International Journal of Multidisciplinary Innovation and Research Methodology (IJMIRM)
ISSN: 2960-2068, Volume 2, Issue 2, April-June, 2023, Available online at: https://ijmirm.com

Cyber Security Risks for Global Businesses and Solutions Expected

Sultan Aljabri[1], Ahmed Almalki[2], Amro Altalhi[3]

[1]Trainer, Sultan Aljabri (Technical College in Alais), Saudi Arabia
[2]Trainer, Ahmed Almalki (Technical College in Almandaq), Saudi Arabia
[3]Trainer, Amro Altalhi (Technical College in Almandaq), Saudi Arabia

ABSTRACT

The use of the internet and its applications in businesses are increasing with the advent of modernization and ease of access of the internet. The cloud-based platforms are helping organizations to limit flaws and to improve their quality and communication. Every technological advancement has its own advantages and disadvantages involved and this research paper is aimed at investigate the cyber security issues and their effects on processes, people, and technology. The research highlights the expected and proposed solutions to overcome these issues as well. In the same manner, the future prediction to the problem along with their solutions is the part of this study. The major issues associated with cyber security highlighted in the paper are data breaches, CEO scams, Mining crypto currency, misuse of employee privileges, BYOD, and various hacking techniques. With that the paper also spread light on the solutions that that assist businesses to ensure secure cyber operations like integrated Fire eye solution, security results for industry and infrastructure, and data encryption products. The research concludes that the Cyber security is actually the protection of systems connected through internet. It protects all the hardware, data, and software present in these systems from cyber attacks such as MITM attacks and DDoS attacks.

Keywords: Cyber security, scam, fraud, password, encryption, data security, application, internet, breach, attacks, artificial intelligence, confidential data, crypto currency, cyber security issues

INTRODUCTION

The use of the internet and its applications in businesses are increasing with the advent of modernization and ease of access of the internet. Businesses are using the internet for various applications such as managing customer data, inventory management, in production systems, and almost every industry around the globe is using such systems to improve the speed and quality of its services (Byres and Lowe, 30). The cloud-based platforms are helping organizations to limit flaws and to improve their quality and communication. Likewise, these systems are helping organizations to track their customer likes and dislikes and they can easily improve their service structure based on their customer feedback. All such innovation and advancement are by the virtue of the internet. However, every coin has two sides and the darkest sides of cyber systems is the privacy and security issues related to these systems. The essence of these issues is to access data of internet-connected systems through un-authorized manner to use it for criminal activities such as blackmailing, ransom, and extortion. Moreover, businesses can steal data of their rival through these attacks to determine their strategies and plans (Cebula and Young, 112). The major aim of this research is to investigate the cyber security issues and their effects on processes, people, and technology. The research highlights the expected and proposed solutions to overcome these issues as well. In the same manner, the future prediction to the problem along with their solutions is the part of this study.

Cyber security issues and their effects on people, technology, and processes:

Some of the most prominent and the most significant cyber security issues along with their impacts on people, processes, and technology are listed and briefly described below.

Data Breaches:

Data breaches and the loss of precious data is one of the major security and privacy issue related to cyber systems. It has adverse effects on people, processes, and technology. Data breaches are one of the most common issues when it comes to internet connected systems as it compromises the privacy of data and it can cause immense damage to person and businesses. Attackers play a vital role in data breaches as they are spying the activities of the users and they insert their data or simply steal the data when they need (Sommestad, Ekstedt and Johnson, 55). For instance, a person buys something from an online shopping store and he has to pay the amount in the account provided by that store. The hackers are continuously noting the conversation between the two parties and they stay hidden so that no one can identify their existence. They change the account information of the store sent to the customer for making payment and then alter the account number with their personal account numbers and in this way, they steal the money. Likewise, the confidential and top-secret data of business organization and even the law enforcement agencies like the CIA is breached using various cyber attacks like MITM. The data are then used for terrorists' activities and other such illegal activities. The details of data breaches show that data breaches always have negative effects on the lives of people, processes, and technology. Likewise, data breaches are lethal for global businesses.

