A Critical Analysis of the Effectiveness of Cyber Security Defenses in UAE Government Agencies

Abdulla Al Neaimi, Tago Ranginya, Philip Lutaaya
SecureTech, LLC, UAE
alneaimi@gmail.com, tago.ranginya@gmail.com, lutaphilo@gmail.com

Abstract: Cyberspace has become the new frontier for countries to demonstrate power. Nations that have developed defense tools or those that can successfully launch attacks against adversaries will become the next global superpowers [1], [2]. While cyber threats and attacks by government agencies are well documented, most widespread attacks are done by individuals or hacking groups for personal gains [3], [4]. The UAE has become a major target for cyber conflicts due to increased economic activity, tourism, technology and rise of the oil and gas industry. Furthermore, the wide spread of internet in the region to the tune of 88% has exposed it to attackers [3]. Recent attacks against Saudi Arabia's ARAMCO and Qatar RasGas and the Stuxnet attack on the Iranian nuclear plants are often cited as examples [3], [5].

Previous reports show that the UAE Government is set to double expenditure on homeland security [6]. Therefore, we need to assess whether available cyber-security defenses are effective and guarantee comprehensive cybersecurity strategies that would uphold the highest security standards in line with the vision 2030. In this paper, a critical review of the existing cyber security mechanisms has been done and a framework for effective management of cyber security threats proposed for the UAE government agencies.

Keywords: United Arab Emirates (UAE), Cyberspace, Cybersecurity, Cyber-attacks, and Security Framework.

1.1 INTRODUCTION

In the world today, cyberspace has become part of the daily life of many people in different societies including industry and Government agencies. The Continued development of Information and Communication Technologies (ICT), Social media, internet shopping, and online banking has created a powerful economy while enabling borderless exchange of information and media [2].

Furthermore, several attacks like malware, phishing, corrupted programs, password manipulation, computer session hijacking and denial of service have increased massively in the UAE and the Gulf region. Among such attacks include the August, 2012 attack which affected the major oil and gas company in Saudi Arabia company ARAMCO, the Stuxnet worm of 2009 that targeted the Programmable Logical Controllers (PLC) of the Iranian nuclear industry; the Lulzec Sony pictures attack that took bio data of many people [7], [8], the Shamoon Virus that infected over thirty thousand (30,000) stations and destructed business processes for almost a week, among others [9]. The increase in IT security attacks on vital government and industrial data could partially be attributed to the vast amounts of data available in data centers, increased number of mobile subscribers and massive internet connectivity. Furthermore, attackers have improved their levels of organization and research especially in the area of cloud security, yet most of the next generation networks would use it as a hub for data storage. The cyber criminals have also been highly motivated by the recent political instabilities in the Arab region and financial support from some Islamic groups.

Saeed et al [3], categorized cyber threats into two groups; those whose emergency resulted from Internet or the traditional activities of crime and others from Internet technology development, for

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

example, cases of cyber terrorism and cyber theft of highly sensitive data and traditional criminal activities enhanced by computers like stealing intellectual property and sexual exploitation of young children online among others. The authors further argue that the UAE residents are a major target for phishing scams. It is therefore, of utmost importance to devise strategies that can be used to combat the cyber security related challenges in the UAE public and private sector agencies as well as protecting the massive innocent citizens online. The rest of the paper is organized as follows; section II provides a detailed study of the existing cyber security attacks and defense mechanisms globally and the UAE region in particular, section III critically looks at the challenges of cyber security defense, Section IV proposes a framework for cyber security defense in the UAE, while section V and VI provide a discussion of the proposed framework, conclusions and future work respectively.

1.2 STUDY BACKGROUND

The cyber security problem has been discussed so much in literature over the recent years, for example Aloul [10], reported that in 2010 several users lost their UAE Bank savings through internet fraud. Hackers succeeded in stealing ATM and credit card data from processing companies and adjusted available balances on these accounts. These cards were later distributed to other hackers in target countries to withdraw large volumes of cash. The authors suggested some of the measures for increasing Cyber security awareness in middle eastern countries including the UAE, for instance, by proposing a review of the existing legal system of technology, making workable solutions in regards to preservation of evidence, developing protocols to obtain traffic data, cooperation with ICT industry in developing new technologies to combat hi-tech levels of crime, among others.

