Nathaly Flores

CYSE 605

Final Paper

Old Dominion University

Security Awareness Program

Introduction

The Chief Information Security Officer (CISO) is the President or CEO of a company. The executive role's duties are to execute a security awareness program, creating procedures and methods that will adequately make awareness and educate the entire firm workforce spanning all divisions, departments, and office sites. The security agenda choice is to promote a wholesome security awareness program under control with all the finest international security methods implemented. The Chief information security officer oversees a company's network security and promotes new hires to maintain security systems that protect all its trade secrets and goods. The Chief information security officer amends the existing plans for the latest prospects. A superb imitation infrastructure should contribute but also assure the Company can connect to the cloud. The expansion is permitted and vital. Heightening the information security plan is critical for defending data storage; this is very needed in a commerce enterprise. It uses a suitable security plan to ensure a whole content process that demands determining functions, procedures, and measures to create a new IT security system for a company.

The Duties of a CISO

All companies must recognize and enforce information security guidelines, criteria, policies, strategies, and techniques to improve security enterprise duration defending their objectives and statement. The organization's vital information and workspace are secure. Safeguarding the susceptibilities are kept in the data storage domain and instructs employees about data security and privacy threats. To control all-inclusive data security compliance, all corporate divisions form a Chief information security Office CISO (Tu & Yuan, 2014). The

CISO supervises all the corporate security agendas. The most vital goals of an information security program are the five detailed below:

1. The Company's objective is to guard and oversee all bodies of information. The Company's director must undergo an extreme data security and risk assessment annually. as soonest the management and privacy agendas are approved, it is feasible.
2. The resource control team ought to analyze to secure the Company's guidelines and security practices are obeyed. A corporation accepts and does not yield sway over this connection; therefore, the information security officer must always brief the person liable for embracing new processes and not to a division.
3. The CISO must comprehend the Company's roles and task segments and roles. Employees must be conscious of the growing technologies to enforce new security measures if they are accountable for being a threat pinpointing practices for the organization and noticing and recognizing hazards. The company administration knows the Company approaches by comprehending the tactical risk analysis.
4. The ground for a company's leadership is to design a plan so everyone can communicate their ideas and opinions successfully.
5. Technological capability is vital for a Chief Information Security Officer to guide a security industry. It demands a fundamental knowledge of technical problems, firms, and corporation policies. Earning respect with technical security skills is simple for a security manager.

The central function of a company's needs mainly defines the centralized information technology system. Information technology arises in the middle of the organization format founded on the content of Information technology and Cybersecurity; it vastly contributes to the companies, and it is rare for the senior executives to convey different classes of a matrix. Pivoting on the length and complexity of the companies, explicit connections between line managers and the CEO are helpful. The proportion of concentrated versus decentralized determinations is related to the class of a company's anticipations.

Risk Management

All aspects of risk governance for a company's acquisitions, including computer systems, people, facilities, and other acquisitions, are under security control. Security administration procedures seek to bring the cornerstone of cybersecurity practices. Those methods permit an organization to effectively detect potential threats to its resources and organize and categorize acquisitions as per their value to the organization and degree of susceptibility founded on their probability of misuse and the possible effect on the organization. Without a footing, guiding for cybersecurity entanglement can be very challenging. On the contrary, thrusting a strict security framework to correspond with the companies thoroughly corporation, specialized and legal regulations may take much work. Data grows into a less reachable security procedure and evolves into a more robust and companies' performances plunge. When security defenses become more neglectful than they should be, the threat of information loss and corruption skyrockets, which can hinder production.

Information security created the CIA Triad as a conception to earn resistance. It demands companies' actions to safeguard their information. Confidentiality, Integrity, and availability, known as CIA in Cybersecurity, are the three columns of a security architecture. Only authorized persons have admission to or permission to edit information. Only some people are handed that responsibility. as stated, confidentiality and Integrity promote information reliability by securing the proper state and impenetrable. Authorized personnel must be able to have admission to data when they need to, which is why availability necessitates. Security experts evaluate threats and susceptibilities and assess their effect on a company's acquisitions (IntelliPaat, 2022). Therefore, the CIA Triad thrives at every infosec specialist's priority checklist.

