A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security

Mohammed I. Alghamdi
Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia.
E-mail: mialmushilah@bu.edu.sa

Received June 15, 2020; Accepted August 18, 2020
ISSN: 1735-188X
DOI: 10.14704/WEB/V17I2/WEB17031

Abstract

The cyber-security development for future generations is at stake as a global concern. The existing strategic and policy structures on cyber security and awareness-raising at many levels needs more investigation in order to formulate workable and efficient strategic vision that addresses actual needs and challenges. The justification for this work is therefore to test the robustness, in contrast with some of the most technologically advanced countries on the Asian Continent and others like the USA, Japan, of Saudi Arabia's current cyber security strategy in order to keep the NCSS up-to-date. This research aimed to develop a strategic vision to combat cybercrime to enhance cyber security. The research results confirmed the approval of the members of the study community to a medium degree on the reality of digital extremism and cyber terrorism as seen by the researcher. Moreover, the approval of the members of the study community was to a high degree on the role of combating cybercrime in promoting human security as seen by the researcher. The members of the study community agreed with a high degree on the obstacles identified by the researcher to combat cyber-crimes to enhance human security in Saudi Arabia. There was a high approval of the study community members on the strategic vision developed by the researcher to combat cyber-crimes to enhance human security in Saudi Arabia.

Keywords

Cyber-Security, Strategic Vision, National Network for Cyber Security (NCSS), Cyber-Crime Prevention.

Introduction

Technology is a continually changing expression in modern times, which has enhanced security concerns and driven us to build a cyber-environment. A country's National Network for Cyber Security (NCSS) reflects the cyber strength of the country, which is a target and vision for a country's cyber safety. Researchers worked on NCSS by comparing

NCSS for international cooperation and harmonization between various nations and some researchers worked for their respective governments in the policy framework (Sarker, K., et al., 2019).

The Internet has become a basic and critical need for people's lives and socio-economic activities. Although it facilitates things for people, it also creates new risks. Never stopped cyber-attacks and never will they, but they exponentially increase instead. That country therefore needs an ICT infrastructure secure, efficient and robust. There can be a high risk of a poor ICT infrastructure. Every interested cyber intelligence specialist can use ICT to manipulate state-of-the-art government and industry classified information. However very small attempts were made to estimate Saudi Arabia's strategic strength in the NCSS by comparing the NCSS of the various nations.

Training in cyber-security is an effective response to an increasing number of intrusions and attacks (Nagarajan et al., 2012). 80 percent of all vulnerabilities exploited by hackers are due to human vulnerabilities (IBM, 2013) but cyber security is a priority of information technology on tools and technologies (Hershberger, 2014). Human vulnerabilities include employee incompetence, misinformed management and limited training in cyber security, malicious insiders and third parties having access to a company's network, but are not confined to them. Current politicians, government bodies and academic researchers have come to know the need to improve cyber security capabilities and increase awareness in the workforce and leadership (Evans & Reeder, 2010). After the breach of Target Organization information in 2013, an empirical review of the attack found that the Target security systems recognized the intrusion. But the management and the personnel involved in taking action lacked the know-how and skills necessary (Hershberger, 2014).

Cyber security is then built on cyber defense or on a series of technical and non-technical measures that allow a country to defend information systems that are deemed essential to the creation of cyberspace. Cyber security could then be called a state desired by an information system that would allow it to withstand cyberspace events that might jeopardize the reliability, integrity or privacy of the data stored, processed, distributed and the related services provided or made available by those systems. It uses security techniques of information systems and is based on cybercrime combat and cyber defense.

As a prerequisite for technological growth and globalization dynamics as well as a resource for sustainable development, cyber security concerns that entity (individual, government, institutional, etc.) and represents thus cross-cutting challenges. These challenges range from the securing of IT and IT systems (Industrial IT, IT management, connected objects, etc.) to the economic, political and capacity-building strategies (Willemant and Foulgoc, 2016).

The current combination of the exponential increase in internet flows and the increasing connection between players and their information makes cybersecurity a comprehensive and global issue. In addition, through the Agenda for Sustainable Development, the Millennium Development Goals are one of 17 goals to be reached in 2030 for technological development and capacity building in this region. In this regard cyber security and cyber-crime prevention, as a means of ensuring this space for trade and growth, constitute major issues in this process. Estimates suggest that cyber-attacks cost the global economy about EUR 400 billion a year (El Melhem, J., et al., 2019).