The national security awareness campaigns launched in November, 2007 by the aeCERT to protect online information and to provide online identity platform has tried to safeguard some of the government critical information by blocking some of the immoral websites from access within the region. This has temporarily reduced the issue of child abuse and pornography. For instance on 22nd, July, 2013 the Telecommunications Regulatory Authority (TRA) successfully defended a series of cyber-attacks that targeted some government websites. The Computer Emergency Response Team aeCERT managed to neutralize the problem with minimal damage [11]. However, popups, phishing threats, denial of service, ignorance of users about security threats among others remain a major challenge.

The Symantec Report, 2013 on UAE, looks at the extent of the cyber threats in the region. It claims that 17% of People in UAE have been victims of cyber threats, however, we have no analytical results to prove this validity. An extensive study is necessary in UAE to prove this validity [12].

Meanwhile, Rogers et al [4] argue that real time threats are more sophisticated and so require continuous monitoring by government and all other stake holders due to massive threat to data and proprietary information. Much as governments are trying to keep pace with these threats they have not integrated their security strategies to provide a more complex solution to cyber-attacks. These ever increasing information security threats call for the development of complex cyber security defenses for the UAE government agencies and the entire GCC region.

Fadi et al [13], looked at the security concerns of the UAE traditional electrical power grid that will soon evolve into a smart Grid system. They analyzed the vulnerabilities and looked at the current and needed security solutions. One major concern is the under construction Barakah Nuclear power plant that is set to be completed by the year

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

2020 to raise the region's power output voltage from 15.5 Gwe to about 40 Gwe. Power Grids normally face attacks on intelligent devices and physical connections attacks like IP spoofing and denial of service attacks. Therefore, if the UAE grid falls under a cyber-attack it would pose a very big danger and loss to the government.

Furthermore, Kaist et al [14], accentuates that nuclear power plants are very important infrastructures for providing efficient and non-interrupted electricity, therefore require continuous government vigilance and protection. The use of such digitized systems brings new vulnerabilities and threats over the cyber space since they are more dependent on software and networks.

Michael and David [15], provided an insight into enhancing cyber security workforce, they propose the need to devise ways of building professionals who can build, manage and secure reliable digital infrastructures and effectively identify plans blended for threats. They presented a model for developing the next generation cyber workforce which combines assessments, simulations, customization and support systems**.** However, we are not sure if their model can be applied to the UAE Government Agencies since it is not effective for interconnected networks. We need to put in place a framework that can aid the UAE interconnected network systems to jointly detect and control cyber threats and this is the major contribution of this paper.

Meanwhile, the United Nations Institute for Disarmament Research report, 2013, claims that Government efforts to protect infrastructure and undertake law enforcement in the cyber sphere are complicated by the fact that most infrastructure and assets involved are owned and operated by private sector actors with diverse motivations and competing equities to protect. This complicates the legislation process for instance civil liberties are majorly concerned about protecting people's rights than protecting the privacy of people online [1]. Therefore, we need to incorporate cultural sensitive training and awareness programmes in the UAE cyber security framework such that private sector actors and other citizens understand why the must be protected online.

Cyber-attacks can seriously disrupt or even paralyze segments of critical national infrastructure, (NIST Report, 2014), therefore, a military like defensive or offensive posture or action may be required. Appropriate strategic management theories and principles are needed that guide the control and prevention of these attacks [16]. The NIST report claims that the Executive Order by the USA President calls for the development of a voluntary risk-based Cybersecurity Framework which involves a set of industry standards and a set of best practices to help organizations manage cybersecurity risks. The resulting Framework, was created through collaboration between government and the private sector and uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses, [16];

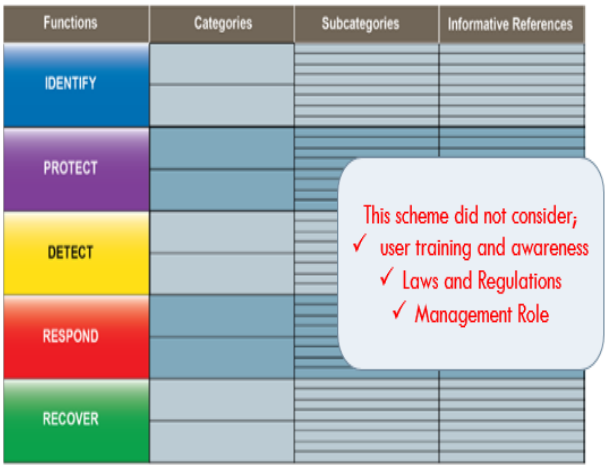

Fig1: Illustration of NIST cyber security Framework. Source: NIST Report, 2014.

