Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.6, No.11, 2016

Latest Trends and Future Directions of Cyber Security Information Systems

Hadi Saeed Alqahtani
Computer technology and admin system department, Arab East College for High Education, Kingdom of Saudi Arabia

Abstract
The significance of the information system security is critical issue for the organizations since it leads to big financial losses. The understanding of cyber security threats is not only an innovative requirement but also it is a conservative task. The rapid changes in technologies and services are major driving and leading concerns to the cyber security, requiring reassessment and renewal of standardized policies for counter measures to the resistant vulnerabilities. The main aim of this paper is to improve the understanding and perception of latest security threats, security counter measures, and the future trends of cyberspace security. Therefore, we look forward proposing a new classification model of security threats in order to generalize the impact of threats into classes rather than the impact of every individual threat. The importance of this study comes from the neediness to forecast the future trends of information system cyber security on the long basis, as well as the identification of future security measures that would be reliable. Cyber security models need to improve according to the situational awareness over all situations and at all levels in order to avoid conflicting interests and priorities.
Keywords: security, cyber security, cyber-attacks, information system security.

1. Introduction

Various threats can cause several kinds of damage to the information systems that are exposed and vulnerable to harm. Some effects of the threats reach the data integrity, availability, or confidentiality. The most significant impact of these threats is the financial losses, whereas other small losses can occur to the information system destruction. Many organizations are stressed to the continuous challenge of addressing the main threatening risks to their information system assets in order to understand how to employ necessary means to struggle them (Jouini et al., 2014).

The security or assurance of information defines the information security that requires the capacity to sustain the information authenticity. It also contains three common components: integrity, availability, and confidentiality. These essential components form a significant basis for the information security measurements (Von Solms and Van Niekerk, 2013).

The employment of cyber defense is not much easier than cyber-attack; cyber defense should successfully struggle all attacks to be an effective. In contrast, the attacker might gain the access to the information system by only one successfully exploited weak. However, cyber-attack is faster, cheaper, and easier than cyber defense; this refers to the number of skilled experts in cyber-attack larger than those experts in cyber defense. The efforts of cyber defenders should be allocated for supply and encouraging exceeds the requirements of cyber-attack (Dhillon, 2007).

The evaluation of cyber security of an organization is difficult since it requires using sophisticated mechanisms to define the key success factors and indicators of the cyber security program. However, the total amount of time elapsed from the occurrence of hacking to the detection process is the most important metric to ensure the effectiveness of the employed techniques to track its progression in this significant aspect (Graham et al., 2016). The main aim of this paper is to improve the understanding and perception of latest security threats, security counter measures, and the future trends of cyberspace security. Therefore, we look forward proposing a new classification model of security threats in order to generalize the impact of threats into classes rather than the impact of every individual threat.

2. Background

In the past decade, the area of cyber security and connected security research subjects has been frequently explored in research development activities (Maughan, 2009). The concept of Information and Communication Technologies (ICT) has emerged and evolutionally distributed, whereas the protection of ICT and its content becomes known as cyber security. This term is somewhat fuzzy concept, but its definition is focused to be precisely explained. Cyber security refers to a group of activities, tasks, and operations taken to protect information systems from attacks such as disruption, harm, damage, loss, or other attacks threatening the computer networks, hardware, software, files, and information contained in cyberspace. Therefore, cyber security aims to protect the state or quality from several threats and risks, as well as to improve and implement the activities of quality (Trautman, 2015).

The development of an effective cyber security program is a challenging task, especially when the

interests of the organizations are competing. In addition, the improvement of social media today increases the communication, collaboration, online transactions, not to mentioning their risks. Generally, it attracts the interesting partners to counter these risks by creating cyber security particularly to sensitive information of the information systems (Sharp Sr, 2010). The vulnerabilities of the information systems create a weakness that the attacker can exploit and make the damage. The existence of these vulnerabilities in information systems increases the potentiality to cause undesired effects (Jouini et al., 2014).

