

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions

Sadiq Nasir

School of Information Technology and Computing (SITC)

American University of Nigeria

Yola, Adamawa State, Nigeria

E-mails: sadiq.nasir@aun.edu.ng

Phone: +2348061562786

ABSTRACT

Cybersecurity education is essential in equipping individuals with the proper knowledge and skill sets to protect devices, computers, networks and data from cybersecurity risk. This research examines past research in cybersecurity education and training, evaluates the existing literature on Cybersecurity risk to identify research gaps and suggests the future direction of the research phenomenon. The paper evaluates the mechanics that influence the effectiveness of cybersecurity training programs. The paper also presents best practices and success factors for developing cybersecurity training programs. The research presents the benefits of cybersecurity training and awareness program underpinned around addressing human vulnerability to promote a better and positive cybersecurity awareness culture within organisations. It also highlights the need for a company to adhere to legal and regulatory requirements, which is essential in mitigating cybersecurity risk. The findings of this work propose a model for examining the relationship between cybersecurity training and user behaviour; this is made up of the input, process and output components, which are presented with a model to show the connection of the three elements.

Key words: Cybersecurity awareness, Training effectiveness, Human factor, Organisational support, Evaluation methodologies, Security culture, User behaviour

Proceedings Citation Format

Sadiq Nasir (2023): Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 151-160. <https://cybersecurenigeria.org/conference-proceedings/volume-2-2023/>.
[dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P18](https://doi.org/10.22624/AIMS/CSEAN-SMART2023P18)

1.. INTRODUCTION

Cybersecurity breaches and risks have posed significant threats to individuals and organisations (Hussain et al., 2020), and these risks have become prevalent and complex. Over the years, cybersecurity awareness and education have been used to mitigate cybersecurity risk and enhance organisations' cybersecurity posture. (Bada et al., 2019) argues that capacity building can reduce the related risk by 45% to 70%. The fast pace of technological advancement creates unintended consequences in the cybersecurity domain (Nobles, 2019); this challenge is present due to the sophistication of technology, making detecting the threats even more difficult. Traditionally, technology has been used to mitigate cybersecurity risk; however, humans have always been considered the weakest link in any organisation (Yan et al., 2018), making it paramount to address this complex cybersecurity concern. For effective resilience in any organisation, human resources should be placed at the centre of building strength and safeguarding against cybersecurity threats.

In cybersecurity resilience, there are several factors to bear: safety, usability, behaviours and culture (Fairburn et al., 2021). This resilience is better managed through cybersecurity education and training (Rajamäki et al., 2018), aiming to bridge the gap by enhancing personal knowledge and awareness; through this, the individual can better manage threats to prevent and respond to cybersecurity incidents (Angafor et al., 2020). Through the analysis of empirical studies, theoretical frameworks and best practices, the research aims to produce mechanics that contribute to the effectiveness of cybersecurity awareness programs.

The review will delve into various factors that influence the effectiveness of cybersecurity training programs, including delivery methods, content development, participant characteristics, and organisational support. It will examine the evaluation methodologies employed to assess training effectiveness, such as measuring knowledge acquisition, attitude and behaviour changes, and the long-term impact of training interventions. It will also discuss future research in cybersecurity awareness and training educational programs, with a broader view of enhancing cybersecurity mitigation.

1.1 Background

Cybersecurity risks have become so common in today's societies that they may greatly concern individuals and organisations (Al-Ghamdi, 2021). Cybersecurity education and training has become a versatile tool for mitigating threats and has received attention over the years (Zwilling et al., 2022). This research will equip individuals and organisations with the knowledge, behaviour, and skills to protect them and promote the desired behaviour. Technology is ever-changing, offering a complex landscape; cybersecurity is continuously changing (McLaughlin, 2023). The traditional way of cybersecurity mitigation has always relied on technology (Falco, 2018).

Cybersecurity programs discussed in this research paper cover a wide range of activities such as employee training, academic educational programs, and public awareness, which all aim to enhance cybersecurity awareness and best practices. Academic programs are mainly designed towards cybersecurity integrating academic programs to prepare the participants for future roles.

