Sustaining Cyber Security Protection through SETA Implementation

Subjects: Information Science & Library Science

Contributor: Guangxu Wang , Daniel Tse , Yuanshuo Cui , Hantao Jiang

It is undeniable that most business organizations rely on the Internet to conduct their highly competitive businesses nowadays. Cyber security is one of the important elements for companies to guarantee the normal operation of their business activities. Security education, training, and awareness (SETA) training cover many aspects, which can comprehensively improve staff's ability of cyber security.

cyber security SETA sustainability supervised learning awareness related factors

1. Introduction

Cyber security protection has become a constantly high-profile topic for businesses since e-commerce became an essential part worldwide. It is also the foundation of strategy making and investment making for a company [1]. Besides, computer viruses and hacker technology are multiplying as the importance of data increases, which directly impacts a company's core competencies and reputation. Within this background, some media exaggerate the seriousness of reports related to cyber security problems, and consumers also react negatively to data breaches [2]. More senior managers in various industries are concerned about maintaining cyber security to ensure the regular operation of the business and to not just regard cyber security as an IT problem. In fact, there is no panacea in cyber security protection, the best way reserachers can do is to mitigate the impact caused through proper security management in order to sustain such protection in the business operations.

Although it is known for most companies to protect cyber security, many do not take enough measures to prevent cyber security threats [3]. Even under the urging of government and policy, the proportion of companies conducting staff training is not high. Some companies may mistakenly believe that staff with IT skills can prevent cyber security threats, so there is no need to conduct training on cyber security for staff. Although cyber security protection and IT skills have certain relations, there is still a huge difference between them. All the staff lacking the understanding and awareness of cyber security is likely to lead to internal vulnerabilities and losses. Actually, cyber security's social engineering is one of the biggest threats, and staff awareness plays the most important role in controlling this threat [4]. To prevent this kind of attack, one of the best methods is to conduct education and training for the workforce of companies and further boost their related knowledge and awareness [4].

Security education, training, and awareness (SETA) training cover many aspects, which can comprehensively improve staff's ability of cyber security. It involves common sense, culture, and awareness training, as well as staff training to normally operate organizations' websites, systems, accounts, email, and social media. Besides, through

SETA implementation, staff can learn how to prevent and deal with cyber security vulnerabilities and threats and consciously protect the organization's data and confidential information [5].

Some research studies have proven that SETA programs are the most effective way to improve employee information security protection behavior [6][7]. In contrast, there are also some studies showing that without the intervention of other factors, SETA programs alone do not have a significant effect on the improvement of employee safety behaviors [8][9] and that the failure of employees to take timely protective measures is not mainly due to the lack of safety training and safety awareness [10]. Research pointed out that SETA could play the most significant role in safety behavior through monitoring, followed by employee relations, and then accountability [11]. Thus, while some studies have shown that SETA implementation alone has no substantial impact on corporate cyber security protection, SETA implementation can influence employee behavior in other ways, such as monitoring, and further indirectly protecting the company's cyber security. It has a positive effect on the protection of corporate cyber security.

Due to the above current situation of people's attitude towards cyber security, researchers found the need to dig out the factors affecting the companies' focus on cyber security and explain how such factors affect the companies' decision on effective SETA implementation. Within the factors, the governments are efficient in taking additional measures to carry out the corresponding publicity related to the importance of SETA implementation, boosting the information security sustainability of businesses.

2. Current Status

2.1. Difficulties in SETA Implementation

SETA implementation is a common and necessary measure to maintain information security. Due to its low cost, most training courses are designed to improve employees' security awareness and reduce human errors. Aoyama et al. summarized that most teams have experienced similar management challenges, and the management challenges observed in incident handling training are possible challenges in real-world cyber incident management [12]. The demand for SETA implementation in industries is increasing, and some authoritative organizations are providing training in cyber incident handling. Traditional network security training mainly raises employees' awareness of vigilance to respond to network security attacks. These training items mainly include on-site training and awareness training through screen savers, posters, program reminders, and online courses [13]. Ghafir et al. pointed out that the shortage of corporate training budgets has adversely affected employees' awareness training [14]. The company managers generally tend to minimize their budgets. This also provides opportunities for hackers who carry out cyber-attacks. If network security implementation is not sufficient, physical access threats, including information leakage and theft of items, may cause significant economic losses for companies and individuals. Furthermore, researchers also learned that due to the difference of employees in educational backgrounds and cultural levels, etc., giving on-site training and awareness training to all employees from top to bottom is also a huge problem faced by companies in SETA implementation [15][16].

2.2. Human Behavior toward SETA Implementation

Some scholars take human behavior into consideration and describe the changes in human behavior before and after conducting SETA Implementation. McCrohan, et al. claimed that when users have accepted proper cyber security training, they change to enhance security and tend to be more sensible to cyber security issues [17]. Puhakainen and Siponen found that some employees are not in compliance with security training, which causes security problems, so leaders need to motivate employees to cogitative processing the information they trained before [18]. Furman, et al. conducted an interview with users and finds that users are aware of cyber security, but they do not have enough skills to prevent cyber-attacks, so it is very important for users to accept training and obtain relevant skills [19]. In these articles, through investigating human behavior related to cyber security, the scholars find ways to enhance people's ability and training effectiveness when facing a cyber security attack.