Training is probably ignored with time. A security awareness program should be constantly trained. Individuals are progressively under strain to increase performance. Therefore, security is viewed as a waste of time and an inappropriate obligation, and they pursue ways to get around it. People's intentions intensify after an incident, as indicated by the US security hearings after the 911 attacks and the following steps. There are no differences in the case of an incident entailing data security. It does not matter what kind of organization we work for; employees are the first line of safeguarding. The significance of the broad data security agenda relies on the operation of the security awareness program (Wright, 2008).

There are numerous kinds of security awareness training. How education/training is provided, designed, and dispensed will greatly influence its capacity to enhance security outcomes in the Company.

Objectives and Roles for training in a Workplace

Corporations, companies, and government bureaus progressively utilize computers and the internet to acquire combative benefits over their rivals. Technology development, especially the launch of innovative computer networks and communications devices, is vital, spanning transmission intermission between individuals globally (Li, et al., 2019) additionally, technological development has lessened transmission obstacles between people, improved regulation, and enhanced operation procedures. The assurance of cyber threats comes with technical development, which has extensive repercussions for corporations and firms. Cybersecurity threats/attacks the consequences can be economic flops for a business by acquiring client data and damaging a business trademark, spoiling clients' trust (Johnson, 2016). Because of the shortage of teaching, training, of cybersecurity awareness, cyber threats are out of control in today's society. Employees and technology customers constantly ignore security standards and safeguards (Li, et al., 2019). Embracing cybersecurity awareness training agendas is an excellent method of improving companies' and government establishments' organizing and preventing cyber-attacks while enhancing the methods' security. Concentrating on examining the function of cybersecurity awareness and why training employees and educating them can benefit any company in handling cyberattacks.

How vital is a Cybersecurity Training

Cybersecurity and information security are at the vanguard of everyday exercise. Worldwide everything has altered, as well as standards of stealing or sabotaging private, susceptible, and confidential data. It has turned almost unthinkable to go without hearing about a virus or hacking. Cybersecurity enterprise is embarking on political intrusion, machine understanding/artificial intelligence, and the cybersecurity mastery intermission (Marr, 2020).

Nevertheless, with numerous cybersecurity improvements, information violations remain an endless battle. Yearly, organizations execute compulsory online security training. These trainings are about an hour long, encouraging employees to create a unique password with special characters, not to save passwords into the website memory, and not share passwords with others. The training also incorporates a quiz to test the worker's understanding and satisfy a passing score. With workers trying to fight security breaches, internal security crises and external attacks have stayed the same.

Indicating that security breaches have not declined, there is no reason to say that cybersecurity training is unneeded. Cybersecurity awareness education is vital to defend a company's systems. Training and educating workers on various cyber security risks and threats/attacks to ensure they are taught about these risks is the best technique and policy for maintaining networks and information from any harm. If one fails to maintain from cyber threats, outcomes may include losing one's job, criminal penalties, and even irremediable damage to the organization (Terra, 2022).

Cybersecurity awareness education benefits in supporting workers to be attentive in identifying when an email, website, or pop-up is questionable. Security awareness education delivers a basic understanding to every person and the impending and persistent cyber threats/attacks, training business workers for typical cyber-attacks and threats will help identify those risks (Dash & Farheen Ansari, 2022).

Best methods to take in a Workplace

The best methods to integrate into cyber security training are the following:

1. Keep away from the unfamiliar messages- this appears like an easy request, but workers are easy to trust because the unknown request comes from the internal employee's network. Unknown sites or pop-ups are usually masked as authentic sources, known as phishing. Users are tricked into acquiring entrance to rob and cause harm to sensitive data.