This is to enable them protect vital information on platforms such as computers, other devices and networks. Awareness campaigns are centred around informing a selected group or the general population on a select topic in cybersecurity and putting individuals in a position to take proactive measures to mitigate cybersecurity incidents (P. R. J. Trim & Lee, 2019). Researchers argue that Cybersecurity training and education go beyond knowledge dissemination; a good training program aims to influence the user's behaviour and help develop a good cybersecurity culture (Uchendu et al., 2021). This also includes engaging individuals to take responsibility and maintain adherence to cybersecurity policy.

2. RELATED WORK

This section of the work considered past research in cybersecurity education and training; it will synthesise findings from research, identify gaps and suggest future areas for development. Definition of Cybersecurity Training and Education: Cybersecurity training can be classified into three main types: awareness, education, and skills development. Cybersecurity training can also be delivered through various methods, such as lectures, workshops, simulations, games, e-learning, and blended learning (Creutzburg, 2018). An essential factor to consider here is the content and curriculum of the cybersecurity training.

Cybersecurity training imparts knowledge and skills to individuals to protect computer systems, networks, and data from unauthorised access, cyber threats and attacks (P. R. Trim & Lee, 2021). This training can be in a classroom or multimedia base, which may include a combination of text, images, audio, animation, video, and interactive content (Zhang-Kennedy & Chiasson, 2022). At the same time, Cybersecurity Education is defined as the formal academic programs and curricula that provide in-depth knowledge and understanding of cybersecurity principles, theories, and practices. (Crick et al., 2019) advocates that cybersecurity education should be made compulsory in school curricula; this is an excellent attempt to highlight the importance of cybersecurity.

2.1 Factors Affecting the Effectiveness of Cybersecurity Training Programs:

Cybersecurity Training is an important part of protecting an organisation's data assets; it is important to note that several factors can affect the effectiveness of cybersecurity training; some of these factors are;

An essential factor for a training program in cybersecurity is the content and the way the program has been designed. A good cybersecurity training program needs to be relevant, current and built to target the training needs of the participants (He et al., 2020). In addition, the programs need to have the support of the decision-makers in the organisation (Nasir, 2023). There are several ways to make training conform to these concepts with this, such as implementing simulators, quizzes, games, and feedback to improve learning outcomes. An effective anti-phishing training program should comprise knowledge assessments, refreshers, leadership buy-in, and monitoring (Dawson, 2019). Another critical factor that can influence the effectiveness of cybersecurity training programs is the motivation and attitude of the participants (Yoo et al., 2018).

The participants are expected to have a good and positive attitude towards new skills and behaviours. Several factors, such as organisational culture, incentives, rewards, recognition, and peer pressure, can influence the motivation and attitude of the training participants. Evaluation and measurement of the training outcomes can influence cybersecurity training programs. The matrix used to evaluate a training program must be executed by implementing a reliable matrix; this needs to capture the changes in knowledge, behaviour, perceived risk, and the possibility of cyberattacks.

For an efficient evaluation of training, this should be done at intervals and continuously; this will enable the assessment of the cybersecurity training for impact. A limitation of cybersecurity awareness programs, organisations depend on best practices and industry guidelines that contain no empirical evidence or theoretical foundation to assist with understanding which strategies are effective in which contexts (Alkhazi et al., 2022).

A critical factor in developing good cybersecurity training is the need for a universally accepted body of knowledge or a standard set of competencies for cybersecurity professionals. Cybersecurity risk keeps changing in nature with the advancement in technology. To mitigate this, cybersecurity training programs must be consciously updated and adapted to cybersecurity training content (Zhang et al., 2021). There are discrepancies between theoretical knowledge and the practical skills required to have a solid functional cybersecurity program; there needs to be a balance between conceptual understanding and hands-on experience in cybersecurity training.

Delivery and implementation of cybersecurity training include; the lack of resources, time, and motivation; the diversity and heterogeneity of learners; and the resistance to change and learning. Limitations of finance, human and technical resources can be a barrier in the delivery of training programs; a specific because these are limited resources, especially for small and medium-sized enterprises (SMEs); they are hardly able to prioritise quite budget to address their training needs and sometimes lack expertise, and infrastructure to support cybersecurity training initiatives (Kabanda et al., 2018).

