An investigation into the effect of cybersecurity on attack prevention strategies

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

Abstract

Our economy, infrastructure and societies rely to a large extent on information technology and computer networks solutions. Increasing dependency on information technologies has also multiplied the potential hazards of cyber-attacks. The prime goal of this study is to critically examine how the sufficient knowledge of cyber security threats plays a vital role in detection of any intrusion in simple networks and preventing the attacks. The study has evaluated various literatures and peer reviewed articles to examine the findings obtained by consolidating the outcomes of different studies and present the final findings into a simplified solution.

Keywords: Cyber Security; Attacks; Phishing; Threats; IT department

1. Introduction

Cyber security deals with issues that surround various cyber-attacks and designing of defensive strategies which help in preserving confidentiality, availability and integrity of information and digital technologies. The term Confidentiality is used for preventing the revelation of information to unofficial systems or individuals. The term integrity is used for prevention of any deletion or modification in unlawful manner [1]. The term availability is used for assuring that a system responsible for processing, storing and delivering of information can be accessed whenever required and by the ones who require them [2]. Cyber security is a cumulative term used for the collection of all processes and technology that safeguards the electronic data and computer systems. The role of definition is to explain what the term literally means but it cannot highlight the importance of cyber security in virtual world. Cyber security plays a vital role for each individual, small and medium corporation and government as well [3]. Cyber security awareness is the act of doing and knowing something for safeguarding the information assets of a business. Employees who are aware of cyber security have good idea about the various cyber threats, its impact on their business and the strategies needed for reducing and preventing the infiltration of cyber-crime into their workplace [4]. Having good knowledge about cyber security is helpful in detection of various malicious events but situated idea about a particular network helps in making precise decisions.

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

2. Literature Review

This section of the paper discusses and critically reviews the literatures that has explored the importance of knowledge among the users to prevent the cyber security threats. According to a study by Bada et al. (2019) the extent and rate of changes taking place in cyberspace is quite unpredictable and variable when compared to any other environment which is associated with physical limitations. The service providers, network topology and the ones using the services are undergoing constant changes. This result in the emergence of new vulnerabilities and required strategies to deal with them are also being developed [4]. This requires the cyber security expert to have updated knowledge about ways to defend their network. They constantly supervise the network, identify the various threats, and repair the vulnerabilities. The attacker on the other hand looks for a single vulnerability which they can exploit [3]. This clearly indicates the asymmetric association between the attacker, the complicated environment and the security analyst. As described by Hadji kyprianou [5] the key responsibility of the analyst is to make interdependent and multiple decisions within the dynamic environment. Making dynamic decisions is a complicated process as it requires knowledge about interrelated and multiple attributes along with the ability to predict the environmental developments. In some cases, the decision maker plays a significant role by taking the right decisions at the right time for maximizing the decision value [5]. According to David et al. [6] domain knowledge is described as the basic knowledge acquired via deliberate and long learning. It also comprises of theoretical knowledge acquired by the expert via certification, training, or formal education. Practical knowledge acquired via experience and hands-on practice with the help of workflows, modes of operation and tools is also included in domain knowledge. A cyber security analyst acquires the required knowledge from domain knowledge gained via formal learning [6]. Nevertheless, it has been seen that domain knowledge is not enough for detecting cyber-attacks in an operational environment.

As per the study by Fraser [7], the analyst apart from domain knowledge also requires situated knowledge. It is organization based, difficult to articulate and is implicit in nature. This knowledge pool is dynamic in nature and is acquired by experts by constantly interacting with a particular operating environment. With respect to network and information security, adjusting and tuning of the IDS is important for learning a network's nuances so that the threats can be detected and the security needs of an organization can be met successfully [7]. Thus, it is important for the analyst to have complete idea about operating IDS to detect the network threats effectively. Cyber-attack is the most common risk which every business faces today. As per the study by Zwilling et al. (2017) back in 2017 in the UK it was seen that cyber-attacks cost amounted to £10 billion. Also, 7 out of every 10 companies were victimized by breach or cyber-attack. Data Breach Investigations Report from the year 2017 showed that most of the cyber-attacks were the result of human error indicating that these mistakes amplify and cause cyber-crime. Thus, an organization can deal with these threats by creating a risk-aware culture in the workplace which begins with awareness regarding cyber security [8]. Cyber-attacks can be classified as abnormal network activities. Thus, analysts must be capable of differentiating between abnormal and normal network activities and use them for detection of attacks. It should be noted that an activity can be normal in a specific environment but malicious in another. Thus, detection of intrusion will depend on integration of situated knowledge and domain within a dynamic environment [9]. Using the ethnographic

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

qualitative research approach for understanding the general workflow and mental model of cyber security analysts requires measures of performance and quantitative tools for analysis and evaluation of the processes for intrusion detection.