2. Having a strong password will prevent any attacks/threats from happing. Using robust passwords is the way to go since it will be harder for others to guess- it is typical for users to want to use their child's birthday, anniversary, or school passwords; those passwords are easy to remember. Sadly, those sentimental passwords are easy to access.
3. IT division is there for those who need help in the It section, and they help fix technology problems that can occur. one method to take into count is not to install or update any programs without being instructed to do so. It is wise to convey security warnings from the internet security software.
4. Using a secure Wi-Fi to connect for work, whether at the Company or at home, using fast and preventive action must be implemented to protect information. VPNs are very vital when working internally or externally for a company. Public Wi-Fi networks are hazardous and vulnerable to stealing sensitive information (Johansen, 2019).

Why are security breaches still happening with organizations going to significant heights to execute cybersecurity awareness education to defend their acquisitions? Shred-It reported information protection that recognizes understanding, ideas, and methods of information security among small business owners and c-suite executives; it showed that the bulk of information breaches are an immediate effect of human error (Ayereby, 2018).

Why we need Cyber Awareness

Affirmation revealed that human mistakes are responsible for ninety-five percent of adequate cybersecurity attacks/threats. Most cyberattacks cause by end-user mistakes (Li, et al., 2019). Hackers have constantly found ways to acquire entrance to companies' systems by sending phishing emails to all their employees. These attacks are conveyed through ransomware and man-in-the-middle approaches to gain a company's system. End users who are appropriately trained will be more aware of the hacker's method to acquire an edge over the Company's systems and find forms to mitigate these attacks/threats. They are vital in decoding human learning into practical ways to aid an organization by decreasing cyber-attacks risks (Blackwood-Brown, Levy, & D'Arcy, 2021).

Emphasizing education, training, and cybersecurity awareness are essential to lowering cyberattacks/threats. For instance, if an employee is trained not to click on websites or malicious emails, the organization will see a decrease in phishing attacks. However, preparing and educating employees will show the vital strategies and exercises to control these cyber-attacks from acquiring admission to the Company's systems.

Periodically a company may encounter various threats pivoting on the core of a data breach. For example, the hacker will send numerous phishing attacks to an employee if they open phishing emails without knowing. Employees who have chosen weak passwords risk endangering their sensitive information and the confidentiality of an organization's information (Li, et al., 2019). Companies employ technology to decrease threats and must secure their workers and utilize it precisely and without any errors that can threaten a security defense. Training employees about the risks and learning how to prevent them and what should be done if precise circumstances occur and training about Cybersecurity is the best choice anyone can make. Furthermore, constant training awareness meetings for workers should be recommended to secure everlasting retention of lectures learned.

Companies' reliance on training and bringing cybersecurity awareness programs to address cyber-attacks is vital to react to cyber-attacks.

How companies grasp how cyber-attacks/threats happen spans through a corporation's technological assets (Blackwood-Brown, Levy, & D'Arcy, 2021). Cybersecurity training programs are adequate for addressing cybersecurity attacks. They require conveying data to the public, so the public is aware of the countermeasures to use in the circumstances of a cyberattack (Zwilling, et al., 2022). Specialists think that workers and end users who have appropriate cybersecurity education are feasible to know the fundamental security practices used to mitigate cybersecurity threats.

Workers, for instance, ought to be trained in creating robust passwords, recognizing malicious emails from legitimate emails, and constantly updating their software to handle and contain the event of a cyber-attack. Cybersecurity awareness and training programs are very successful and should be developed to fit any firm's basic guidelines, procedures, and requirements (Blackwood-Brown, Levy, & D'Arcy, 2021). Adequately preparing and educating employees will have an excellent place to make the right choice in a convenient determination to defend themselves from hackers/attackers from any inquisitiveness.

In Contrasting

Worth mentioning that cyber-attacks be addressed by forcing employees to train and bring awareness to their employees. For example, a few workers who make a mistake that results in an attack may be reprimanded for their actions. In situations like this, employees are improbable to inform errors, and their cyber security awareness in cyberattacks will not be unavoidable by the attacker. The cyber-attack has caused a threat to the Company by not informing about the mistake that has occurred (Blackwood-Brown, Levy, & D'Arcy, 2021). regardless of the cautious steps to make the employees aware of the risks of cybercrime, it is critical to grasp their error and use it to teach others of the risks that can occur and to teach something other employees have not seen before. Before initiating an agenda to increase awareness among workers, the Company should constantly secure that it will be persuasive and define how the result will be measured (Zwilling, et al., 2022). Various companies must develop a program to deliver an ideal training awareness agenda for employees, which will significantly benefit companies to be liable to cyberattacks/threats.