In a busy work environment, the trainer and the trainees can give up a limited amount of time to engage in cybersecurity awareness activities, mainly due to conflicting work demands and the inability to prioritise quality work. There also exists a challenge in factors of motivation and interest of participants regarding the training; the participants tend to perceive that most cybersecurity programs are not too exciting, complex and irrelevant to them. There is also complacency regarding what they already know, which can put them off any cybersecurity knowledge-sharing session. The dynamic nature of the work environment where people come from different backgrounds concerning the area of training and the role they play in organisations has a significant interest in the attitude of the patients towards cybersecurity training.

2.2 Best Practices and Success Factors

Cybersecurity training and awareness are the foundation of an organisational aspect of defending itself from cybersecurity risk. Organisations are continuously experiencing setbacks when it comes to cybersecurity risk due to the factors highlighted above.

This section of the research work aims to provide some of the best practices and success factors in establishing and delivering solid cybersecurity training. The literature review is grouped into four sections: (1) the importance of cybersecurity training and awareness, (2) the types and methods of cybersecurity training and awareness, (3) the best practices for cybersecurity training and awareness, and (4) the success factors for cybersecurity training and awareness.

3. THE IMPORTANCE OF CYBERSECURITY TRAINING AND AWARENESS

Cybersecurity training and awareness are essential for numerous reasons; It can help reduce human factors as a source of vulnerability in cybersecurity. Human factor refers to human beings being the weakest link in the cybersecurity setup for several reasons. First, they can help address existing deficiencies' vulnerability (Sabillon et al., 2021). Human errors, negligence, or malicious actions often cause many cyber incidents, such as phishing, malware infections, data breaches, or insider threats (Bandari, 2023). Educating and informing participants about the best practices to stay safe is a great way to mitigate cybersecurity incidents.

Training and awareness help organisations develop a positive security culture; culture refers to shared values, beliefs, norms, and behaviours supporting cybersecurity goals and objectives (Bada et al., 2019). A positive security culture can enhance employees' awareness, attitude, and behaviour toward cybersecurity and their sense of responsibility and accountability for protecting the organisation's assets and information (Amankwa et al., 2018). A positive security culture can facilitate communication, collaboration, and trust among employees and management regarding cybersecurity issues (Ioannou et al., 2019).

An essential aspect of training is toward legal and regulatory requirements; training enables the staff to be able to comply with the regulations; an example of such is the National Data Protection Regulation (NDPR), which the National Data Protection Bureau administers, a regulation agency in Nigeria that oversees penalty for noncompliance, ranging from fines to penalties depending on the regulation.

3.1 The types and methods of cybersecurity training and awareness

Cybersecurity training and awareness can be broadly grouped into formal and informal. Formal training refers to structured learning activities which aim to develop knowledge, skills, and abilities related to cybersecurity. Formal cybersecurity training can be delivered through various methods, such as online courses, webinars, workshops, simulations, quizzes, or certifications. While the informal form of training refers to unstructured training, such as; news articles, web pages containing cybersecurity advice, and stories about the experiences of friends and family (Rader & Wash, 2015).

4. DISCUSSION

This section of the work discusses the findings from the literature evaluation of the research phenomenon and the promotion of the desired user behaviour, a topic of significant interest and research in recent years. A possible proposed model for "Cybersecurity Training and Education Programs in enhancing user behaviour" is as follows:

The proposed model is made up of three main aspects; these are input, process, and output. The input here means the characteristics of the users who participate in the cybersecurity training program, such as his/her prior knowledge, motivation, attitude, and personality. The second aspect refers to the cybersecurity training program's process, design, and delivery, such as the content, methods, duration, frequency, and feedback. While the fire aspect is the output, this refers to the outcomes of the cybersecurity training program, such as the changes in user behaviour, knowledge, skills, and awareness.

