International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(1): 290-301
The Society of Digital Information and Wireless Communications, 2015 (ISSN: 2305-0012)

A Framework for Effectiveness of Cyber Security Defenses, a case of the United Arab Emirates (UAE).

Abdulla Al Neaimi, Tago Ranginya, Philip Lutaaya
SecureTech, LLC, UAE.
alneaimi@securetech.ae, tago@securetech.ae, p.lutaaya@secutech.ae

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 of the widespread attacks are done by individuals or various hacking groups for personal gains [3]. The UAE has become a major target for cyber conflicts due to increased economic activity, tourism, technology and the rise of oil and gas industry. Furthermore, the wide spread of internet in the region to the tune of 88% in 2014 has exposed it to attackers [3], [4]. Recent attacks against Saudi Arabia's ARAMCO and Qatar RasGas, the Stuxnet attack on the Iranian nuclear plants are often cited as examples [4], [5]. However, in the digital arena no space is out of control by the law, therefore, it is important to guarantee democratic principles in this domain. The fundamental drivers to the cyber security market are geared towards increasing the digital risk from cyber users by creating greater vulnerabilities because of more pervasive utilization of engineering and cloud computing platforms.

Previous reports show that the UAE Government is set to double expenditure on homeland security [6]. Consequently, we need to assess whether existing 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.

It is only in an environment of trust and mutual respect that nations can benefit from digital infrastructures through secure, safe and reliable cyberspace. More still, network interdependence, intrinsic asymmetry of cyber-threats and pervasiveness of the cyberspace in different aspects are all features that call for holistic approaches and synergetic efforts from all stake holders to ensure adequate level of security in the UAE. The government needs to approve a framework upon which it can coordinate all efforts to ensure effectiveness and efficiency of cyber security defenses within and outside its agencies. However, with the international community still much divided regarding principles and values that apply to the cyber domain, solutions to major cyber space challenges still remain a major concern and therefore require broad involvement of all stakeholders from public, private sectors and all other organizations across the globe [7].

More still, 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 Cooperation Council (GCC) in the recent years. Among such attacks include the August, 2012 attack which affected the major oil and gas company in Saudi Arabia 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 [8], [9], the Shamoon Virus that infected over thirty thousand (30,000) stations and destructed business processes for almost a week, among others [10]. 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. Additionally, attackers have improved their levels of organization and research especially in the area of cloud security which will be the hub for next generation network 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 hacktivist groups. In addition, most recent statistics shows a dramatic increase in UAE cyber security threats. For instance official statistics from Dubai police have shown a dramatic 88% increase in the number of electronic crime cases reported in 2013 compared to the year before. The cyber investigation department of Dubai Police received a total of 1,419 reports in 2013, 792 in 2012 and 588 in 2011 [11]. This trend demonstrates a continued increase in cybercrime within the region as indicated in Fig 1.

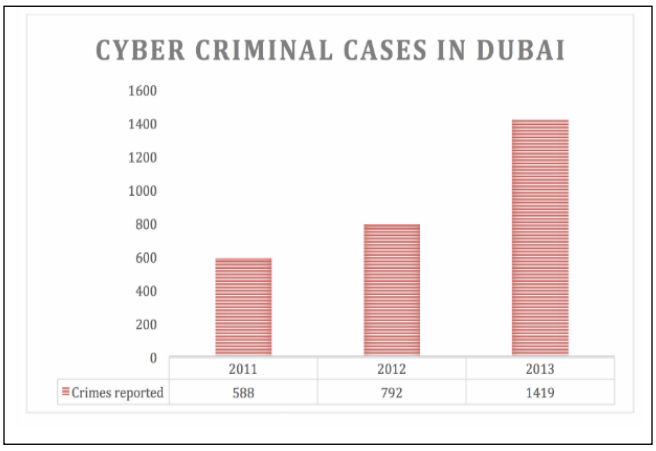

Fig 1: Statistics showing recent cyber incidents in Dubai. Source: http://securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae/, 14/10/2014.

From Fig 1 above, the number of security threats reported to Dubai police were analyzed for a period of three years from 2011 to 2013. The results show a bigger increase in the number of cyber threats between 2012 and 2013 as compared to the period 2011 to 2012. Such results provide a justification for the study leading to the design of an appropriate cyber security framework for detection and prevention of such incidents in the region.