CEO Scams:

CEO Scams are another significant cyber security issue. The CEO Scams are becoming popular with the passage of time. However, these frauds require high level computing and hacking skills and abilities. The hackers have to examine the internal language and the security protocols of the organization for a little while (Von Solms and Van Niekerk, 88). The keep on examining till they get access to these protocols, and then they change these protocols urging the employees to transfer funds in their fraud accounts. This process is difficult; however, it seems very simple. Then they use the same domain that is actually the primary or the principle domain used by the company to send legitimate emails to their employees (Von Solms and Van Niekerk, 88). The hackers send such emails to employees to provide confidential data of the organization and to make transactions in their fake accounts. They use fake emails in this context, but when they use the same domain, then it becomes are a hard nut to crack to identify those emails. The hackers use such strategies with the combination of Artificial Intelligence techniques to analyze the large number of emails to determine the internal language and tend of the organization and the targeted persons so that they can speak in the same manner. It is one of the most trending scamming methods used by the hackers in the contemporary world and it is the hard way to catch such attackers.

The effects of this cyber security issue are disastrous and it can ruin the entire organization financially and morally. The organizations think that the employees are not faithful and they don't liable for this loss and the employees feel the same safe due to these attacks. Likewise, the loss of confidential data of staff and customers can cause various legal difficulties for the organizations as well (Von Solms and Van Niekerk, 88). It delays the processes and imparts negative impacts to the technology used by the respective organization and its information system.

Mining Cryptocurrency:

Cryptocurrency is becoming popular in the contemporary world and it is replacing the traditional currency notes as the trend of using an electronic currency in businesses is becoming popular. The trend has increased, especially with the advent of Bitcoin in 2009 that is the most popular form of cryptocurrency. The hackers are taking good advantage of this currency and they are mining it to earn Bitcoins (Ralston, Graham and Hieb, 99). This strategy is helping them to make crypto-buck at a rapid pace and they are stealing money from organizations, individuals, and even from governments. The process of mining crypto currency is simple, as they just need to design or to access a powerful malware that can run in the background on the computers of their victims. The victims are very unaware of this fact that some malware is running in the background of their device and their money is being looted continuously. The effect of this cyber security issue is lethal and it is the major cause of the decline in the reputation and use of crypto currency around the globe. The organizations and individuals and even the governments are reluctant to use this form of currency for transactions, as they are not sure about the safety and security of their money. Likewise, such attacks can ruin an individual and an organization financially as they the hackers can loot their entire Bitcoins.

Misuse of employee privileges:

Another most significant cyber security issue in global businesses is the misuse of employee privileges. It is seen that this issue is trending with the ease of availability of the internet in the organizations. Most of the employees are using the company devices for non-work purposes and in such locations that are not secure. Most of the devices are vulnerable to serious security threats and they have fragile security systems that can easily be hacked. The misuse of the company owned devices could pose serious threats and security risks to the internal infrastructure of an organization. It is the responsibility of the management and the IT department of the organizations and businesses to limit the access of un-authorized employees to these devices. Only the authorized people should have access to the confidential data of the organization and the IT department should keep track of the activities of the employees so that they cannot misuse their privileges.

BYOD (Bring Your Own Device):

Bring Your own Device (BYOD) is another cyber security issues that are causing serious issues in the global businesses. It is the strategy used by most of the organizations that the employees are allowed to bring their own devices in the organization and there is no concept of company owned devices. Most of the devices are vulnerable to the security threats and they have no capacity to deal with malware. Such devices result in serious security threats like hacking and data breaches. The confidential data of the organizations are compromised. In the same manner, every device has the password of the major domain of the organization. People can use it or even sell to the other organizations in case of blackmailing or bribery. Likewise, these devices can be used to hack the entire domain and to weaken the security protocols of the business organizations.

Hacking (DDOS, Cookie Theft, Key Logging):

Hacking and especially the ethical hacking is one of the most significant issues faced by the business organizations, individuals, and governments around the globe. The major cause of such issue is that the internet-connected systems are not secured and there is no backup and recovery plan at all. In the same manner, the domains are not encrypted and people are not using authentic tools and browsers for search and other such activities. The hackers are the attackers who can use cookies, key loggings, and various other things to compromise the safety and security of the user account. Man-In-The-Middle (MITM) and DDOS attacks are the most commonly seen attacks in this regard and the major aim of these attacks is to steal data and money. The effect of this type of cyber security issue has been always negative on people, processes, and technology as these attacks always causes severe damages in terms of finance and ethics (Amin et al., 90). Encryption and other such techniques like changing protocols of the system can helpful in this context.