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

From Fig1 above the NIST framework majorly focused on business drivers that drive Cyber security activities and considered Cyber security risk as part of the organization's risk assessment process. However, this framework did not consider other important aspects of cyber terrorism like cultural sensitive user training and awareness, strict laws and regulations and the critical management role in the prevention of cyber-attacks in major government agencies.
We need to embed this technological framework into other strategies and provide a more robust and all inclusive framework for the UAE Cyber security. The Framework needs to be a living document that will continually be reviewed and updated as industry, community, researchers, the defense among others provide feedback on implementation.

As organizations expand their use of advanced security technologies, hackers attempt to break into their security by using the weakest security link or the less-informed computer user [17]. Users are the biggest security threat in IT-Security of any organization, therefore, continuous cultural sensitive training and awareness programs are required to change their perception of information security. Furthermore, cultural change in the operations of government employees is needed to make IT security and the ethical use of the state IT resources as ubiquitous as technology since it involves changing the way state employees perceive IT Security. In [18] a comprehensive survey on wireless networks was carried out on thousands of access points in Dubai and Sharjah Emirates in 2008 and 2010, the results of the survey showed that most of them where either unprotected or used the weakest protection techniques. The results showed that 32% of the access points were unprotected while the others used weak security encryption techniques. Such weak security protocols placed on internet access points or lack of any expose the people to all forms of cyber threats.

A good national identification infrastructure can help the government to obtain credentials of cyber enemies. The UAE government established a strong identity management infrastructure (Emirates ID) to enhance homeland security [19]. The smart identity card comprises security parameters stored on an embedded chip together with a person's physical identity. This has enabled secure e-Government transactions and monitoring of the influx of foreign worker's since it links a person's electronic identity and attributes which can be stored across a single distinct identity management systems [20]. The government needs to improve the security features on both the emirates and labour cards given to avoid any form forgery by incorporating temper proof RFID features on the cards.

Application of strategic management tools to prepare for and respond to the uncertainties presented by cybersecurity risks against UAE government agencies raises awareness of the risks among senior employees which then leads to actions being taken organizationally to prevent these attacks. Since cybersecurity attacks are usually against critical national infrastructures, senior management takes the responsibility to demonstrate both "due care" and "due diligence" as established in the Federal Law No (2) of 2012 [27]. This law requires preventive measures be taken to avert and respond to cyber-attacks against national infrastructures.

1.3 CHALLENGES TO THE EFFECTIVENESS OF CYBER SECURITY DEFENSES

The 2012 ITU report revealed a number of challenges in the prevention of cybercrime globally [21], such challenges include but not limited to over reliance of ICTs for the control and management of security functions in buildings, cars, aviation services, water and energy supply which has made the systems more vulnerable to cyber-attacks. Other challenges include an

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

overwhelming increase in the number of internet users to over 2 billion by 2010 world-wide. In the UAE, for instance 66% of the UAE households are already connected to broadband internet, (TRA-survey, 2014). The availability of up to date information on major platforms like Wikipedia provides cyber terrorists with massive data to exploit systems makes it difficult to draft national criminal laws for investigation and prosecution of cyber criminals. Such information has been a major threat leading to attacks on critical government infrastructures like central banks [22], [23]. While there are delays in establishing regulations that would respond to threats against new technologies as they emerge, attackers are able to quickly adjust their techniques to suit any technological advancements. The UAE Government, therefore needs to put in place strong research groups in the area of cyber and cloud security to combat the next generation cyber-attacks in the region. Authors in [24], argue that whereas it is cheap to mobilize cyber-attacks, technologies for guarding against such crimes are becoming more and more expensive. This implies that the war against cybercrime needs to be jointly handled by all stakeholders in the UAE region with major support from Government. Furthermore, the problem can be eliminated by a combination of defensive technology, continuous in depth analysis, traditional diplomacy and cultural sensitive cyber security training and awareness programs. More still top management in the different government agencies especially at C-level need to be very vigilant in the planning stages for their organizations by incorporating cyber security in their strategic plans.

1.4 FRAMEWORK FOR THE EFFECTIVENESS OF CYBER SECURITY DEFENSES IN THE UAE.

In this paper we present a framework that can be used for the effective evaluation of cyber security defenses in the UAE government agencies. The proposed framework is based on a critical review of the existing mechanisms and strategies available in literature as well as proposing new strategies that suite the region.

