International Journal of Management, IT & Engineering
Vol. 13 Issue 11, November 2023
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

STAFF EDUCATION FOR CYBERSECURITY

Dr. Vineet Kumar, Assistant Professor,
Dept. of Cybersecurity, Noida Institute of Engg and Technology, Greater Noida

ABSTRACT

Cyber crimes and criminals are increasing day by day due to the advancement in technology and the dependency of people more and more on technology. Therefore, companies or institutes with no cybersecurity training or education are always at risk. The best cyber protection devices or software will not be useful until the people in institutes and companies have proper knowledge of cyber security and usage of these software or devices. Thus, every organization needs to strengthen its cyber Security through its staff and proper cyber tools. In this research paper, we will discuss why we are requiredto update our staff knowledge and what various organizations can do about it.

Keywords: Cybercrime, Cyber Security, Software, Cyber tools, Internet

Address for correspondence
Dr.Vineet Kumar
Noida Institue of Engg and Techn. (NIET)
19,Knowledge Park II Greater Noida
Uttar Pradesh 201306
Vineet.kumar@niet.co.in

1. INTRODUCTION

The computerization of every industry whether education, airlines, food and beverages, software, railways, Commerce, etc. has led to the dependency of all staff members of these industries on computers and the Internet. The threats from cybercriminals are becoming more sophisticated, and businesses without cybersecurity awareness training are at risk. It is therefore imperative that employees within organizations start taking the initiative to strengthen their cyber defense. There are reasons why every company should invest in cybersecurity awareness training for employees.

As more employees work from home, attacks are on the rise.
The coronavirus pandemic caused dramatic changes in many organizations, forcing them to work remotely.As a result, cybercriminals are utilizing this change in the work environment to attack unsuspecting devices.With the prevalence of remote working, vulnerable services such as virtual private networks (VPNs), unpatched Windows machines, and an absence of security at home are being used more often, increasing the danger to people and businesses.To prevent falling victim to potential cyber threats during these crucial times, employees must implement the right security measures.

Standards for information security need to be upgraded.
Every organization strives to implement security controls and procedures. These policies are clarified through cybersecurity training programmes, which also demonstrate to staff how multiple protocols and frameworks interact and function as a unit.Training

programmes ensure that employees are aware of the difficulties posed by security concerns and are equipped to handle any issues that may arise.

Employees can track security problems as they emerge from the ground up and address them before they worsen and escalate.Most cybercrime events start tiny and don't develop into full-fledged data breaches until it's too late. Thus, by educating users and improving information security standards, cybersecurity training programmes assist in preventing such incidents.

To lower the levels of stress and anxiety at work.

If there is a cybercrime everyone is worried and tense about it. After a case, there is a lack of trust and a negative atmosphere at work. Employees are unaware of what went wrong or whether somebody from their place of employment was involved in the incident due to a lack of cyber awareness.

By giving workers trust in technology and cybersecurity protocols, a strong employee cybersecurity training programme can reduce workplace stress. Employees are less likely to make mistakes when they understand how to engage with sensitive data and communicate online with security professionals and other employees.

To address problems related to human error.

Firewalls cannot prevent an employee from falling for a phishing email, according to the IBM Cyber Security Intelligence Index, which estimates that 95% of cybersecurity incidents are due to human error. Even if your company spends millions on cutting-edge security software, it won't matter if your staff is not properly trained in how to recognize and respond to cyberattacks.

In the unlikely event that your employees are unprepared for a cyberattack, the unpleasant fact is that your business is also unprepared. As a result, a training programme can help increase people's awareness and knowledge of potential hazards, ranging from phishing to physical security.

Organizational compliance requirements are increasingly focused on employee training.

Employee training is a requirement of compliance standards. This is because they are aware of the importance of providing training to all employees within an organization, not just the IT department.They want to make sure everyone is fully up to date on the rules and understands what's expected of them. In the alternative, a company risked a fine and eventual reputational harm. Consequently, with excellent security awareness training, your company can be prepared for a cyber breach.

Financial losses of the organization are reduced

The importance of employee training is very low compared to other areas of the security of an organization. It is possible to categorize cyber vulnerabilities into two categories[12]: technical vulnerabilities, such as gaps, weaknesses, or faults, and nontechnical vulnerabilities, such as unsuitable rules, processes, standards, or guidelines.Different technical solutions are available to safeguard the specified systems. The best protection would be attained if only well-tested programs from reputable developers were installed, and if these applications were updated and patched. It is virtually always viable to assess vendors and test apps before deployment as a strategy to improve control over any cyber environment. It is also conceivable to give the developers some of the responsibility for identifying threats. Methodologies for the non-technical portion vary and may involve, for instance, beginning the day by scanning social media and various forums for patterns and hints to new dangers from outsiders [2]; this is a form of context-based threat assessment.However, in this case, the system may not necessarily be safe against insiders like company personnel. Insiders may choose to take advantage of security gaps or even unintentionally let outsiders access. According to research, introducing an information security awareness programme is a useful strategy for managing insider threats.A programme of this kind may be a successful strategy to lessen insider threats if it is well-planned and executed [4]. Given this situation, it seems necessary to create training for all relevant stakeholders. Information security training is important, according to numerous research [4][1][10][13].According to a recent global information security survey [11], the biggest hazard comes from irresponsible or uninformed staff. All staff should receive training, which is crucial, but the training must be carefully organized in terms of when, how, and what to cover. It's also crucial to consider how people learn. Edgar Dale's "cone of experience" was developed because of research showing that people learn and retain information best when they "do the real things" firsthand, or at the very least when they simulate doing so [5].Serious games might offer a setting where students can replicate behaviors more interestingly. Studies have demonstrated that serious games can serve as useful teaching tools [9]. Considering this, training should be created so that the students participate actively, much like they would in simulations and serious games. In keeping with this strategy, the following portion of our paper lists the four primary goals of this study.The third section of the study examines the theoretical basis necessary for situation and threat evaluation while considering the first key purpose. The paper's final portion offers an outlook on the next research that will concentrate on gamifying cyber security training. Gamification [14] in this context refers to the use of game mechanics and ideas to engage users, address issues, etc.