The significance of the information system security is critical issue for the organizations since it leads to big financial losses (Jouini et al., 2014). Over the last decade, the digital technology has changed the scale, scope, and the prospective issues in business in a way that traditional organizations and business models cannot adapt new risks that never experienced before (Kaplan et al., 2015).

3. Significance

This research would help to advance the scientific interests in the research of cyber security, particularly to answer the methodological questions of the prediction of future information and activities relevant to security trends and issues. The importance of this study comes from the neediness to forecast the trends of information system cyber security in the long term, as well as the identification of future security measures that would be reliable. This study sets a background to start implementing guidelines practically according to the expected security issues and solutions to information systems.

The community research in cyber security has extremely addressed many challenges in cyber security through the adaption and evaluation of information visualization techniques into the field of cyber security (Staheli et al., 2014). From another perspective, the crimes in economic and financial domain cause huge effects to the companies. According to many reports prepared in business, 61% of companies have become victims to economic crimes in the last decade. The effects of economic crimes are damaged substantial monetary, lost morale, high financial losses, damaged business, and lost reputation (Koch et al. 2012).

4. Problem

In particular, the old security models cannot be deployed against evolved cyber security risks, as well as the businesses approaches need continuous updates to manage and keep the business in safe place (Kaplan et al., 2015). Today, the cyber risk management systems are complex, thus they require wide engagement, management, and sophisticated mechanisms having new capabilities and skills of defensing security (Singer and Friedman, 2014). Due to the increasing number of the interconnections around the world (personal, military, government, and commercial information on the infrastructure of internet), the advent of new networking technologies emerged. For this reason, the developments in the field of network security have become an excessive necessity especially for intellectual property protection (Daya, 2013).

5. Aims and objectives

This paper tries to address several criteria of cyber security risks, threats and solutions based on reviewing different threats classification models. In this paper, we aim to define the common information system threats classifications and architectures that follow the most popular principles and strategies of information systems security. This type of paper is important to the security threats classification, as we can protect our information systems and security assets in advance through identifying threat sources, potential impacts and effects in specific areas of systems. Considering several basements (source, effects, motivations, actions, behaviors, and agents), we can classify and identify security threats in multiple ways, and then assessing the impact of threats and developing strategies to mitigate and prevent their consequence.

This research incorporates a set of techniques applied and might be improved to serve cyber security in terms of predicting the operational validity of the approaches of evaluation standards. The purpose of this paper is to present an overview of the future picture of cyber security field, in addition to the exploration of the increased dependencies on the security due to the varying number and type of threats with the increasing vulnerabilities in current systems and their associated challenges.

We aim to achieve the following goals:

- To identify the main threats of information systems cyber security have been and being addressed and what are the challenges.
- To address the current state of the practice and the current research gap with respect to information systems cyber security.
- To anticipate the potential receivers and the effects of these threats on the individuals and organizations.
- To describe the main respective needs of these receivers of the current and prospect threats and what are the major cyber security approaches might be desirable in future.

We attempt to answer the following questions:

- What are the main threats of information systems cyber security have been and being addressed and

what are the challenges?

- What is the current state of the practice and the current research gap with respect to information systems cyber security?
- What are the potential receivers of these threats, and what are the effects on the individuals and organizations?
- What are the main respective needs of these receivers of the current and prospect threats and what are the major cyber security approaches might be desirable in future?

6. Types of cyber security information

The focus of cyber security measures is commonly on the threat coming from the outers, instead of threats that can be created by insiders, authorized users, such as employees of the organization (Maughan, 2009). We have various types of cyber security information that we should know including incidents, threats, vulnerabilities, mitigation, situational awareness, strategic analysis, and best practices in terms of information system cyber security. Here, we will identify every type with short explanation (Koch et al. 2012). The growth of threat to the security of public systems is located under cyberspace domain. Consequently, the main focus of threat actors today is on malicious intentions, the political stimulations, and the theft of information (Sommestad, 2012).