Cyber threats can be categorized into two groups; those whose emergency resulted from Internet or the traditional activities of crime and others from Internet technology development, for 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 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 cyber security defense mechanisms and frameworks available 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 debated so much in literature over the recent years, for example Aloul [12], 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 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. Furthermore, 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 [13]. However, popups, phishing attacks, 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, there are no analytical results to prove this validity. An extensive study is necessary in UAE to prove this validity [14].

On the other hand, the 2012 UNDP report revealed a very big potential in the Middle East to build strong e-Government portals that would streamline communication and reduce operational costs to the tune of 95% with Internet penetration and usage reported at 35.6% by 2012[15]. This trend has continued in the same direction up to today, for instance, the 2014 world internet statistics report showed a considerable increase in the Middle East Internet penetration to approximately 44.9% by the end of 2013 [16]. This is the highest in the whole world which poses a very big cyber security threat to the GCC member states;

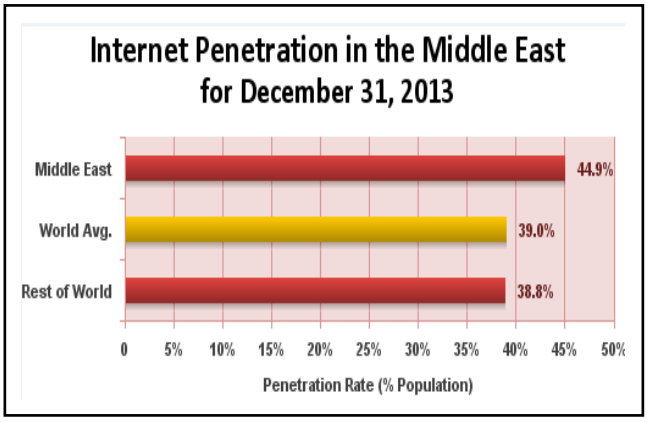

Fig 2: Source: Internet World Stats - www.internetworldstats.com/stats5.htm, © 2014, Miniwatts Marketing Group.

From Fig 2; the rapid increase in Internet penetration in the Middle East up to the tune of 44.5% by the end of 2013 shows that the region has become a major target for different forms of cyber-attacks such as malware, phishing and Denial of Service attacks. This calls for an urgent need for strategic frameworks that can be used to protect the big number of people online from such disastrous cyber-attacks.

Many organizations fail to address employee and insider vulnerabilities as well as assessment of third party partners and supply chains. Furthermore, they fail to strategically invest in cyber security to ensure that it is in line with their business objectives [16].

The PWC annual global geographical survey 2014, revealed that 69% of the US citizen were worried of the impact of cyber threats. The authors identified 8 cyber security strategies that could be of concern to governments, that is to say; aligning cyber security strategies with organizational objectives, addressing third party security, avoiding missing link in supply chain management, mobile phone security issues such as encryption and device management policies, suspicious employee behavior among others. The report further emphasizes funding processes that fully integrate predictive, detective and incident responsive capabilities [17].

In addition to the above strategies, the 2013 KPMG report on cyber security identified the five (5) common cyber security mistakes that most organizations make when handling the cyber problems;

i. We have to achieve 100% security in our organization,
ii. When we invest in the best of class technical tools, we are safe,
iii. Our weapons have to be better than those of hackers,
iv. Cyber security compliance is all about effective monitoring,
v. We need to recruit the best professionals to defend ourselves from cybercrime.

However, it should be noted that 100% security is not feasible, effective cyber security is not only dependent on technology, good security policies or determined by organization goals. Furthermore, learning is as important as monitoring and finally we need to note that cyber security is not a department but rather an attitude of people in every organization [17]. Therefore, appropriate cyber-security frameworks should strike a balance between any of the above common security mistakes if organizations are to achieve the best security defenses.

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 at large [18].

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. Users are the biggest security threat for IT-Security of any organization, therefore, continuous cultural sensitive training and awareness programs need to be in place to change their perception of information and cyber security. Furthermore, cultural and attitude 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 [19] 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 were 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 can 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 [20]. 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 workers since it links a person's electronic identity and attributes stored across a single distinct identity management systems [21]. 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.

Meanwhile, Fadi et al [22], 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 located in the Western Region of Abu Dhabi by the Emirates Nuclear Energy Corporation (ENEC) that is set to complete by the year 2020 in order 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 and the entire economy.

Furthermore, Kaist et al [23], accentuates that nuclear power plants are very important infrastructures for providing efficient and non-interrupted electricity and so 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 [24], provide 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.

