THE ROLE OF CYBERSECURITY IN INFORMATION TECHNOLOGY EDUCATION

Shejin.T.R

Lecturer in Computer Engineering,
Sree Rama Govt. Polytechnic College, Thriprayar, Thrissur, Kerala.

ABSTRACT

The main goal of cyber security is protecting electronic data and computer systems. As cybercrime increases day by day it is necessary to safeguard individuals, companies, and their data and hence cyber security professionals are more and more necessary.Cyber security has been featured in news more often in recent years. Around 30,000 skilled cyber security professionals are there in the US Public Sector alone, despite the fact that this is one of the highest paying technologyrelated fields. Academic institutions are increasingly facing a key responsibility to nurture students who are proficient in the ideas and technology of cyber security, in order to protect against everevolving cyberthreats. The greatest techniques and tactics for fending off cyber attacks are taught in cyber security education. This entails becoming knowledgeable about current cyber threats, how to spot them, and how to put in place reliable security measures. This article explores the function of cyber security in the context of IT education and argues for the inclusion of this subject in IT curricula. The connection between advanced cybersecurity topics and information assurance and security, a currently acknowledged IT discipline, is discussed.

***Keywords: -** IT; cybersecurity; Information Assurance; cyberthreats; Security.*

INTRODUCTION

Data technology or cybersecurity which comes under Information technology's security domain deals with safeguarding computer systems and preventing unwanted access, use, or modification of electronic data. It addresses the security of networks, hardware, software, and data within them. Modern industries rely heavily on computers to store and communicate vast amounts of sensitive personal data.So cybersecurity is a vital service that many organizations require insurance for. Computer systems are also shielded from harm and theft by it. Because it guards against theft and destruction to all types of data, cybersecurity is crucial. Sensitive information, personally identifiable information (PII), protected health information (PHI), personal information, data related to intellectual property, and information systems used by the government and business sectors are all included in this. A company becomes an easy target for cybercriminals because it lacks the ability to protect itself against data breach operations without a cyber security program[1].

Both innate gamble and leftover gamble are expanding, driven by the worldwide availability and utilization of cloud administrations, similar to Amazon Web Administrations, to store delicate information and individual data. The far and wide unfortunate design of cloud administrations matched with progressively refined digital hoodlums implies that the gamble that an association experiences a fruitful digital assault or information break is on the ascent. Business pioneers can never again exclusively depend on out-of-the-container network safety arrangements like antivirus programming and firewalls.Cybercriminals are getting more brilliant, and their strategies are turning out to be stronger to customary digital protections[2]. It means quite a bit to cover every one of the fields of network safety to remain very much safeguarded. Digital dangers can emerge out of any level of an association. Work environments should incorporate network protection mindfulness preparing to teach staff about normal digital dangers like social designing tricks, phishing, ransomware assaults (think Winery), and other malware intended to take licensed innovation or individual information. Online protection alludes to the insurance of organizations, gadgets, and information from unapproved or accidental access or unlawful use[4].Schools need venture class safety efforts and equipment empowered security to assist with safeguarding their understudies, staff, and information from cyberattacks. The verytroublemakers that target undertakings additionally search for weaknesses in nearby school regions. Network protection is significant in any business setting, yet particularly in training. Cyberattacks not just trade off the wellbeing and security of educators and school organizations, yet additionally the protection of understudies especially minors in school level foundations. Today a huge number of understudies are learning through innovation in mixture, remote, or in-class conditions. Online protection is vital on the grounds that it defends a wide range of information against burglary and misfortune. Delicate information, safeguarded wellbeing data (PHI), by and by recognizable data (PII), protected innovation, individual data, information, and government and business data frameworks are undeniably included[4]. Numerous sites would be basically difficult to appreciate if network protection experts didn't work perpetually to forestall forswearing ofadministration assaults.

Digital protection is the act of safeguarding PCs, servers, cell phones, electronic frameworks, organizations, and information from pernicious assaults. It's otherwise called data innovation security or electronic data security. The term applies in different settings, from business to versatile processing, and can be partitioned into a couple of normal classifications[6].