In the current scenario of development in information technology field, opting for a well-explained training program on cyber security for all employees across all departments is a necessary step that each organization shall focus on. In order to secure the company's data, enforcement of training cum awareness program for cyber security shall be on top priority list. It is a prevailing myth that such training events will be beneficial for only IT department [10]. The findings from most of the literatures have highlighted the fact that the role of knowledge in minimizing the cyber threats is extremely crucial. Review of literatures shown above has illustrated that the data compromise occurs from human errors, irrespective of their department [4]. This is a serious issue that organization must prepare a cyber-information enabled task force to fight the intruders and identify the loop holes at an early stage.

3. Methodology

The study has used secondary research methodology to explore the effects of knowledge in cyber security attack prevention. The key source of secondary data are the literatures associated with websites, newspapers, newsletters, magazines, proceedings, periodicals, articles, books, journals and other relevant sources had been considered from the industrial sectors. Data acquired from working documents, procedures, manuals, case study reports, policies, and regulations is also be considered for this study. The findings from these types of sources are consolidated, critically compared and contrasted and the final outcome is drawn.

4. Results and Analysis

The way the user detects malicious events depends on their pool of knowledge which helps them in interpreting a network event. They can then also understand the connections existing between the various attributes which lead to an event and judge it with respect to a particular network activity. The results from the primary sources like study by [10] and [11] illustrated the users who have previous experience have good understanding of the link between the network load, IDS alert and operations of the network [10]. The rate of false alarm is lower, and the hit hate is higher for them when compared to the beginners. A case analysis report conducted explored the similarities between the performance of beginners and experts while detecting a cyber-attack. The findings showed that the users with expert level knowledge perform well when the stimulus is found to be static and much better when the decision is associated with a judgement and not the behavior or process. This justifies the lower performance by experts, but it also highlights some of the environmental aspects that obstruct the experts from making the most of their existing knowledge and experience [11].
The reason can be that the experts were pulled away from a known operational environment which resulted in lack of situated knowledge. Thus, the significance of situated knowledge is quantitatively confirmed by this finding acquired from existing qualitative studies. Lack of situated knowledge and dependency on domain knowledge hampered the ability of the expert to assess the network event sequence [12]. A study by Vozikis et al. [13] showed that indicative events that popped up at the end of network scenarios (Stealing of Confidential Data scenarios and DoS) benefitted the beginners while

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

detecting a cyber-attack. The model developed below shows the scenario of Stealing of Confidential Data and DoS attack [13].

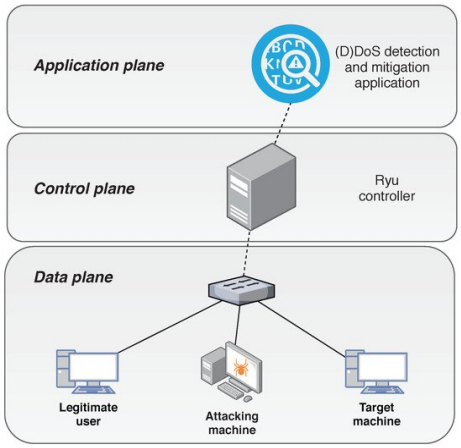

Figure 1: DoS Attack prevention model [13]

According to the studies, the findings were slightly contradictive from that of [10] and [14]. The key results indicated that beginners were highly skilled than experts in judging a network scenario even when limited evidence is available. This is because they made the decision about a cyber-attack after studying the various network events. Nevertheless, experts are expected to observe a cyber-attack faster than the beginners and prevent any damage by restricting the spread of the attack throughout the network. The experts were seen to be sensitive to the order of the events that took place within a particular scenario. According to one of the participants of the study by Wirth [15] reflecting on classification of a DoS network scenario under cyber-attack, '*The sequence of connections showed that the attacker exploited the workstation of a user via the webserver and used it for accessing the fileserver and installed a backdoor on this webserver.*'

It is quite interesting that the expert highlights an action taken by the attacker and not a particular network event attribute such as load. It is highly contradictory to the explanations given by beginners as they were basically concerned with the network event attributes. The literature and previous studies have shown that beginners also exhibit a confidence level similar to that of experts which negates the logic that experts are overly confident. This can be explained in two ways [13]. Firstly, it is a great possibility that the situated knowledge of experts contributes largely to their overconfident nature. A study by Yunos et al. [12] showed that a cloud-based data is compliant to the GDPR regulations and is safe [12]. A continuous interlocked process helps in providing a detailed procedure for cyber security threat prevention even among the common users. The model developed illustrated that we also need to ensure that all employees have clear idea about the strategies and their responsibilities.