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 concerned about protecting people's rights than protecting the privacy of people online. Therefore, the need to incorporate cultural sensitive training and awareness programmes in

the UAE cyber security framework is very important as it contributes to changing one's online behavior.

The use of "edge" devices, cloud applications and the increased regulatory requirements has created an urgent need for organizations to advance their security and re-think traditional approaches to stay ahead of the ever escalating risk levels. A new strategic framework is therefore needed to address numerous disruptive trends across the IT landscape in securing data, mobile devices, cloud computing environments among others .The major challenge is to address disruptive technologies and trends like "everything connected", social computing and at the same time manage inherent risks [25].

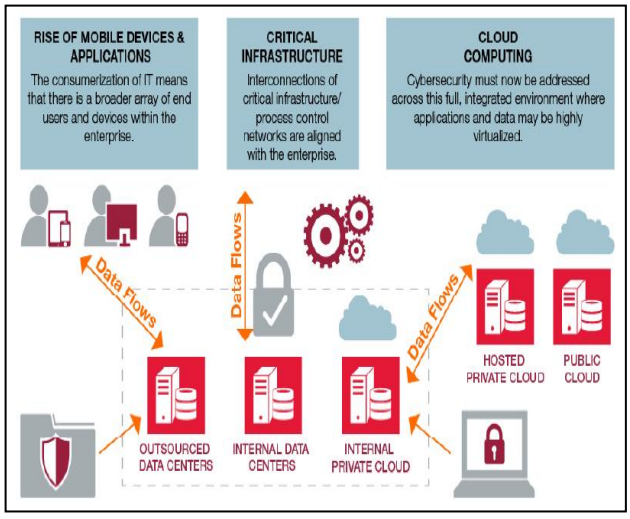

Fig 3: Increasingly sophisticated porous security perimeter. Source: Cyber security in modern critical environments CGI group INC, 2014, page 5.

Fig 3 shows a highly connected IT infrastructure environment that combines data flows from mobile devices, critical infrastructures and cloud computing environments. All these provide sensitive data to internal and out sourced data centers under a common back bone. As a result an attack on such an environment would be disastrous to organizations in terms of massive data loses and destruction of critical infrastructure. Therefore, we need to design cyber security frameworks which can protect critical data in such highly connected and distributed network environments. This is the case for the e-Government portal of the UAE through which all Government to Citizen (G2C) transactions have been channeled through platforms like the Emirates Identity Management System.

Meanwhile, the latest 2014 report by Cisco Systems International reveal that malware encounters have shifted focus to electronics, manufacturing, agriculture and mining industries at a rate six times the average encounter across industry verticals. It is revealed that 99% of all mobile malware in 2013 targeted android mobile devices which are the most used devices in the region. More still mobile devices introduce a major security risk to organizations especially when they are used to access company resources, they easily connect with 3rd party cloud services and computers with security bearings that are outside enterprise control. This problem is expected to increase especially with the arrival of IPV6 deployments across the globe [26].

It is further reported that by the end of 2014 more mobile devices will be connected to the internet to about 7 billion devices more than the number of people on the planet and in two years' time between 15 billion to 25 billion devices will communicate across the internet [26]. This trend implies that governments and organizations would find it extremely difficult to identify and isolate invalid devices trying to access their ICT infrastructure.

Authors in [27] assessed the cyber security problem in selected ministries of the Government of Kenya by providing both descriptive and inferential analysis into cyber security assessment. They claim that cyber-attacks are highly sophisticated to the extent of troubling

many organizations in identifying the greatest risk vulnerabilities, they reveal that the Kenyan government does not own any global network as with most African countries which makes them very vulnerable to cyber-attacks. However, the case study approach used in this research only focused on responses from highly qualified IT experts leaving out the most suspect computer users with little or no IT skills at all. We need an all-inclusive framework that considers requirements of the different categories of people.

The findings of this study revealed that 72.1% of the respondents were in agreement that their organizations had no secure cyber security infrastructure and 62.8% had no risk assessment and IT security audits. They proposed a cyber-security assessment framework based on Karl Pearson correlations between the cyber security challenges and cyber security state at 95% confidence interval.