- ❖ Network security is the act of getting a PC network from gatecrashers, whether designated assailants or deft malware.
- ❖ Application security centers around keeping programming and gadgets liberated from dangers. A compromised application could give admittance to the information its intended to safeguard. Fruitful security starts in the plan stage, certainly before a program or gadget is conveyed[5].
- ❖ Data security safeguards the trustworthiness and protection of information, both away and on the way.

- ❖ Functional security incorporates the cycles and choices for dealing with and safeguarding information resources. The consents clients have, while getting to an organization and the methodology that decide how and where information might be put away or shared, the entire fall under this umbrella[1].
- ❖ Fiasco recuperation and business congruity characterize how an association answers a digital protection occurrence or whatever other occasion that causes the deficiency of tasks or information. Debacle recuperation approaches direct the way that the association reestablishes its activities and data to get back to a similar working limit as before the occasion. Business congruity is the arrangement the association returns to while attempting to work without specific assets[7].
- ❖ End-client schooling addresses the most flighty network protection factor: individuals. Anybody can incidentally acquaint an infection with a generally solid framework by neglecting to follow great security rehearses. Helping clients to erase dubious email connections, not plug in unidentified USB drives, and different other significant illustrations is imperative for the security of any association.

THE SCALE OF THE CYBER THREAT

The worldwide digital danger keeps on developing at a quick speed, with a rising number of information penetrates every year. A report by Hazard Based Security uncovered that a stunning 7.9 billion records have been uncovered by information breaks in the initial nine months of 2019 alone. This figure is over two times (112%) the quantity of records uncovered in a similar period in 2018.Clinical benefits, retailers and public elements encountered the most breaks, with malevolent crooks liable for most episodes. A portion of these areas are more interesting to cybercriminals in light of the fact that they gather monetary and clinical information, yet all organizations that utilization organizations can be focused on for client information, corporate surveillance, or client assaults.[4-5]

With the size of the digital danger set to keep on rising, worldwide spending on network safety arrangements is normally expanding. Gartner predicts network protection spending will reach $188.3 billion out of 2023 and outperform $260 billion internationally by 2026. States across the globe have answered the rising digital danger with direction to assist associations with executing powerful network protection rehearses.

In the U.S., the Public Organization of Guidelines and Innovation (NIST) has made a network safety system. To battle the expansion of pernicious code and help in early recognition, the structure suggests persistent, ongoing checking of every single electronic asset.

The significance of framework observing is reverberated in the "10 moves toward digital protection", direction given by the U.K. government's Public Network protection Center. In Australia, The Australian Network protection Center (ACSC) routinely distributes direction on how associations can counter the most recent digital protection dangers[6-7].

IMPORTANCE OF CYBER SECURITY EDUCATION AND AWARENESS IN INFORMATION TECHNOLOGY

As the world continues to fill in innovation, programmers are tracking down a better approach to acquiring or getting to delicate data. Part of harm should be possible utilizing a single gadget like a telephone or PC. Clients these days should know about how a programmer attempts to acquire individual data that can be utilized against them to get to their records or the delicate individual data of the organization. Perhaps the most well-known way a programmer attempts to take information or delicate data is through social design assaults. Programmers generally use phishing assaults as one of the social design assaults. In this assault, programmers will send an email or message to acquire the client's consideration, which can produce interest in the client, which they use to accumulate information. They likewise put out fliers where the clients can see them and call them at the number given on the flier to gather information. When a client calls them, the programmer will attempt to trap them into giving out their username, secret key, or financial balance. They will likewise, at some point, go through the dumpster to find any reports that might have delicate or individual data. This is called 'dumpster jumping'[9].

A portion of the further developed methods the programmer utilized is that they at some point will send an email to the client, which will seem to be a typical email and will have a connection. This email will continuously attempt to tap on the connection on the email or will attempt to tap on the connection that diverts the client to the web architecture to acquire data. This connection contains worms or infections that are intended to take one’s information. On the off chance that the client in an association has training about these techniques, organizations and clients can constantly alleviate the impacts of programmers, and clients can begin to be more careful.

Cyber Security

Digital protection has been the subject of conversation in association, IT industry, trainings divisions and so on. As we as a whole know the recurrence of cyberattacks are rising, legislatures, associations are making preventive moves to decrease the gamble of effective cyberattacks [5]. One of the occasions occurred in 2009 including a SCADA framework and the STUXNET infection and furthermore occasions including enormous organizations like Sony, Hurray were found to fall in the snare of cyberattack yet even after such high media inclusion there are still shortcomings in different organizations[5].