Solutions:

In the activity of cyberspace, cybercrime attacks on every organization and firm. There are specific resources available which can assist to secure the business systems. For the development of the websites, every company should use software of anti-piracy to decrease the threat of the cybercrime and other activities. The companies have to need to employ some specialist in computer and network security systems; these people protect the company' website from these threats by using some robust strategies and planning. The employees also monitor the activities and content of the company. Furthermore, it is recommended to the companies to enter into the organizations or international groups to reduce the threat of piracy and assist in creating an international law against cybercrime to protect the environment of the companies. The method of alternative infiltration can get quickly around the current antivirus which works to catch these hackers. Also, the latest information technology and software system can fulfill the requirement, and the small and big companies are looking for the latest update to more secure their system.

Current plans to mitigate/control the risk:

Integrated FireEye solution:

In the critical situation, the Fire Eye solution can be used to protect the organization control system and infrastructure in non-invasive. According to the federal regulations and industry standard, this software can also monitor all the activities and protect the environment of an organization. The FireEye software includes many parts of the comprehensive solutions. In the current security environment the components are easy to install individually for smooth working. The FireEye solutions usually start from the Mendicant ICS Health Check which consists the interview of the employees, contextual assessment of related threats and custom risk, and revision of the architectural graph of an organization (Aziz, 88). The next step of this solution is to examine the system performance manually and analyze its networking traffic with related technology.

The FireEye solution system provides intelligence in the organization on a cyber-system, ICS risks, information technology and automation, also provides capabilities to the team of an organization about targeting threat. This service of subscription informed the organization that who they are, what are they later and now, so the organization can make better strategies and decisions to improve the networking systems from threats. In the Belden integrations, the FireEye solutions find OT system using with IT system to reduce the significant threats.

The "Cloud-based FireEye TAP" system take assistance from numerous sensors globally and integrate it into the systems of IT and OT in order to reduce the threats (Aziz, 88). Integration between the Threat Analytics Platform (TAP) and Belden portfolio, the Xenon industrial security appliance can identify the threat of malicious activities with the help of ICS protocol.

Security results for industry and infrastructure:

In the global entities, the FireEye considered as one of the best solutions, which is used to reduce the threats of advanced attacks, along with identifying the risks and controlling the networking system .The consultancy provides an appropriate testing service to make the consumers more secure from the threats and meet their needs (Aziz, 88) . Partnership with the OT integrations allows analyze, prevent, respond, and detect the future risks which move literally from the OT to IT network. The fully developed integration, biological infrastructure has been deployed and saved the ICS network with the help of risk management solutions from IT to OT environment.

Data encryption products:
Protect data on the networking system, storage devices, desktop, mobile devices and laptops.

Data Leakage products and Support:
Provides management, monitoring and the safety of data, even though it resides, and restricts its information from printed, copied and emailed (Aziz, 88).

Mobile device protection:
Its help to the public agencies to keep their mobiles secure at BYOD.

Defense-in-depth:
Identify the networking system which allows the agencies to cope with cyber-attacks and data loss, and it increases productivity against any damages from viruses and other threats (Aziz, 88).

Future prediction on Cyber-security policies in Invensys Company:

Introduction of Invensys Company:
Invensys Ltd was a multinational information technology and engineering company, its head quarter is situated in London, United Kingdom. The company offers the cyber security portfolio and the primary goals of this cyber security portfolio is to deliver the security complaints, solutions (Roy, Kim and Trivedi, 129).

Hardening services:
The system of hardening documentation is a process of the system configuration of documents and protect against unauthorized access to make stronger the systems.

NERC GAP analysis:
In the NERC GAP analysis, the review of the current system in under the NERC CIP compliance instructions (Pfleeger and Caputo, 56). The GAP analysis will be the result of the documentation, which will help further explain the NERC compliance program.

Event Logging:
The performance of event logging on the network is an important source of tracking and analyzing cyber security events for analysis, modifications, and troubleshooting. I/A cyber assets is a system which can move security events on the main monitoring server, in which the main monitoring server will collect information from the different systems and provides notification of the selected events. After the date, it can allow saving the analyzed data.