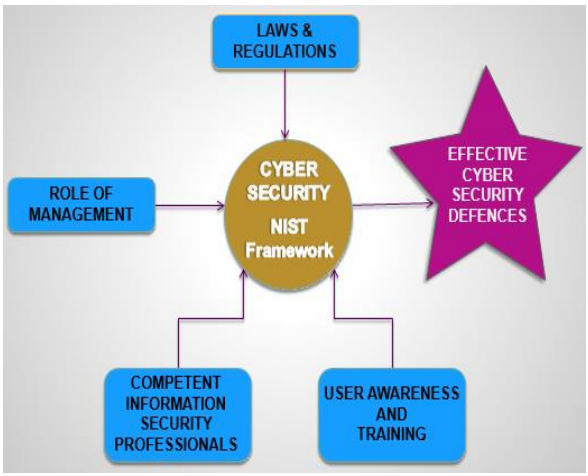

Fig 2: Proposed Framework for Cyber security defense in the UAE government agencies.

1.5 DISCUSSIONS

From Fig 2 above, the NIST framework has been integrated within the developed design to provide the technological capabilities within the new framework. Therefore, we propose a hybrid framework that provides for advanced technology accompanied by culturally sensitive Training and Awareness Programs, Competent Information Security Professionals, enforceable Laws and Regulations as well as strong senior Management Role (support) in cyber security.

a) Role of Management

The prevention of cyber-criminal activities is considered a strategic issue in both private and public sectors. It is therefore important that management in all UAE government agencies incorporates cyber security into the planning and budgeting processes of the organization. The plans need to deal with turbulent or unpredictable

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

situations that would arise following a cyber-attack.

b) Competent Information Security Professionals.

The UAE government needs to build a very strong workforce in area of information security and cyber security by equipping a selected number of people with appropriate skills through tailor made training programmes. Furthermore, emphasis needs to be put on research to ensure readiness of the trained personnel in case technological changes occur. The government can also apply the Training of Trainers (TOTs) method to increase the number of these skilled personnel by investing heavily in the lead trainers who can later train others in a culturally sensitive approach. Local post-secondary and university curriculum needs to be revised from time to time to meet the ever changing demands of cyber-attacks. This can possible by availing a research grant in the area of cloud and cyber security to enhance innovation and continued supply of strong information security professionals, protocols and standards.

c) Laws and Regulations

Regulatory frameworks are necessary in ensuring that the public and critical national interests are protected. National laws on privacy, integrity and confidentiality of personal information and data provided to financial, health and government agencies can only be enforced by ensuring compliance of the different agencies. In the case of the UAE, it was not until 2006 that the UAE Federal government came with a law against cybercrime. The Federal Law No. (2), 2006 on - the Prevention of Information Technology Crimes (English) came into existence at a time when issues of information security were being recognized as a global issue that required each country to put in place such laws. This law was further updated in 2012 [3]. The government needs to be more vigilant in the implementation of these laws and at the same time review the legislations annually to ensure that next generation threats are incorporated in national security frameworks and planning documents.

d) Training and Awareness

Evidence has been provided in the literature about the importance of user training and awareness as a factor in cyber-security effectiveness. An organization might have implemented the best technology that is supported by the most experienced technical team but without effective user awareness and training programs. In such situations its cyber-security programs will still fall short. The actions of a single user can compromise the data and infrastructure of the entire organization. Successful cultural sensitive user training and awareness programs will have the following results:

i. Users that are committed to the use of strong passwords as a matter of routine.
ii. Users that exhibit behaviors and attitudes that are aligned to the organizations overall cyber-security policies and procedures.
iii. Users who possess a general common sense in their security behavior such as: not opening email attachments with executables; backing up their important files; connecting personal devices such as smartphones and other devices to corporate networks; emailing a highly sensitive document outside the organization.
iv. Citizens who value the pride of their nation and critical national infrastructure among others.

All these four discussed strategies together with the NIST technological framework contribute a strong combined framework that can be used to ensure effective cyber security defense in the UAE government agencies.

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com

1.6 CONCLUSION

In this paper, a framework for effective cyber security defenses in the UAE government agencies has been proposed. The proposed framework merges technological defenses together with strict legislation, strong management responsibility especially in planning and analysis of critical issues as well as establishment of cultural sensitive training and awareness programmes. However, the cyber security issue still remains a very expensive global concern that requires strong cooperation from all stakeholders in UAE and globally. In future we intend to study role of culture in the design of effective cyber security training and awareness programmes and also critically analyze the cyber security problem in the entire Gulf Cooperation Council.