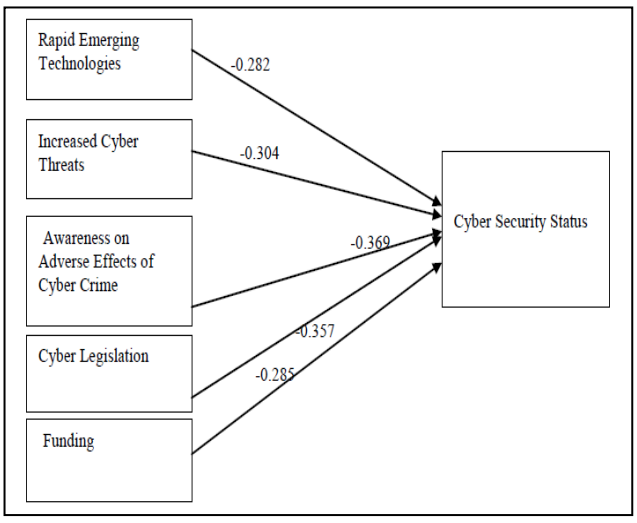

Fig 4: A framework for assessing cyber security challenges. Source: Cyber security assessment Framework, a case of government ministries in Kenya, 2014, pp 6, ISSN 2349-1582.

The correlation results from Fig 4 reveal that;

Lack of awareness of information security issues poses the greatest danger to the effectiveness of cyber security in many organizations, this hierarchy is followed by inadequate cyber legislation, inadequate funding and the rapidly changing technologies. Therefore, if cyber security frameworks do not emphasize adequate legislation and cyber security training and awareness, their organizations would be highly vulnerable to all forms of attacks. This assessment framework for the Kenyan Government can also be applied by the UAE government in the prioritization and emphasis of the most pressing cyber security issues.

The NIST Report, 2014 shows that Cyber-attacks can seriously disrupt or even paralyze segments of critical national infrastructure, therefore, a military like defensive or offensive posture or action may be required. Appropriate strategic management theories and principles are needed to guide the control and prevention of these attacks [28]. The report claims that the an executive order by the US President called for the development of a voluntary risk-based Cybersecurity Framework which involved a set of industry standards and best practices to assist organizations in the management of 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, [28];

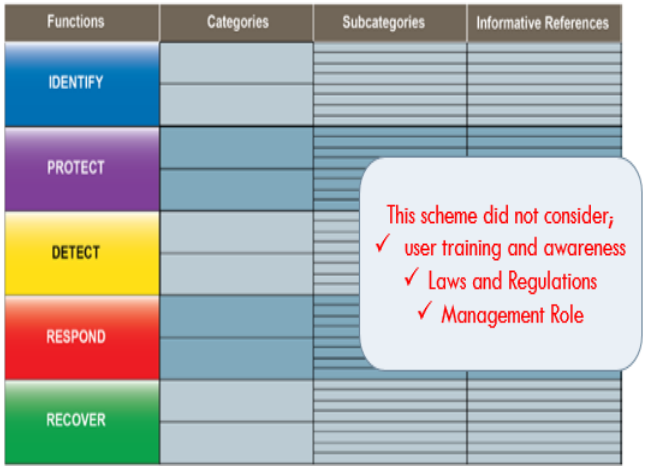

Fig 5: Illustration of NIST cyber security Framework. Source: NIST Report, 2014.

It can be seen from Fig 5 above that, the NIST framework mainly focused on business drivers that influence security activities and considered Cyber security risk as part of the organization's risk assessment process. The framework is a risk based compilation of guidelines designed to help organizations in assessing current capabilities and drafting prioritized roadmaps towards improved cyber security practices. Its major goal is to improve risk based security, however, it fails to fully address all critical areas and may not work well for private sector agencies. In addition, the NIST 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.

Other implementation issues like attacker motivations, statutory and contractual obligations and the fact that most organizations may not manage continuous technological upgrades remain a major concern. Therefore, 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 and control.

The 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 managers which then leads to actions being taken organizationally to prevent such 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 UAE Federal Law No (2) of 2012 [28]. 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 International Telecommunication Union (ITU) report revealed a number of challenges in the prevention of cybercrime globally [29], such challenges include but are 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 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 threat leading to attacks on critical government infrastructures like central banks [30], [31]. 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. In [32], it is said 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 reduced 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 [33], [34].

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.