Employee Contradiction

In spite of the debate, training workers may not affect controlling the cyberattacks, exposing them to heighten training projects that can embrace their prospects of handling the cyberattack/threats concerns—additionally, participating workers while creating a training program that can benefit and support measures to mitigate cyberattacks. On top of that, companies will constantly perform in a secure environment. They must always focus on embracing new methods to reduce cyberattack vulnerability.

Training and Malware in a Workplace

Malicious software is explained as a part of software created to induce damage to data, devices, and people. Companies are worried more than ever and constantly seeking new ways to secure their information. Reverse, social engineering, and phishing, to name a few, are threats that every Company should also educate and train regarding security awareness. Social engineering is the skill of controlling people to give up their personal or Company information through human interactions. Many attackers use their skills through social manipulation. That is how they can acquire sensitive information, keep in mind that they do not use technical skills.

Technology has tremendously progressed quickly it is easy to detect technical vulnerabilities. Companies keep their IT department secure because of threats they can encounter at any moment, but companies need to prepare for employees that can pose a security threat. Social Engineering is still a problem for many businesses because of human manipulation. Social engineering threats have increased significantly because of the lack of employee awareness (Lohani, Social Engineering: Hacking into Humans, 2019). These attacks happen by gathering delicate information from cell phone numbers, emails, text messages, and even direct approaches. Companies should focus on IT divisions to prevent cyber-attacks and cannot stress enough the importance of educating their employees to notice/detect social engineering threats.

Identify Cyber-attacks in Social Engineering

Risk managers are essential in teaching employees in a corporation security awareness and how to identify cyber-attacks and social engineering threats that would lessen the effects of ever being attacked. Help employees not fall for these types of threats, gain knowledge, and teach background information on an attack that can occur without awareness. Also, let employees know how hackers are good at manipulating people and give examples of manipulations they have done in the past. Social engineering threats can also contain Phishing attacks. Phishing attacks are used to manipulate someone in power/authorized user in gaining their credentials by gaining their trust.

Phishing is a cybercrime in which these hackers use targets by sending emails, telephone, or text messages by someone pretending to be someone they are not. Although there are different ways cyber-attacks can occur, employees should know how they can happen. Like, for instance, to lure people into giving out sensitive information like social security, bank cards, credit cards, and passwords, all for malicious intent. The benefits of training employees to know when there is a suspicious attack will help them identify the process to act.

Security Training Awareness

Training and awareness of how social engineering threats are executed, where a hacker/attacker can fake being an IT employee and bring quick action to users to change their passwords and manipulate the system. Security training awareness includes activities that will help employees take quick action at the right time on different occasions and help identify, inform, and help flag down a suspicious person. Furthermore, learn how to question their motives and use corporate policies and techniques containing the correct action and conduct to intensify security. Companies can demonstrate awareness of social engineering by displaying different strategies, tabletops exercises, and implementing videos in many other ways to teach employees how to discover these threats.

Hackers use websites and emails and send them to employees from an organization they are interested in stealing information from. When employees/users click on the malicious email and then on the malicious website, the hacker can access their sensitive information, like social media accounts, credit cards, and social security information. Once the hacker has gained stolen information, they use it for identity theft. The hacker can use a pretexting attack. Pretexting is a social engineering method to manipulate the victims into disclosing information by building a pretend situation to have the target disclose some sensitive information. The hacker can also use a modified script of phishing called baiting in which the victim is tricked into downloading malicious software, such as web links like music downloads (Lohani, 2019).

How does Reverse Social engineering work?