Patch management:
Patch management is one of the essential features to find missing patches. It is stated that missing patches are the only main reason for breaches of networking security. The team of Invensys Cyber security identifies the threats with the help of automation detection and installation of missing patches.

Remote Relay Access Server:
A remote relay access service will be connected to the remote access association with I/A remote views, HMI remote access. To protect the cyber assets access to the business network in ESP zone, the consultant of Invensys cyber security installed a standard access platform as a relay server.

Access control firewall:
The cyber assets connected with the processing control and it need to share data with assets on both trusted and not trusted network (Roy, Kim and Trivedi, 129). To stop the attacks of the cyber system, the security solution will organize to control the zone approach, in which the assets of the security system will be grouped to create a secure form zone.

Managed security services:
The processing control networking act as an affected environment that requires a solution to secure the information technology systems, it is generally unavoidable in the process of environmental control. For careful development, some standard techniques and tools can be used to protect the system of process control (Ericsson, 100).

SOP (Standard operating procedure):
Design and deployment are based fundamentally on SOP aka standard operating procedure, it is also referred as the 'cyber security software' (Ericsson, 100).

Policy and procedure development:
The consultant of Invensys cyber security conduct interview with employees, revision of different documents and apply excellent practices to create strong policies and procedure for the development of the client's cyber security system (Ekstedt and Sommestad, 88).

My Opinion:
Examining the cyber security solutions, I personally believe that Fire Eye solution is a bit overpriced and the services generated by it are expensive as compared to the other solutions available in the market. Moreover, I personally believe that even though there are numerous technologies and cyber security solutions available, however, there is no exemplary or gold solution to protect organizations from an attack. To get protection against all cyber vulnerabilities, a multiple dynamic approach is required, which involves people, processes and technology. I believe that cyber security metrics are an effective way to know which cyber security solutions work best for the organization. Therefore, establishing and using effective cyber security metrics can assist in generating accurate measurements regarding the functions of the organization and help individuals determine the sort of improvements that are required. These security metrics could help individuals and organizations in determining the amount of systems that have corrupt or expired applications and configurations installed, moreover, it will also assist in pointing out the number of people having access to wrong or faulty links along with identifying the number of false and correct incidents reported every month. Therefore, I think that integration of such data, which is accessible in every cyber security program, should be used to develop metrics, this would also generate guidance, information and would help in reducing cyber security concerns.

CONCLUSION

It is concluded that the Cybersecurity is actually the protection of systems connected through internet. It protects all the hardware, data, and software present in these systems from cyber attacks such as MITM attacks and DDoS attacks. The hackers have to do tough struggles to access the passwords of the executive management of the respective organization.

WORKS CITED

[1]. Amin, Saurabh, et al. "Cyber security of water SCADA systems—Part I: Analysis and experimentation of stealthy deception attacks." IEEE Transactions on Control Systems Technology 21.5 (2013): 1963-1970.
[2]. Aziz, Ashar. "The evolution of cyber attacks and next generation threat protection." RSA Conference. 2013.
[3]. Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.
[4]. Cebula, James L., and Lisa R. Young. A taxonomy of operational cyber security risks. No. CMU/SEI-2010-TN-028. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2010.
[5]. Ericsson, Göran N. "Cyber security and power system communication—essential parts of a smart grid infrastructure." IEEE Transactions on Power Delivery 25.3 (2010): 1501-1507.
[6]. Ekstedt, Mathias, and Teodor Sommestad. "Enterprise architecture models for cyber security analysis." Proceedings of the IEEE/PES Power System Conference and Exposition (PSCE'09). 2009.
[7]. Pfleeger, Shari Lawrence, and Deanna D. Caputo. "Leveraging behavioral science to mitigate cyber security risk." Computers & security 31.4 (2012): 597-611.
[8]. Ralston, Patricia AS, James H. Graham, and Jefferey L. Hieb. "Cyber security risk assessment for SCADA and DCS networks." ISA transactions 46.4 (2007): 583-594.
[9]. Roy, Arpan, Dong Seong Kim, and Kishor S. Trivedi. "Cyber security analysis using attack countermeasure trees." Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. ACM, 2010.
[10]. Sommestad, Teodor, Mathias Ekstedt, and Pontus Johnson. "Cyber security risks assessment with bayesian defense graphs and architectural models." hicss. IEEE, 1899.
[11]. Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." computers & security38 (2013): 97-102.