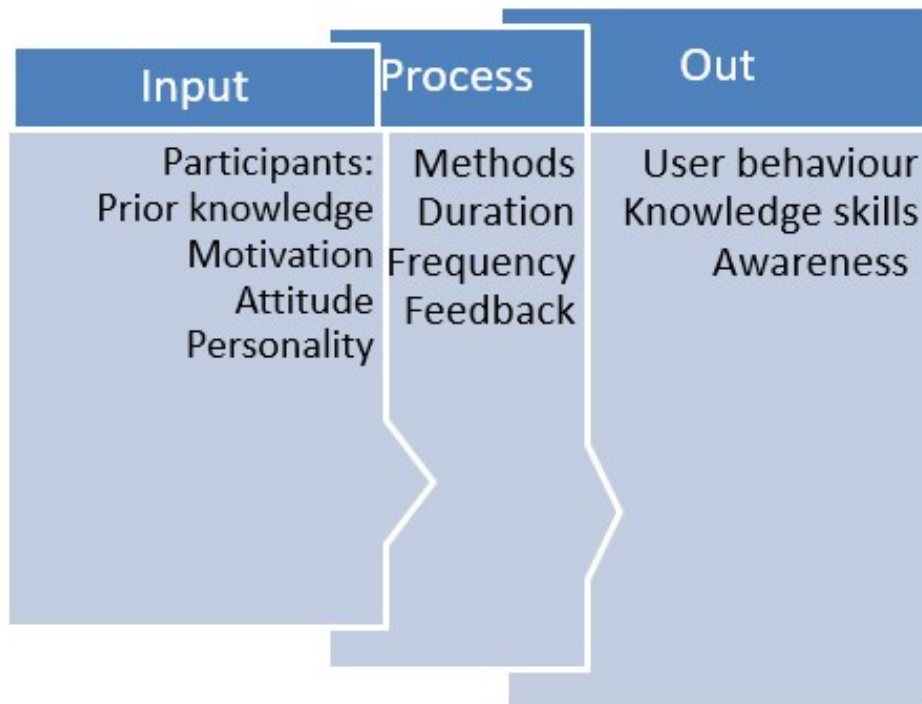


Figure 1.0 Model for Effectiveness of cybersecurity awareness

The above represents the proposed model for the effectiveness of cybersecurity awareness; the proposed model works, assuming that the input significantly influences the process. The model also assumes that the process component influences the model output. This means enhancing the behaviour of users through cybersecurity; it is essential to consider the relationism between the input and the processes to determine the desired output.

Some of the best practices and success factors of cybersecurity training programs include the conduct of needs assessment to identify user gaps and other training requirements, The use of diverse methods and media, such as lectures, videos, games, simulations, case studies, and quizzes, are to consider to make training more effective. Getting feedback from participants is also very important for training evaluation. Reinforcement of the learning outcomes via the follow-up process helps the overall assessment. There is a need to also evaluate training based on mixed methods, which are quantitative and qualitative, to be able to come up with a dynamic understanding of the training programs.

Some factors that influence the effectiveness of cybersecurity training programs include the learners' prior knowledge and experience, the level of inter of the patients also plays a role in this and its relevance to the participants.

Cybersecurity training and education programs positively impact user behaviour, although the effect size may vary based on the program type, method, and duration. Awareness programs effectively enhance user knowledge and awareness of cybersecurity issues but have limited influence on changing user behaviour. Skill-based programs successfully improve user skills and confidence in performing cybersecurity tasks, but they require more extensive time and resources for implementation. Behaviour change programs effectively shape user attitudes and intentions towards cybersecurity behaviour, but it is crucial to reinforce them with feedback and incentives.

5. FUTURE WORK

Future work on this research phenomenon need to should consider proposing a standard framework and guidelines for cybersecurity education guidelines. This framework can propose a strong foundational for designing and delivering security training programs. There is an existing gap between theory and practice in cybersecurity training. Future research can utilise the application of training simulation to make cybersecurity training and research more practical and more in touch with reality.

Organisations need more support in applying for cybersecurity training programs; as a result, there needs to be a stronger desire to develop effective programs that will be relatively inexpensive for small organisations, research in this direction is strongly desired.

Motivation and attitude plays essential in making a cyber study training program elective; future research should explore ways to enhance training activities, such as gamification and a reward system, to ensure participants are well motivated.

6. CONCLUSION

This paper has offered a detailed evaluation of past literature on the research phenomenon while highlighting the key findings, identifying gaps and prompting future areas that need further research. The work presented definitions and boundaries for practical cybersecurity training and education. Organisations can better deliver executive programs with a good understanding of this training program and its scope. This research has been able to propose best practices and success factors for the building and the delivery of cybersecurity training programs.

This mechanism has a significant influence on the effectiveness of the training program, which in turn will help in the enhancement of the overall cybersecurity posture of any organisation where this is taken seriously.

A proposed model that aims to present the relationship between the cybersecurity training prong and user behaviour has been presented, which captures the defining and evaluating intervention programs. Through the relation between user characteristics, program design and delivery, and desired outcomes, organisations can better develop training programs that effectively address the specific needs of their personnel.