Government organizations are also vulnerable to cyber-attacks. It has been shown over the past 12 months that nearly 70% of organizations have reported that a successful cyber-attack has affected their security. 65 percent of organizations say that there is a shortage of qualified cyber response professionals. In a report, Kim and Solarwinds reported that in the United Kingdom Government in 2017, almost two-thirds of the nation's largest company was cyber-attacked over the past 12 months. Cyber security is therefore an important government priority. Data theft or cyber-attack could cost government agencies millions. It also harms an organization's image and can have devastating consequences for the people.

In their analysis, Saad et al. (2016) analyzed the need to examine any gap in current technology in network security at current times, thereby promoting the intensification of researchers ' expertise while finding answers to these potential issues. Although such systems might be more valuable, it is usually smaller networks, such as a campus network, that are vulnerable to hackers. They studied in their paper the current field of research based on a 6-fold survey, {what, where, how, who, how} and developed a mental map to catch lacunae and the opening doors to network safety research.

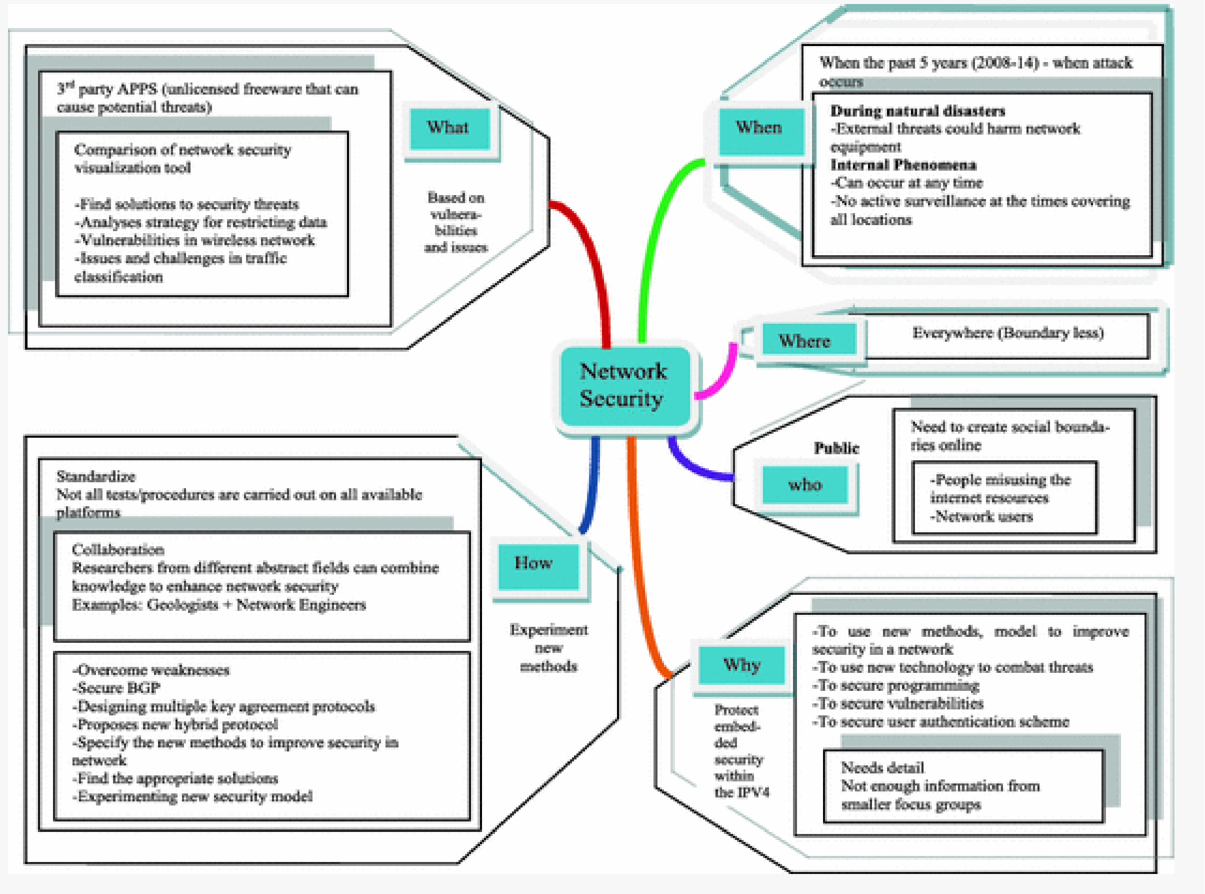
3rd party APPS (unlicensed freeware that can cause potential threats)
Comparison of network security visualization tool
-Find solutions to security threats
-Analyses strategy for restricting data
-Vulnerabilities in wireless network
-Issues and challenges in traffic classification
What
Based on vulnera-bilities and issues
When
When the past 5 years (2008-14) - when attack occurs
During natural disasters
-External threats could harm network equipment
Internal Phenomena
-Can occur at any time
-No active surveillance at the times covering all locations
Network Security
Where
Everywhere (Boundary less)
Public
who
Need to create social bounda-ries online
-People misusing the internet resources
-Network users
Standardize
Not all tests/procedures are carried out on all available platforms
Collaboration
Researchers from different abstract fields can combine knowledge to enhance network security
Examples: Geologists + Network Engineers
-Overcome weaknesses
-Secure BGP
-Designing multiple key agreement protocols
-Proposes new hybrid protocol
-Specify the new methods to improve security in network
-Find the appropriate solutions
-Experimenting new security model
How
Experiment new methods
Why
Protect embed-ded security within the IPV4
-To use new methods, model to improve security in a network
-To use new technology to combat threats
-To secure programming
-To secure vulnerabilities
-To secure user authentication scheme
Needs detail
Not enough information from smaller focus groups