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

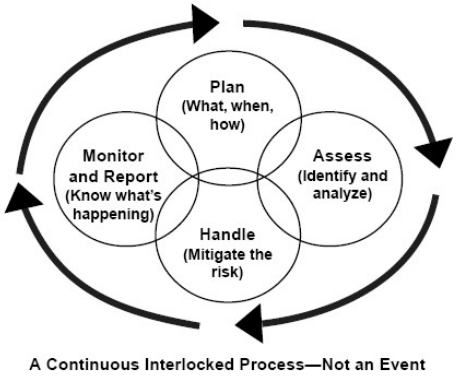

Figure 2: Interlocked process for Cybersecurity [4]

Secondly, it is also possible that cyber security experts just like experts from other domains seem to be conservative and cautious [10]. The reason behind this cautious behavior seems to be associated with a precise understanding of the consequences of taking wrong decisions with respect to cyber security. Users with better knowledge present higher confidence levels while deciding on an attack compared to their poor confidence levels while concluding that no attack has taken place supports the idea that cyber security analysts exhibit cautious behavior while supervising a network [3]. The results of Renaud et al. [10] showed that the weakest aspect of cyber security is faulty human resource. Renaud et al. [10] developed a DDoS mitigation model and the analysis and outcomes showed that employees who are unable to make educated and informed decisions about connecting to the right network or attaching an email at the right place can led you to the risk of cyber-attacks [10]. The cyber security of your business is quite important and it is the responsibility of everyone to develop a risk aware culture within the workplace.

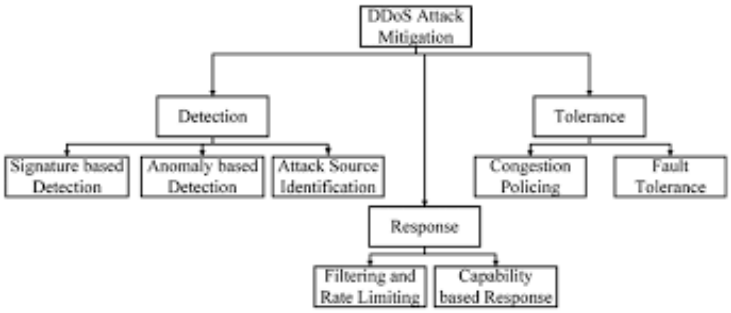

Figure 3: Attack Mitigation [10]

In the current scenario of development in information technology field, opting for a well-explained training program on cyber security for all employees across all departments is a necessary step that each organization shall focus on. In order to secure the company's data, enforcement of training cum awareness program for cyber security shall be on top priority list. It is a prevailing myth that such training events will be beneficial for only IT department. However, report by Sallos et al. [16] highlighted that over 90% of data compromise occurs from human errors, irrespective of their department [16]. This is a

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

serious issue that organization must prepare a cyber-information enabled task force to fight the intruders and identify the loopholes at an early stage.

5. Discussions

The evaluation of this paper has illustrated the fact that a strong knowledge base and an effective ways of knowledge sharing can turn out to be a greatest solution for Cyber Security Threat Preventions in business organizations. It is the mechanism and collective ways to protect the organization data and assure that they are not accessible to unauthorized personals. It safeguards the system from spyware, malware, hackers and varied other malicious way that try to intrude the system. One shall not neglect and compromise with organization security. Data breach is generally the result of errors on user's side, but proper training and guidance to follow protocols and security norms can reduce such incidents to large extent [17]. Employees must be equipped with regular training course, recognizing phishing entities, emergency drill practice related to data breach and other such activities. This will instill the sense of paying attention to cyber security from top to bottom of the organization [14]. Today, companies who are willing to safeguard their data must educate their employees and colleagues to develop a workplace culture which is aware about cyber security [5]. Following are some of the best cyber security practices which can act as a knowledge base manual or a set of practices for the users:

Implement basic cyber security training: Carrying out training sessions ensures that the employees deploy only approved software and keep strong passwords. Implementation of common-sense practices associated with access to technology and safeguarding staff is also a good idea [18]. It can be done through a number of simple steps like not allowing the employees to use office laptops at home during the weekend or deploy a verification process.

Detect and plan: It is the job of the hackers to keep looking for vulnerability, but experts must ensure that there is adequate knowledge and resources for detecting their activities. This helps in preventing damage and resuming business without encountering any huge loss [16]. Deployment of a security information and event management (SIEM) solution helps in analyzing the data acquired from operating systems, network infrastructure and applications and flag them to the best people.

Invest on VPN Technology: No matter how extreme measure the company takes to protect the office data, you do not have control over the outside network. Using free public wi-fi is a big threat. Many a times, a staff may be working remotely and may use hardware or network that are not within the organization security check. Using such networks could pose a big threat to the entire system. Using a VPN for such cases is a perfect solution [9].