Many issues in the internet security are continuously generated, whereas technologies to protect information access and alter can be controlled through the followings (Daya, 2013):

- A widely, useful tool used in security engineering nowadays is Cryptographic system.
- A typical controlling boundaries mechanism and defensing borders is firewall.
- Additional protection mechanism is Intrusion Detection Systems (IDS).
- Anti-Malware Software and Viruses, Worms, and Trojans Scanners (for short Malware).
- The use of a suite protocol, Secure Socket Layer (SSL), to attain a good level of security between web browsers and websites.

Form other perspective, the mitigation methods to remedy the vulnerabilities such as block, contain, respond, and recover from the incidents of threats. The information of the vulnerability exploited, the antivirus deployed, and the direction to remove the malicious program should be logged. In the same context, the situational awareness can be achieved to enable the collected information to help the decision makers responding to the incident. This might requires employing real time responding programs to react the active threats and attacks. The targets and purposes of the attackers should be encountered to determine the status of the critical situation (Koch et al. 2012).

7. Mutual Internet Attack Approaches

The most common types of attacks followed and implemented over the internet are defined as following:

- The interception of communications by illegal parties.
- Self-replication, infection, and propagation programs, viruses.
- Self-replication and propagation into a file, worms.
- Malicious programs that seem kind to the users, Trojans.
- Obtaining confidential information from users through phishing.
- Having an IP address of another trusted computer to gain access, IP spoofing.
- Sending too many requests to a server that cannot respond them, Denial of Service (DOS).

Incidents should be recorded including the details and description of the attempted and happened attacks such as intent, impact, lost, and techniques used to defense the attack. These incidents are ranging from simple blocking attack to a seriously impacting security situation. Likewise, the threats and their serious implications and information such as the indicators of damage, malware effects, the threat actors to help the specialists to detect the incidents early, to learn lessons from these attacks, to build better solutions against these attacks. In this domain, vulnerabilities are associated with threats; the increasing potentiality of the presence of a threat depends on the existence of the vulnerabilities. The vulnerabilities might found in hardware, software, or business systems and processes that can be broken to perform harmful action (Koch et al. 2012).

The challenging issue in the cyber security is the neediness of addressing security problems on a multinational level including national providers, national networks, and future internet. Moreover, the provision of services (cloud services) does not currently enforce locating services and part of services after delivered to the end users. However, the end user is fully interested in the protection and the availability of the service not in the service location, which is significant to national and international providers who look forward securing services, detecting and preventing networks attacks in the next generation (Koch et al. 2012). The prioritization of cyber security activities can be done through establishing better understanding of risk tolerance and allowing organizations to be well informed with cyber security costs. Moreover, the ability of organizations to implement risk management and measure changes to the implemented cyber security programs increases (National Institute

of Standards and Technology (NIST) and United States of America, 2014).

8. Current and future

Cyber security often encompasses several skills to hold to protect data. Security measures involve several duties including creating regulations, enforcing policies, and drafting procedures to guarantee computer information system governance (Von Solms and Van Niekerk, 2013). Every organization must to build a culture of information security throughout the members of the organization to establish the degree of the seriously taken security responsibilities. Thus, they have to apply at least organizational practices and policies significant to provide information assurance and technical mechanisms. These policies must specify the minimal requirements to follow formal structures, protect information, assign access privileges, establish procedures, ensure of accountability, confirm the responsibility, and obey all privacy and security practices of the organization. Hence, it is much needed to lead the individuals in an organization to promote information assurance in the culture of that organization leaded by the senior leadership (Dhillon, 2007).