Figure 1 Cyber-crime mitigation network security mind – map

Most cyber security attacks are due to human errors and attackers focus more on human vulnerability exploitation (Evans, M., et al., 2019; Kelly, R., 2017; Islam, T., et al., 2019). Consequently, it is increasingly important to understand human functions in promoting cyber security. Joins on and van Steen (2018) suggested the incorporation of history, actions and design for that reason of security tools and policies.

In the case of complex situations, Ganin et al. (2016) proposed a multi-criteria policy framework incorporating risk assessments (threat, vulnerability and consequences) for prioritizing countermeasures using user friendly technology. Dykstra and Orr (2016) proposed a human decision-making evaluation framework for defining security risks and responses context accordingly.

This research aimed to develop a strategic vision to combat cybercrime to enhance cyber security in Saudi Arabia through the following steps:

1. Identify the nature and types of cybercrime.
2. Knowledge of the nature and dimensions of cyber security.

3. Identify the reality of digital extremism and cyber terrorism and its impact on cyber security.
4. Know the role of combating cybercrime in promoting cyber security.
5. Identify obstacles to combating cybercrime to enhance cyber security.

Methodology

An online survey was carried out in which 16 cyber security hazards rates were measured on the basis of the previous research as an independent variable. A total of 200 web users were surveyed. The study was carried out. The students' risk perception and precautionary actions in terms of safety during internet usage were examined through a qualitative empiric on-line analysis with psychometric methods. The survey found it clear that in cases of crimes such as identity thieving, cyber bullying, social engineering, and loggers, the perceived risk increased. Among the most optimistic predictors, we are afraid, voluntarism, catastrophic and immediate threats. In addition the top scores are Internet competence and its level of use. In fact, regulation was an important precautionary measure. Identity theft was discerned as dangerous threat by students.

Results and Discussion

The research results confirmed the approval of the members of the study community to a medium degree on the reality of digital extremism and cyber terrorism as seen by the researcher. Moreover, the approval of the members of the study community was to a high degree on the role of combating cybercrime in promoting human security as seen by the researcher. The members of the study community agreed with a high degree on the obstacles identified by the researcher to combat cyber-crimes to enhance human security in Saudi Arabia. There was a high approval of the study community members on the strategic vision developed by the researcher to combat cyber-crimes to enhance human security in Saudi Arabia.

