriate agencies of these Muslim governments must work together with the ICT industry to ensure the developed new technologies are tailor made to combat the high-tech levels of crime through the collection and preserving of the required evidence.

vi. Certain elements to ensure workable solutions must also be put in place by the Muslim governments. These include; ensuring that the freedoms and private

lives of people are well protected, making sure that the ability of the government to fight cyber high tech crime is preserved, and providing training to all stakeholders and the public to empower the masses, to clearly define an appropriate and transparent framework that is needed to address the challenge of cybercrime.

REFERENCES

[1]. Ahmad, A. (2011). Type of security threats and its prevention. *International Journal of Computer Technology & Applications*, *3*(2), 750-752. Retrieved from http://ijcta.com/documents/volumes/vol3issue2/ijcta2012030240.pdf

[2]. Aloul, F. A. (2010, November). Information security awareness in UAE: A survey paper. In Internet Technology and Secured Transactions (ICITST), 2010 International Conference for (pp. 1-6). IEEE.

[3]. Battah, F., & Hussain, A. (2011). Enhancing information systems security in educational organizations in KSA through proposing security model. *International Journal of Computer Science Issues*, *8*(5), Retrieved from http://ijcsi.org/papers/IJCSI-8-5-3-354-358.pdf

[4]. Bronk, C., & Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. Survival, 55(2), 81-96.

[5]. Europe, I. (2011). Big boost in cyber-security spending. Network Security.

[6]. Ghazal, R. (2010, May 19). UAE vulnerable to cyber attacks, Bush adviser says. Retrieved October 26, 2013, from TheNational: http://www.thenational.ae/news/uae-news/uae-vulnerable-to-cyber-attacks-bush-adviser-says

[7]. Hachman, M. (2011, May 23). PlayStation Hack to Cost Sony $171M; Quake Costs Far Higher. Retrieved November 02, 2013, from PCMAG: http://www.pcmag.com/article2/0,2817,2385790,00.asp

[8]. Jim, K. (2005). Combating cyber crime and cyber terrorism. Retrieved from http://www.worldsecuritynetwork.com/Other/Kouri-Jim-1/Combating-Cyber-Crime-and-Cyber-Terrorism

[9]. Ministry of Communication and Technology. (2007). Developing national information security strategy for the kingdom of Saudi Arabia. Retrieved from http://www.mcit.gov.sa/NR/rdonlyres/514E7B51-5710-46D9-9EC5-2D78BC2E1219/0/NISS_Draft_7_EN.pdf

[10]. Pepitone, J. (2011, June 02). Group claims fresh hack of 1 million Sony accounts. Retrieved October 25, 2013, from CNNMoney: http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/

[11]. Perlroff, N. (2012). Connecting the Dots After Cyberattack on Saudi Aramco. New York Times.

[12]. Price Water House Coopers. (2011). Cyber security M &A decoding deals in the global cyber security industry. Retrieved from http://www.pwc.com/en_GX/gx/aerospace-defense/pdf/cyber-security-mergers-acquisitions.pdf

[13]. Purewal, S. (2011, June 15). 24,000 Pentagon Files Stolen in Major Cyberattack. Retrieved November 02, 2013, from PCWorld: http://www.pcworld.com/article/235816/Pentagon_Files_Stolen_in_Major_Cyberattack.html

[14]. Reuters. (2013, May 18). Saudi Arabia faces major cyber attack. Retrieved October 25, 2013, from Gulf News: http://gulfnews.com/news/gulf/saudi-arabia/saudi-arabia-faces-major-cyber-attack-1.1184977

[15]. SANS. (2013, January 31). Interest in cyber security on the increase across the Middle East and gulf region says expert. Retrieved November 03, 2013, from SANS: https://www.sans.org/press/interest-in-cyber-security-increase-across-middle-east-and-gulf-region.php

[16]. Schreier, F., Weekes, B., & Winkler, T. H. (2011). Cyber Security: The Road Ahead. The Geneva Centre for the Democratic Control of Armed Forces.

[17]. Sindi, A. (2006). Cyber security initiatives in Saudi Arabia. Retrieved from http://www.itu.int/osg/spu/cybersecurity/2006/presentations/sindi-saudi-arabia.pdf

[18]. Sutton, M. (2013, May 10). Cyber attacks rob $45m from Gulf Banks. Retrieved October 30, 2013, from ITP: http://www.itp.net/593259-cyber-attacks-rob-45m-from-gulf-banks#.UoCzKZEUXFI