Digital protection is one of those difficulties that requires worldwide coordinated effort as network safety ranges past lines. It is obvious that network protection is area of interest. Assuming there is any uncertainty in the significance of digital protection schooling association, one ought to see ongoing reports. Given the significance of information being put away these days on the web, the delicate data to be spilled or hacked is getting simpler [2].

Phishing Attacks

While going after or hacking an individual, programmers generally use con procedures. They will constantly attempt to send messages that seem to be in the locales that the client generally utilizes. They will have connections. Assuming the email has connected, the connection will divert the client to various sites, which appear to be the ones the client has been utilizing, and the site will request the individual data. With that data, the programmer will get into people's PCs, bank data, or any kind of delicate data. Except if the client focuses on the email address of the source, they could succumb to such con strategies. Organizations now a days convey counterfeit emails to workers to check whether a representative succumbs to such emails. In the event that they do, the data innovation office will let the worker know what the representative fouled up and what they can do to relieve their mix-ups. This test helped the worker become more mindful and begin viewing phishing assaults in a serious way. This execution is known as SERUM [5].

Well known ways programmers will attempt to con or acquire delicate data are:

- **Lottery.** In this situation, an individual for the most part receives an email saying that he/she has scored a sweepstakes and to move the cash into their ledger they need the singular bank subtleties. This is one of the ways of acquiring bank data from a person.
- **Against Infection.** In this hacking method, an individual receives an email saying that the singular PC has been contaminated and to eliminate the infection, introduce the antivirus. The email will have connection or connection which will a malware and if the singular snaps on the connection his/her PC will be contaminated with the malware.

On the off chance that worker or the singular will have preparing or schooling about these assaults, they can moderate these assaults[4].

IMPACT OF SMART PHONES

Cell phones, in the ongoing past, have turned into a fundamental piece of our everyday lives. Everybody utilizes cell phones for web-based entertainment, perusing, calling, messaging, and so on. It is so imbued in our lives that no one needs to leave their loft or home without their cell phones. There has been a remarkable development in innovation in cell phones in the last 10 years. Individuals use cell phones to make online installments or do internet shopping. Cell phones additionally have the capacity to pay without utilizing any money or cards. Cell phones utilize the

Wallet application to pay[6].Each telephone has been saved with MasterCard or check card data. From this, we can agree that cell phones have a parcel of individual data saved in their memory. Imagine an individual's cell phone gets taken or he drops his telephone, and in the event that the individual has not opened his telephone, then, at that point, the cheat will have all the individual data. Imagine a scenario where the programmer utilizes the individual cell phone to get into their association's organization with the assistance of a VPN. Currently, the programmer will approach all the organization's delicate data accessible on this individual's one drive.Some of the time, an individual has his Bluetooth or Wi-Fi turned constantly. Envision that in the event that the individual is associated with a public organization, and assuming the individual is associated with a public organization, programmers can lay out a snare for the person by setting up joins, which will seem to be a genuine site and will attempt to provoke the client to finish up private data. As indicated by ongoing concentrate, practically 51% keep their Wi-Fi turned constantly[6].The association ought to make their representatives aware of the weaknesses of cell phones and how the worker can moderate this by following security methodologies like saving a confounded secret word for their cell phones or how to utilize the Web on the off chance that the representative is associated with the public organization. Network safety schooling will make them more prepared and careful[10].

END-USER PROTECTION

End-client protection, or endpoint security, is a pivotal part of digital protection. All things considered, it is often an individual (the end-client) who coincidentally transfers malware or one more type of digital danger to their work area, PC, or cell phone. Things being what they are, how do network safety measures safeguard end clients and frameworks?.Digital protection depends on cryptographic conventions to encode messages, documents, and other basic information. This safeguards data along the way, yet additionally prepares for misfortune or burglary. Also, end-client security programming examines PCs for bits of malignant code, isolates this code, and then eliminates it from the machine[6]. Security projects might distinguish and eliminate malevolent code concealed in essential boot records and are intended to scramble or clear information off of a PC's hard drive. Electronic security conventions likewise center around ongoing malware discovery. Many utilize heuristics and conduct examinations to screen the way a program behaves and its code to shield against infections or Trojans that change their shape with every execution (polymorphic and transformative malware). Security projects can keep possibly malignant projects in a virtual air pocket separate from a client's organization to dissect their way of behaving and figure out how to all the more likely distinguish new contaminations. Security programs keep on advancing new safeguards as network safety experts distinguish new dangers and better approaches to battle them. To take full advantage of end-client security programming, workers should be instructed about how to utilize it. Critically, keeping it running and refreshing it often guarantees that it can safeguard clients against the most recent digital dangers[4].