Strategic Steps to Avoid Cyber Crimes

Monitoring and alerts	Network monitoring and alerting settings to detect suspicious activity are very important – a malicious attacker should not be allowed to access and store sensitive data on a peripheral device by means of comprehensive system monitoring.
Risk management decision-making	By means of a risk assessment, they can determine how assets and a limited budget should be expended. If the piece in question is downgraded or attacked by a virus, it will access technical equipment, software system and allocate monetary risk value
Up-to-date technology	The proper use of security technologies and the equipment necessary: The company will remain vulnerable to hackers by outdated computer firmware, weak protocols and out - of-date safety technology.
Security team	A well-trained professional staff should be able instantly to protect sensitive and private information – the IT department should be vigilant to know about common threats
Knowledge is power	To avoid cyber-crimes, maintaining good knowledge about potential threats and attacks

Conclusion

This decade has seen an exponential increase in the number of internet users. It's going on all over the world. Each world now has the blessing and curse of technology from underdeveloped to developing and developed countries. Cyber-attacks are increasing and more complicated. This also increases. It's not restricted to a state but is beyond the boundaries to make things worse, unlike federal crimes. Therefore, when there is no proper infrastructure to combat it, it is more likely to remain undetected.

The development of cyber security policy is at a turning point. Cyber-security has become a national priority, while the importance of' sovereignty' is increasing. National cyber security policies are aimed at promoting economic and social prosperity and at protecting cyber-reliant societies against cyber risk. Common elements of such approaches are improving policy and organizational government coordination; strengthening the collaboration between public and private sectors; emphasizing the need for fundamental values such as the security of personal data, freedom of expression and the free flow of information; and calling for better international cooperation.

Recommendations

1. Promptly prepare a draft law called (Cyber Security Law) that defines the controls of the operators of telecommunications and Internet service providers in the Kingdom of Saudi Arabia, and promotes the fight against cybercrime and the protection of the Saudi society in cyberspace.
2. Establishing a national specialized cybersecurity authority to protect Saudi's cyberspace and enhance infrastructure security.
3. Establish a specialized prosecutor to investigate, confront and control all types of cybercrime.
4. Establishing a specific security unit at the Ministry of Interior specialized in combating cybercrime and its tasks (attached in detail to the strategic vision).
5. The need to educate the Saudi society - individuals and institutions - ways to protect against cyber-crimes.

References

Dykstra, J.A., & Orr, S.R. (2016). Acting in the unknown: the cynefin framework for managing cyber security risk in dynamic decision making. *In IEEE International Conference on Cyber Conflict (CyCon US),* 1-6.

El Melhem, J., Bouras, A., & Ouzrout, Y. (2019). Toward a Holistic Approach of Cybersecurity Capacity Building through an Innovative Transversal Sandwich Training.

In Industry Integrated Engineering and Computing Education, *Springer*, *Cham*, 187-212.

Evans, M., He, Y., Maglaras, L., &Janicke, H. (2019). HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, 74-89.

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D., & Linkov, I. (2017).Multi-criteria decision framework for cyber security risk assessment and management. *Risk Analysis*, *40*(4).

Hershberger, P. (2014). *Security skills assessment and training: The "make or break" critical security control.* SANS Institute Info Sec Reading Room.

IBM. (2013). *The 2013 IBM Cyber Security Intelligence Index.*IBM Security Services.

Islam, T., Becker, I., Posner, R., Ekblom, P., McGuire, M., Borrion, H., & Li, S. (2019). A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. *In International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications*, *Springer*, *Singapore*, 277-293.

Joinson, A., & Steen, T.V. (2018). Human aspects of cyber security: Behaviour or culture change?. *Cyber Security: A Peer-Reviewed Journal*, *1*(4), 351-360.

Kelly, R. (2017). *Almost 90% of cyber attacks are caused by human error or behavior.* Chief Executive.net.

Kim, J. (2017). Cyber-security in government: reducing the risk. *Computer Fraud & Security*, *7*, 8-11.

Nagarajan, A., Allbeck, J.M., Sood, A., & Janssen, T.L. (2012).Exploring game design for cybersecurity training. *In IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 256-262.

Saad, A., Amran, A.R., Afif II, Zolkeple, A.H., Said, A.I.A., Hamzah, M.F., & Salim, W.N.S.W. (2016). Privacy and security gaps in mitigating Cybercrime: The review. *In IEEE 2nd International Symposium on Agent, Multi-Agent Systems and Robotics (ISAMSR)*, 92-99.

Sarker, K., Rahman, H., Rahman, K.F., Arman, M., Biswas, S., & Bhuiyan, T. (2019). A Comparative Analysis of the Cyber Security Strategy of Bangladesh. *International Journal on Cybernetics & Informatics (IJCI)*, *8*(2), 1-21.

Willemant, R., & Foulgoc, S. (2016). *Legal Aspects of Cyber-security*. Action Canada Fr., *25*, 18-19.