Currently, many computer security specialists are developing more sophisticated approaches to prevent, detect, and respond the security related issues. In general, there is not one solution to resolve and address all types of these cyber threats and associated evolving challenges. However, there is remaining important aspect, which is the implementation of adaptable cyber security controls to have strong response plans for several changes in the landscape of threats and the event of attacks (Graham et al., 2016). The transmission of petabytes of data, the trillions of devices, and the emergence of new services/needs and technologies increase the potential threats and vulnerabilities as well as dealing and handling them (Koch et al. 2012).

Today, the business and social habits are being revolutionized by the internet. The conversion has become from connecting information and computers into a network to connecting people. Potentially, the internet in the future will be a structure of virtualized and scalable resources provided by service providers to the end users. From technical perspective, the technical issues will be changed significantly; more new business models, new problems, and increased number of services over the internet (Koch et al. 2012). The increasing of the connectivity and complexity in the infrastructures of new emerging systems are being exploited by cyber security threats. These threats place the economy, national cyber security, and business and commerce at risk. Cyber security risk effects touch the bottom line of a company similar to reputational and financial risks, impacting revenue and driving up costs. Thus, threats can limit the ability of organizations to innovate, compete, and increase the reputation of customers (National Institute of Standards and Technology (NIST) and United States of America, 2014).

The new realization of threats and attacks increases the interest in the following areas (Kaplan et al., 2015):

- Increasing dependence to the emergence of technology.
- The establishment of organizations on collaboration and trust.
- The business ecosystems include information and data ubiquity.
- Multiple parties are involved in transactions and operations.
- The new technological reality encompasses new and advanced threats.

The new attacks enforce current security community in full attention and interesting as never before since the incidents and risks associated with cyber-attacks are increasing (Choo, 2011). The following points are major examples of the implementation of common cyber security visions, goals, and strategies (Sommestad, 2012). The framework should address:

- The increasing cooperation and focusing inside the security community to motivate active participation of all players and at all levels.
- The leverage and expansion of current best practices of cyber security measures in the research and education fields.
- The emerging of proper related government agencies into this domain.
- The creation of a general framework for identification of the next generation of cyber security controls.
- The establishment of coordinative and collaborative strategies, plans, and policies in terms of cyber security trends.

Many solutions emerged to secure networks such as Intrusion Detection Systems (IDS), Packet Filter (PF), and Application Layer Gateways (ALG). They are not only used to control traffic over networks, for example packets entering and leaving a network are controlled based on packet information, but also to filter malicious traffic over networks based on predefined rules (Koch et al. 2012). One of the best practices that could be employed to defense these incidents is to develop the security controls and responses practices to show the effectiveness of the security metrics. Therefore, we can plan for strategic planning by collecting the useful information to analyze the security stare of an organization such as trends, metrics, and proposed policies and procedures for prospected scenarios and future risks (Koch et al. 2012).

To define cyber security for commercial aviation, we cannot conclude the most common strategies, goals, visions, standards, global policies, and implementation models. The involvement of governments, business, and individuals is necessary to ensure of the security of cyber information systems and to stay ahead for cyber threats evolvement since this issue is shared responsibility. All of these members should be incorporated to adopt collaborative cyber security for risks definitions and decisions based on an agreed cyber security framework. This framework should involve the common strategy and vision of different economic, technical, and commercial concern of the security. They also should address all security layers: teaching and awareness, prevention, discovery and detection, responding, and recovery. Additionally, the eyes should be directed to design successful collaborative teams specialized in cyber security solutions (Sommestad, 2012). Figure 1 shows the estimated major disciplines that are evolving in the field of cyber-security in future.