THE IMPACT OF CYBER SECURITY AWARENESS TRAINING: A CASE STUDY

A college flaunting 40,000 understudies and almost 7,000 staff members cooperated with Fortra's Trinova Security to construct a network safety mindfulness program. In such a huge local area, the chances of information breaks are outstanding, and one single episode can have sensational repercussions. The program zeroed in on phishing reenactments and itemized bits of preparation to impart a network safety-conscious culture across the association. Sending off these projects can be difficult since clients are anxious about phishing tests and the expected repercussions. While network safety is frequently viewed as overwhelming or drawn-out, preventing numerous from connecting with it, this college accomplished a 42% support rate by conceiving fun and drawing in preparation with shifted content sorts. The program was so fruitful with the school personnel that it is presently being carried out for the whole understudy populace. The phishing tests were painstakingly executed, and clear correspondences were shipped off to the staff to control their tension with respect to this action. Eventually, the tests were profoundly effective and considered a remunerating, smaller-than-usual game to place their new information into play[11].

CYBER SECURITY IN EDUCATION: FINAL TAKEAWAYS

The computerized change of instructive establishments is just beginning, and schools will depend significantly more on innovation before very long. Quite possibly of the most expense effective and powerful measure onecan carry out to remain safeguarded is network protection mindfulness preparing. These courses put digital dangers into setting and adjust a clients' way of behaving to make them go about as the most memorable line of guard[12].

CONCLUSION

Areas discussed include penetration testing, a data recovery plan, budget considerations, cyber insurance, the employment of cyber security experts, information security policies, data encryption, the backing up of data, two factor authentication, the integrity of passwords, and database considerations. Even if the organizations are spending millions of dollars on firewalls or updates on the employee computer, but employees remain the weakest link in the structure. If an employee doesn’t follow or is not aware of cyber security attacks, he will most likely fall prey to the hackers which in turn might affect the organizations. If multinational companies were more proactive in educating their employees they might have avoid the security breach in their organization and which could have saved them millions of dollars. All organization should give importance to security awareness.

REFERENCES

1. Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education. 2011.
2. Lehto, Martti. "Cyber security competencies: cyber security education and research in Finnish universities." ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS. Vol. 2015. 2015.
3. Beyer, Richard E., and B. Brummel. "Implementing effective cyber security training for end users of computer networks." Society for Human Resource Management and Society for Industrial and Organizational Psychology (2015).
4. Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015, September). Cyber education: a multi-level, multi-discipline approach. In Proceedings of the 16th annual conference on information technology education (pp. 43-47).
5. Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), 3-7.
6. Le Compte, Alexis, David Elizondo, and Tim Watson. "A renewed approach to serious games for cyber security." 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. IEEE, 2015.
7. Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2015, November). An investigation on cyber security threats and security models. In 2015 IEEE 2nd international conference on cyber security and cloud computing (pp. 307-311).
8. Abubakar, A. I., Chiroma, H., Muaz, S. A., & Ila, L. B. (2015). A review of the advances in cyber security benchmark datasets for evaluating data-driven based intrusion detection systems. Procedia Computer Science, 62, 221-227.
9. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G., & Skourlas, C. (2014). Human factor and information security in higher education. Journal of Systems and Information Technology, 16(3), 210-221.
10. Bandara, I., F. Ioras, and K. Maher. "Cyber security concerns in e-learning education." ICERI2014 Proceedings. IATED, 2014.
11. Abawajy, Jemal. "User preference of cyber security awareness delivery methods." Behaviour & Information Technology 33.3 (2014): 237-248.

12. Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014, September). Using cognitive task analysis to investigate the contribution of informal education to developing cyber security expertise. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 310-314). Sage CA: Los Angeles, CA: Sage Publications.