Reverse Social Engineering is when an attacker does not commence communication with the victim. Instead, the victim is deceived into contacting the attacker/hacker. The attacker/hacker will steal sensitive information from the victim without knowing it (Krombholz, Hobel, Huber, & Weippl, 2014). Another way the hacker can trick the victim is by telling them they can help the victim solve the problem. For instance, the hacker might impair the person's equipment and introduce themselves as skilled personnel who can fix machines. The hackers intend to gain the victim's trust and obtain sensitive information from the victim. A reverse social engineering attack is performed with tremendous creativity to persuade the victim to contact the hacker for help. The hacker's creativity plan shows that he is part of a legitimate company to acquire trust. With the amount of trust given to the hacker, they can quickly gain access to more information than they would have in social engineering attacks.

In conclusion

One of the main reasons cyber-attacks occur is because these attacks are thriving in the workplace. Because of this, there is an enormous need to educate workers on everyday threats to help them operate against cyberattack threats. In essence, without security awareness for employees, hackers find individuals more effortless to exploit than to find a network or a software vulnerability. People do not delete personal information like passwords. Social engineers will request help with data or offer help; spam filters need to be set higher and maintained, and they regularly update anti-virus software, firewalls, and email filters. Furthermore, always be conscious of the risks that can occur in case of a breach. Companies should take immediate action and execute techniques to prevent these attacks and ensure business progression. Systematizing specific policies and counteractions can extend and avert these kinds of threats. Companies have appropriate policies restricting employees from using external hard disks brought from homes to access the company computer systems.

Organizations should pinpoint IT analysts for technical help in preventing employees from replying to anonymous postings or answering anonymous emails. Employee training and education can be meaningful in controlling these kinds of threats. Embracing a comprehensive awareness training program can be instrumental in reducing the threats associated with cyberattacks. Workers should consistently be motivated to convey malicious activities to ensure cyberattacks are reduced before they damage an institution. The everlasting conquest of training awareness strategies demands an ongoing approach that forms with installation and persists with frequent updates about the possible dangers of cyberattacks.

Works Cited

Ayereby, M. P.-M. (2018, January 19). Walden Dissertations and Doctural Studies . *Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems*, 40-57. Retrieved from Human error remains the main cause of data breaches: https://www.grcworldforums.com/breaches-and-vulnerabilities/human-error-remains-the-main-cause-of-data-breaches/386.article

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: a motivation perspective. *Journal of Computer Information Systems*, 195-206.

Dash, B., & Farheen Ansari, M. (2022). An Effective Cybersecurity Awareness Training Model. *First Defense of an Organizational Security Strategy*, 1-3.

IntelliPaat. (2022, March 22). Retrieved from What is The CIA Triad? - Definition and Examples: https://intellipaat.com/blog/the-cia-triad/

Johansen, A. G. (2019, April 9). *Norton*. Retrieved from 10 cybersecurity best practices that every employee should know: https://us.norton.com/blog/how-to/cyber-security-best-practices-for-employees

Johnson, A. L. (2016). Cybersecurity for Financial Institutions. *The integral role of information sharing in cyberattack mitigation*, 277.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Applications*, 2-3.

Li, H. W., Xu, Ash, I., Anwar, M., Yuan, X., & Li, L. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management 45*, 13-24.

Lohani, S. (2019). Social Engineering: Hacking into Humans. *International Journal of Advanced Studies of Scientific Research*, 4 (1).

Marr, B. (2020, January 10). *The 5 Biggest Cybersecurity Trends In 2020 Everyone Should Know About*. Retrieved from Forbes : https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/?sh=277a96417ecc

Terra, J. (2022, September 16). *Simplilearn*. Retrieved from The Importance of Security Awareness Training : https://www.simplilearn.com/importance-of-security-awareness-training-article

Tu, Z., & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management. *A Literature Review Completed Research Paper*.

Wright, C. (2008). Assessing security awareness and knowledge of Policy. *The IT Regulatory and Standards Compliance Handbook*, 161-194.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Nejat Basim, H. (2022). Cyber security awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems*, 82-97.