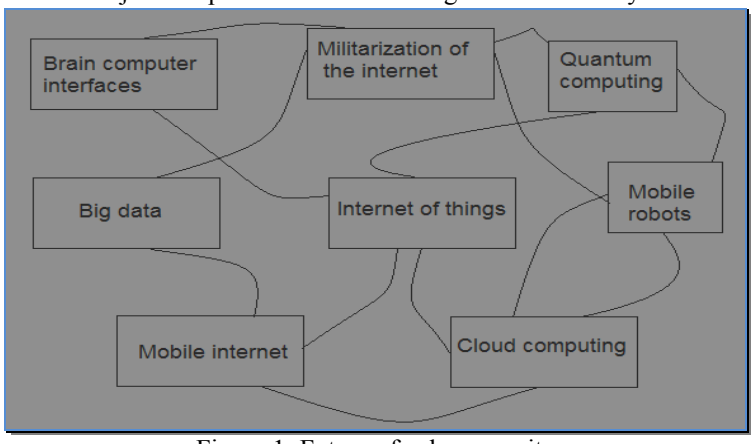

Figure 1: Future of cyber security

9. Conclusion

The understanding of cyber security threats is not only an innovative requirement but also it is a conservative task. The rapid changes in technologies and services are major driving and leading concerns to the cyber security, requiring reassessment and renewal of standardized policies for counter measures to the resistant vulnerabilities. At last, the focus on minimizing, recovering, and eliminating vulnerability is the main, essential trends and responses to the continuous increasing progress and growth in ICT structure and architecture in the security society. In conclusion, these cyber security models need to improve according to the situational awareness over all situations and at all levels in order to avoid conflicting interests and priorities.

References

Choo, K.K.R. (2011). “The cyber threat landscape: Challenges and future research directions”. Computers & Security, 30(8), pp.719-731.

Daya, B. (2013). “Network security: History, importance, and future”. University of Florida Department of Electrical and Computer Engineering.

Dhillon, G. (2007). “Principles of Information Systems Security: text and cases”. (pp. 97-129). New York, NY: Wiley.

Graham, J., Olson, R. and Howard, R. eds. (2016). “Cyber security essentials”. CRC Press.

Jouini, M., Rabai, L.B.A. and Aissa, A.B. (2014). “Classification of security threats in information systems”. Procedia Computer Science, 32, pp.489-496.

Kaplan, J.M., Bailey, T., O'Halloran, D., Marcus, A. and Rezek, C. (2015). “Beyond Cybersecurity: Protecting Your Digital Business”. John Wiley & Sons.

Koch, R., Stelte, B. and Golling, M. (2012, June). “Attack trends in present computer networks”. In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-12). IEEE.

Maughan, D. (2009). “A roadmap for cybersecurity research”. US Department of Homeland SecurityNovember, 2009.

National Institute of Standards and Technology (NIST) and United States of America. (2014). “Framework for Improving Critical Infrastructure Cybersecurity”.

Pieprzyk, J., Hardjono, T. and Seberry, J. (2013). “Fundamentals of computer security”. Springer Science & Business Media.

Pitkänen, O., Sarvas, R., Lehmuskallio, A., Simanainen, M., Kantola, V., Rautila, M., Juhola, A., Pentikäinen, H. and Kuittinen, O. (2011). “Future Information Security Trends”. Kasi Research Project, The Ministry of Transport and Communications/Arjen tietoyhteiskunta.

Sharp Sr, W.G. (2010). “Past, Present, and Future of Cybersecurity”, The. J. Nat'l Sec. L. & Pol'y, 4, p.13.

Singer, P.W. and Friedman, A. (2014). "Cybersecurity: What Everyone Needs to Know". Oxford University Press.

Sommestad, T. (2012). "A framework and theory for cyber security assessments" (Doctoral dissertation, KTH, Royal Institute of Technology Stockholm, Sweden).

Staheli, D., Yu, T., Crouser, R.J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S. and Harrison, L. (2014, November). "Visualization evaluation for cyber security: Trends and future directions". In Proceedings of the Eleventh Workshop on Visualization for Cyber Security (pp. 49-56). ACM.

Trautman, L.J. (2015). "Cybersecurity: What About US Policy?. Journal of Law", Technology and Policy, 2015, p.341.

Von Solms, R. and Van Niekerk, J. (2013). "From information security to cyber security". computers & security, 38, pp.97-102.