REFERENCE

1. Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. *Mater. Today Proc*, 10.
2. Alkhazi, B., Alshaikh, M., Alkhezi, S., & Labbaci, H. (2022). Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior. *IEEE Access*, 10, 132132–132143. <https://doi.org/10.1109/ACCESS.2022.3230286>
3. Amankwa, E., Looock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organisations. *Information & Computer Security*.
4. Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy*, 3(6), e126.
5. Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *ArXiv Preprint ArXiv:1901.02672*.
6. Bandari, V. (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organisation Types. *International Journal of Business Intelligence and Big Data Analytics*, 6(1), 1–11.
7. Creutzburg, R. (2018). Cybersecurity and forensic challenges-a bibliographic review. *Electronic Imaging*, 2018(6), 100-1-100-116.
8. Crick, T., Davenport, J. H., Irons, A., & Prickett, T. (2019). *A UK case study on cybersecurity education and accreditation*. 1–9.
9. Dawson, A. (2019). *Exploring strategies for implementing information security training and employee compliance practices*. Walden University.
10. Fairburn, N., Shelton, A., Ackroyd, F., & Selfe, R. (2021). Beyond Murphy's Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience: An Applied Practice Case Study Discussing Approaches to Assessing Human Factors Vulnerabilities in Cyber-Security Systems. *HCI for Cybersecurity, Privacy and Trust: Third International Conference, HCI-CPT 2021, Held as Part of the 23rd HCI International Conference, HCII 2021, Virtual Event, July 24–29, 2021, Proceedings*, 123–138.
11. Falco, G. (2018). The vacuum of space cyber security. *2018 AIAA SPACE and Astronautics Forum and Exposition*, 5275.

12. He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., & Tian, X. (2020). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, 21(2), 203–213.
13. Hussain, A., Mohamed, A., & Razali, S. (2020). A review on cybersecurity: Challenges & emerging threats. *Proceedings of the 3rd International Conference on Networking, Information Systems & Security*, 1–7.
14. Ioannou, M., Stavrou, E., & Bada, M. (2019). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–4.
15. Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, 28(3), 269–282.
16. McLaughlin, K. L. (2023). DEFENSE IS THE BEST OFFENSE: THE EVOLVING ROLE OF CYBERSECURITY BLUE TEAMS AND THE IMPACT OF SOAR TECHNOLOGIES. *EDPACS*, 1–7.
17. Nasir, S. (2023). Cybersecurity Awareness: Prerequisites for Strategic Decision Makers. In *Cybersecurity for Decision Makers* (pp. 383-393). CRC Press.
18. Nobles, C. (2019). *Establishing Human Factors Programs to Mitigate Blind Spots in Cybersecurity*. 7.
19. Rader, E., & Wash, R. (2015). Identifying patterns in informal sources of security information. *Journal of Cybersecurity*, tyv008. <https://doi.org/10.1093/cybsec/tyv008>
20. Rajamäki, J., Nevmerzhitskaya, J., & Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). *2018 IEEE Global Engineering Education Conference (EDUCON)*, 2042–2046.
21. Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). An effective cybersecurity training model to support an organisational awareness program: The cybersecurity awareness training model (catram). A case study in canada. In *Research Anthology on Artificial Intelligence Applications in Security* (pp. 174–188). IGI Global.
22. Trim, P. R. J., & Lee, Y.-I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, 83, 224–238. <https://doi.org/10.1016/j.indmarman.2019.04.003>
23. Trim, P. R., & Lee, Y.-I. (2021). The Global Cyber Security Model: Counteracting cyber attacks through a resilient partnership arrangement. *Big Data and Cognitive Computing*, 5(3), 32.
24. Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, 102387.
25. Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, 84, 375–382.
26. Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems*, 108, 107–118.

27. Zhang, Z., He, W., Li, W., & Abdous, M. (2021). Cybersecurity awareness training programs: A cost–benefit analysis framework. *Industrial Management & Data Systems*, 121(3), 613–636.
28. Zhang-Kennedy, L., & Chiasson, S. (2022). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, 54(1), 1–39. <https://doi.org/10.1145/3427920>
29. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, 62(1), 82–97. <https://doi.org/10.1080/08874417.2020.1712269>