REFERENCES

[1] James Andrew Lewis and Gotz Neuneck, United Nations Institute for Disarmament Research (UNIDIR) Report, "The cyber index, International Security Trends and Realities", Center for strategic and International Studies, 2013, http://www.unidir.org

[2] James Andrew Lewis, Center of Strategic and International Studies (CSIS), Middle East Programme Report, 2014.

[3] Saeed S. Basamh, Hani A. Qudaih, Jamaludin Bin Ibrahim, An Overview on Cyber Security Awareness in Muslim Countries, International Journal of Information and Communication Technology Research, 2014.

[4] Roger Cressey and Mahir Hayfer, Cyber capability in the Middle East, Seizing opportunity while managing Risk in Digital age, Booz Allen Hamilton, 2012

[5] Pepitone, J. (2011, June 02). Group claims fresh hack of 1 million Sony accounts. Retrieved July 15, 2014, from CNN Money:http://money.cnn.com/2011/06/02/technology/sony_lulz_hack/.

[6] GulfNews;URL:http://gulfnews.com/news/gulf/uae/general/uae-to-invest-10-billion-in-10-years-for-homeland-security, Retreived on 02/09/2014

[7] Internet Society Global Internet Report, Open and sustainable access for all, 2014.

[8] Al-Bawaba (2012). "Cyber-crime laws in the UAE are dangerously vague".

[9] Perlroff, N, Connecting the Dots after Cyber-attack on Saudi Aramco, 2012, New York Times.

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

[11] UAE Computer Emergency Response Team Website, (ae CERT), http://www.aecert.ae/index-en.php

[12] Symantec (2012). Internet Security Threat Report 2013, Symantec. 18.

[13] Fadi Aloul , A. R. Al-Ali , Rami Al-Dalky, Mamoun Al-Mardini and Wassim El-Hajj, "*Smart Grid Security: Threats, Vulnerabilities and Solutions*", International Journal of Smart Grid and Clean Energy, Department of Computer Science American University of Sharjah, UAE, 2012

[14] Kwangjo Kim and KAIST Daejeon, "Challenges of Cyber Security for Nuclear Power Plants", Khalifa University of Science, Technology and Research, Abu Dhabi, UAE, The 18th Pacific Basin Nuclear Conference (PBNC 2012), BEXCO, Busan, Korea

[15] Michael J. Assante and David H. Tobey, "Enhancing Cyber Security workforce", IEEE Computer Society, 2011.

[16] National Institute of Standards and Technology NIST, (Feb, 2014), Framework for Improving Critical Infrastructure Cybersecurity.

[17] Mary Gay (MG) Whitmer, IT Security Awareness and Training, Changing the culture of state government, 2007.

[18] Katz. F, The effect of a University Information Security Survey on instructing methods in Information Security, 2005

www.manaraa.com

[19] Roebuck, k, Federated ID Management, Tebbo Publishing, 2011.

[20] Ali M. Al-Khouri,(PhD), e-Government Strategies, The Case of the United Arab Emirates (UAE), European journal of e-practice, 2012 · ISSN: 1988-625X

[21] Prof. Dr. Marco Gercke, Understanding cybercrime: Phenomena, challenges and legal response, 2012,www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[22] Reuters (2012). "UAE central bank thwarts attempt to-hack-website." http://www.haaretz.com/news/middle-east/uae-central-bank-thwarts-attempt-to-hack-website-1.408645.

[23] UAE Telecommunication Regulatory Authority web portal, http://www.tra.gov.ae/national-emergency-plan.php

[24] Elbanna, S. (2010). "Strategic Planning in the United Arab Emirates." International Journal of Commerce and Management, Vol 20, 1: 26-40.

[25] Hunter, G. S. (2013). "Fresh calls for tighter UAE banking regulations in wake of $45m cyber heist". Retrieved July 25, 2014, from http://www.thenational.ae/business/industry-insights/finance/fresh-calls-for-tighter-uae-banking-regulations-in-wake-of-45m-cyber-heist#ixzz2qRl09jRz

[26] Robert Burgers, Hans Baars, Maurice Adriaensen and Atif Raja, Middle East needs cyber security from within Utilities face energy threat, DNV KEMA Energy & Sustainability, 2013.

[27] Al-Bawaba, "Cybercrime laws in the UAE are dangerously vague", 2012.

ISBN: 978-1-941968-01-7 ©2014 SDIWC

www.manaraa.com