2.3. Innovative Design of SETA Implementation System

Some scholars focus on the innovative design of SETA implementation systems to boost the efficiency of existing training systems. Two general directions are to design new types of SETA implementation systems or take some measures to boost the efficiency of current training systems. Cone et al. concluded that though cyber security training approaches are very universal, most of them are lacking security concepts, there is a new training tool called CyberCIEGE that can successfully and efficiently raise users' security awareness [20]. Abbott et al. found that better structuring of the education and training of cyber security is very significant, so using the technology mining the resulting data logs for relevant human performance variables can improve the quality of the cyber security process [21]. Hatzivasilis et al. used pedagogical practices and a cyber-security model to design a dynamic training program that can provide contentious adaption to users' performance [22]. In fact, SETA implementation is becoming more and more important due to the rapidly developed cyber threat. In conclusion, these articles summarize that the current SETA implementation system is not suitable for schools and companies' needs, there should be a new training system that is more effective than the current one.

Overall, the existing studies on SETA implementation are mainly focused on the difficulties of companies to hold this kind of training, the effects of training on employees, and how to build a more efficient training system for companies.

References

1. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future Internet 2019, 11, 73.
2. Labrecque, L.I.; Markos, E.; Swani, K.; Peña, P. When data security goes wrong: Examining the impact of stress, social contract violation, and data type on consumer coping responses following a data breach. J. Bus. Res. 2021, 135, 559–571.

3. Klahr, R.; Amili, S.; Shah, J.N.; Button, M.; Wang, V. Cyber Security Breaches Survey 2016; Department for Digital, Culture, Media & Sport: London, UK, 2016.
4. Aldawood, H.A.; Skinner, G. A critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. In Proceedings of the 2018 26th International Conference on Systems Engineering (ICSEng), Sydney, Australia, 18–20 December 2018; pp. 1–6.
5. Al-Ghamdi, M.I. Effects of knowledge of cyber security on prevention of attacks. Mater. Today Proc. 2021.
6. Mani, D.; Raymond Choo, K.; Mubarak, S. Information security in the South Australian real estate industry. Inf. Manag. Comput. Secur. 2014, 22, 24–41.
7. Kennedy, S.E. The pathway to security–mitigating user negligence. Inf. Comput. Secur. 2016, 24, 255–264.
8. Zhang, L.; McDowell, W.C. Am I really at risk? Determinants of online users' intentions to use strong passwords. J. Internet Commer. 2009, 8, 180–197.
9. Chin, A.G.; Etudo, U.; Harris, M.A. On Mobile Device Security Practices and Training Efficacy: An Empirical Study. Inform. Educ. 2016, 15, 235.
10. Slusky, L.; Partow-Navid, P. Students Information Security Practices and Awareness. J. Inf. Priv. Secur. 2012, 8, 3–26.
11. Winfred, Y.; Daniel, O.W.; Peace, K. SETA and Security Behavior: Mediating Role of Employee Relations, Monitoring, and Accountability. J. Glob. Inf. Manag. 2019, 27, 102–121.
12. Aoyama, T.; Naruoka, H.; Koshijima, I.; Watanabe, K. How Management Goes Wrong? The Human Factor Lessons Learned from a Cyber Incident Handling Exercise. Procedia Manuf. 2015, 3, 1082–1087.
13. Olusegun, O.J.; Ithnin, N.B. People are the answer to security: Establishing a Sustainable Information Security Awareness Training (ISAT) program in organization. arXiv 2013, arXiv:1309.0188.
14. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149.
15. Gardner, B.; Thomas, V. Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats; Elsevier: Amsterdam, The Netherlands, 2014.
16. Kumar, A.; Chaudhary, M.; Kumar, N. Social engineering threats and awareness: A survey. Eur. J. Adv. Eng. Technol. 2015, 2, 15–19.

17. McCrohan, K.F.; Engel, K.; Harvey, J.W. Influence of Awareness and Training on Cyber Security. J. Internet Commer. 2010, 9, 23–41.
18. Puhakainen, P.; Siponen, M. Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. Mis. Quart. 2010, 34, 757–778.
19. Furman, S.; Theofanos, M.F.; Choong, Y.; Stanton, B. Basing cybersecurity training on user perceptions. IEEE Secur. Priv. 2011, 10, 40–49.
20. Cone, B.D.; Thompson, M.F.; Irvine, C.E.; Nguyen, T.D. Cyber security training and awareness through game play. In Proceedings of the IFIP International Information Security Conference, Karlstad, Sweden, 22–24 May 2006; pp. 431–436.
21. Abbott, R.G.; McClain, J.; Anderson, B.; Nauer, K.; Silva, A.; Forsythe, C. Log Analysis of Cyber Security Training Exercises. Procedia Manuf. 2015, 3, 5088–5094.
22. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G. Modern aspects of cyber-security training and continuous adaptation of Programmes to trainees. Appl. Sci. 2020, 10, 5702.