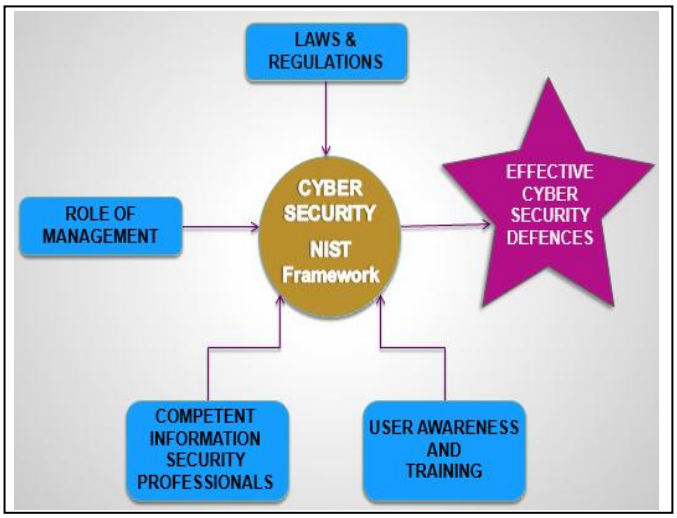

Fig 6: Proposed Framework for Cyber security defense in the UAE government agencies.

1.5 DISCUSSIONS

From Fig 6 above, the NIST framework has been integrated within the developed design to provide the technological and risk assessment capabilities within the new framework. 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 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. 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. It may also be important to apply the cyber security challenge assessment framework proposed in Fig 4 to handle the prioritization of the most pressing challenges in the region.

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 the establishment of cultural sensitive training and awareness programmes. A typical cyber security challenge assessment framework has also been discussed to enable prioritization of the challenges. Some of the strategic guidelines revealed for cyber space security include enhancement of technical, operational and analytical capabilities of all institutions of concern, protection of critical infrastructure and strategic assets, promotion and facilitation of public-private partnerships for promotion of national properties, strengthening online security and full support to international cooperation. Other recommendations may include reviewing the existing system of technology especially for hi-technology crimes and providing a workable

solution for preserving as well as examination of evidence. All these can be achieved by following the guidelines provided by the proposed framework for effective cyber security defense.

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 examine the need for incorporation of cyber security education in the UAE syllabi.

REFERENCES

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

[2] James Andrew Lewis, "Cyber Security and Stability in the Gulf", Center For 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, "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] Italian National Strategic Framework for cyber space Security, Presidency of the council of Ministers, December, 2013.

[8] Kathy Brown, "Open and sustainable access for all", Internet Society Global Internet Report, 2014.

[9] Al-Bawaba, "Cyber-crime laws in the UAE are dangerously vague", 2012.

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

[11] Mohamad Amin Hasbini, "Statistics showing recent cyber incidents in Dubai", http:// securelist.com/blog/research/63682/the-rise-of-cybercrime-in-dubai-and-uae/, visited on 14/10/2014

[12] 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.

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

[14] Symantec Internet Security Threat Report, 2013.

[15] United Nations Development Programme (UNDP) Report,"E-government for the people", retrieved 30th/07/2014, from http://www.unpan.org/egovkb/global_report.html

[16] Internet World Stats, http://www.internetworldstats.com/stats.htm, Miniwatts Marketing Group, 2014

[17] John Hernams, Gerben Schreurs, "The five most common cyber security mistakes, Management's perspective on cyber security", www.kpmg.nl, KPMG Advisory, 2013

[18] Kevin Mickelberg, Laurie Schive, and Neal Pollard**, "**US cybercrime: Rising risks, reduced readiness, Key findings from the 2014", US State of Cybercrime Survey. http:// www.pwc.com/cybersecurity, June, 2014

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

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

[21] 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.

[22] 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

[23] 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, BEXCO, Busan, Korea, 2012

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

[25] "Cybersecurity in Modern Critical Infrastructure Environments", www.cgi.com, 2014 CGI GROUP INC.

[26] Cisco Systems International Inc. "Emerging Cyber Security threats", Annual security report, 2014

[27] Alice Nambiro Wechuli, Geoffrey Muchiri Muketha, Nahason Matoke, "Cyber Security Assessment Framework": Case of Government Ministries in Kenya, International Journal of Technology in Computer Science & Engineering, ISSN 2349-1582, 2014, http://www.ijtcse.com

[28] National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity", June, 2014

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

[30] Reuters, "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, 2012

[31] UAE Telecommunication Regulatory Authority web portal, http://www.tra.gov.ae/national-emergency-plan.php, retrieved on 12/10/2014

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

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

[34] Robert Burgers, Hans Baars, Maurice Adriaensen and Atif Raja, "Middle East needs cyber security from within", DNV KEMA Energy & Sustainability, 2013.