2-Factor Authentication: With the habit of accessing data at the click of a button, may be a risky affair. Ensure that all logins to the system enforce 2-factor authentication process. It could be combinations of captcha, SMS, OTP, email verification and others. To further secure the process and depending on the usage, organization can also think of implementing biometric approval or other security key measures [12].

6. Conclusions

The outcomes of this study show that practical knowledge and expertise have a significant role to play in triage analysis: classification of network events into threats and links between the decisions and

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

regarding attacks based on a set of network events. Talking with respect to cyber security, collecting information about network events serves as the basis for taking decisions about the entire event [17]. Every network event is treated in the same way in this study which means that we do not believe that some of the events are capable of providing more information when compared to others. The expertise of an individual determines the identification of a critical event and supervising them can cause the decision maker to be biased. The finding serves as a benefit for the experts particularly if they can correct informative events correctly. This limitation will be addressed in our upcoming work by focusing mainly on experts and using long network and complicated scenarios.

Also, adequate studies are required for evaluating the process of information accumulation before any conclusions are made and the process of synthesizing the decisions about multiple events. This study will also focus on the possibility which indicates that every network event comprises of a distinct weight and contributes to the final decision about a network scenario. Apart from practical experience and theoretical knowledge, analysts must learn to adapt quickly to dynamic and novel environments [13].

It is important to expand and update their situated knowledge about operational environments. Information about the function and importance of network servers is not collected systematically within a repository and on collection it becomes static and obsolete as the network keeps on changing with change in equipment and modification of existing equipment. Situated knowledge is the most significant pre-requisite for mission-oriented and comprehensive situation awareness [4]. Lastly, there has been a significant rise in the personal networks that are being deployed by end-users. Thus, the variety and increasing number of devices connected to the networks and their complicatedness can make intrusion detection a concern for most of the end-users without any knowledge about network and information security.

References

[1] AlMeraj, Z., Alenezi, A. K., & Manuel, P. An organizational cyber security readiness model: Towards secure IoT foundations.

[2] Al Shamsi, A. A. (2019). Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE. *International Journal of Information Technology and Language Studies*, *3*(2).

[3]. Cardenas, A., & Cruz, S. (2019). Cyber-physical systems security knowledge area. *The Cyber Security Body Of Knowledge (cybok)*.

[4] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. *arXiv preprint arXiv:1901.02672*.

[5] Hadjikyprianou, M., & Hadjikyprianou, G. (2018). The Race Against Cyber-Crime and the Importance of Cyber Security for Governments and Companies: A Case Study for the European Union With a Particular Focus on the Republic of Cyprus. *Cybersecurity, Privacy, & Networks Journal, Forthcoming*.

[6] David, D. P., Keupp, M. M., & Mermoud, A. (2020). Knowledge absorption for cyber-security: The role of human beliefs. *Computers in Human Behavior*, *106*, 106255.

[7] Fraser, D. (2020). Analysis of Quantitative Data: Cybersecurity Knowledge and Skills.

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020

[8] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 1-16.

[9] Pingle, A., Piplai, A., Mittal, S., Joshi, A., Holt, J., & Zak, R. (2019, August). Relext: Relation extraction using deep learning approaches for cybersecurity knowledge graph improvement. In *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 879-886).

[10] Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security?. *Journal of Intellectual Capital*.

[11] Sharma, C., & Maurya, S. A REVIEW: IMPORTANCE OF CYBER SECURITY AND ITS CHALLENGES TO VARIOUS DOMAINS.

[12] Yunos, Z., Ab Hamid, R. S., & Ahmad, M. (2016, July). Development of a cyber security awareness strategy using focus group discussion. In *2016 SAI Computing Conference (SAI)* (pp. 1063-1067). IEEE.

[13] Vozikis, D., Darra, E., Kuusk, T., Kavallieros, D., Reintam, A., & Bellekens, X. (2020, August). On the importance of cyber-security training for multi-vector energy distribution system operators. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-6).

[14] Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., & Zak, R. (2020). Creating cybersecurity knowledge graphs from malware after action reports. *IEEE Access*.

[15] Wirth, A. (2016). The importance of cybersecurity training for HTM professionals. *Biomedical Instrumentation & Technology*, *50*(5), 381-383.

[16] Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. *Journal of Intellectual Capital*.

[17] Tarter, A. (2017). Importance of cyber security. In *Community Policing-A European Perspective* (pp. 213-230). Springer, Cham.

[18] Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, *2019*(8), 11-14.

DOI: https://doi.org/10.54216/JCIM.030203
Received: January 07, 2020 Revised: April 06, 2020 Accepted: April 20, 2020