2. GOALS OF THE PRESENT WORK

There are five key goals for this study: (1) determining the theoretical framework to be used for situation and threat assessment; (2) determining approaches and contrasting automated tools for situation and threat assessment; (3) offering suggestions for new security training methods using simulations and serious games; (4) creating the new training; and (5) evaluating the outcomes of the training prototype strategy.

3. ACHIEVEMENTS SO FAR

Security in the cyber realm is said to need the application of techniques and automated systems for situation and threat assessment [3]. The information fusion theory was identified as a theoretical framework to be employed as an underpinning foundation for cyber security training, which is the main accomplishment of this research to date.

Data is sometimes referred to as information. Information can also be thought of as the interpretational meaning that is given to facts. The definitions of data fusion and information fusion are constantly changing because of the quick advancement of technology [15][7]. There will be some common definitions offered.

Data fusion in this text refers to a "process to organize, combine and interpret data and information from various sensors and sources (e.g., databases, reports) that may contain many objects and events, conflicting reports, cluttered backgrounds, degrees of error, deception, and ambiguities about events and behaviors" [16]. While information fusion is defined as "the synergistic integration of information from different sources about the behavior of a particular system, to support decisions and actions relating to the system" [6], the former is the opposite.

According to this viewpoint, information fusion entails acquiring information, combining it, and interpreting the outcome. The information must be combined to be manipulated and treated afterward.

It is obvious that to deliver high-quality cyber-security training, students must be able to analyze data and information from a variety of sources, including contextual data as previously mentioned.We anticipate that the theoretical and practical discipline of information fusion will serve as the foundation for a fresh and successful method of cyber-security training. [8] contains a more thorough examination of the numerous difficulties in using information fusion technologies to solve security issues.

4. FUTURE WORK

Future work will concentrate on the gamification [14] of cyber security training, taking the protection of communication and information systems into consideration. Within this perspective, the use of methods and automated tools for situation and threat assessment will be taken into consideration while having information fusion theory as a theoretical framework.We'll look at cyber security training requirements and talk about gamification. The utilization of game mechanics will be taken into consideration, with a focus on methods for motivating players to engage in desired security behaviors. It has been demonstrated [9] that using games and gameplay elements can make teaching more interesting and motivate students. There will be a needs analysis of the training requirements. Additionally, a potential architecture for a cyber security gamified training system that satisfies these objectives will be shown. Future work will address the previously mentioned objectives 2, 3, 4, and 5 in this way.

5. REFERENCES

[1] https://www.forbes.com/sites/forbestechcouncil/2019/08/16/seven-tips-for-a-successful-security-awareness-training-program/

[2] LARSSON, D. (2013). Varförbehöverpolisenenasglobaltochinom Europa om bevishanteringochvilken roll harstandardiseringen? (Why do the police need to globally agree on evidence collection and what roll does the standardization have?). Rättsäkerhet. May 21, 2013. Stockholm, Sweden.

[3] SYMANTEC. (2013). Internet Security Threat Report 2013, Volume 18. Retrieved August 22, 2013 from

[4] Baltimore Cyber Range and Cyberbit Open New Cybersecurity Training and Simulation Center. (2017, August 3).

[5] Casey, Eoghan. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* , 3rd Edition. Academic Press.

[6] Kizza, Joseph Migga. (2013). Computer Crime Investigations and Ethics. In: *Ethical and Social Issues in the Information Age,* fifth edition. Springer; Chapter 15

[7] Reed, D., Yung-Hsu Liu, A., Kleinman, R., Mastri, A., Reed, D., Sattar, S., Zeigler, J. (2012, July 25). An Effectiveness Assessment and Cost-Benefit Analysis of Registered Apprenticeship in 10 States.

[8] WALTERS, R. (2013). Bringing IT out of the shadows. Network Security. 2013, 5-11.

[9] https://www.livingsecurity.com/products/cybersecurity-training-content

[10] Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making. (2013).

[11] https://cybersecurityventures.com/security-awareness-training-dont-blame-your-employees/

[12] An Examination of the Cybersecurity Labor Market. (n.d.). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf

[13] 2009 Cyberspace Policy Review. (2015, August 10).

[14] KAPP, K. M. (2012). The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education. Pfeiffer. ISBN 1118096347

[15] Reed, D., Yung-Hsu Liu, A., Kleinman, R., Mastri, A., Reed, D., Sattar, S., Zeigler, J. (2012, July 25). An Effectiveness Assessment and Cost-Benefit Analysis of Registered Apprenticeship in 10 States.

[16] https://www.forbes.com/sites/forbestechcouncil/2019/08/16/seven-tips-for-a-successful-security-awareness-training-program/