E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies

https://semantjournals.org/index.php/ AJEES

| Research Article

Check for updates

Importance of Cybersecurity Awareness Training for School Administrators and Teachers for Sustainable School System

Eguonor Temienor

Department of Educational Management and Foundations, Delta State University Abraka, eguonor18@gmail.com

Nnorom Jane Ndidiamaka

Department of Educational Management and Foundations, Delta State University Abraka, srjfrank@yahoo.com

Oweikpodor Vera Gbaeprekumo

Department of Educational Management and Foundations, Delta State University Abraka gbakumovera@gmail.com

Abstract: In recent years, the rise of technology has led to an increase in the use of digital platforms in educational institutions. However, this development also brings with it the threat of cyberattacks and security breaches. Through rigorous training, administrators and teachers in Nigerian schools can become better equipped to tackle these threats and ensure a sustainable school system. This paper explores the benefits of implementing cybersecurity awareness training in Nigerian schools and its potential impact on the overall security and success of the education system. By examining current security measures and potential challenges, this study aims to provide a comprehensive analysis of the importance of cybersecurity training in Nigerian schools and its role in creating a safe and sustainable learning environment for all stakeholders involved.

Keywords: Cybersecurity awareness training, School administrators, School Teachers

1.0 Introduction

Administrators typically work in schools and universities. They are responsible for overseeing administrative tasks in educational institutions by making sure that the organization runs according to the expected rules and regulations. This qualifies them for managing personnel in the school or university like teachers, heads of departments, and other non-academic staff (Skolera undated). Muhammed and Ogunode (2021) opined that one of the basic functions of school administrators is to ensure that teaching and learning take place and to ensure this, the school administrator needs adequate and quality teachers. School administrators are appointed to help in

the realization of the objectives of the schools. The function of the school Principals/School administrators includes administration of teachers, coordination of student programmes, resources allocation and physical resources application, and school community relationship management (Muhammed et al, 2021). Onafowope, Egwunyenga & Oweikpodor, (2023) viewed the functions of the principal as setting instructional directions, result-oriented, team management, organizational coordination ability, effective communication, development of others and developing self.

Teacher are professional trained to impart knowledge and provide guidance to students of all types. A teacher is a person who helps others to acquire knowledge, competences or values. Teacher is a designation for the office, position, and profession for someone who devotes himself in the field of education through patterned educational interaction, formal and systematic. Ogunode, Edinoh, and Olatunde-Aiyedun, (2023) noted that teachers have the ability to shape leaders of the future in the best way for society to build positive and inspired future generations and therefore design society, both on a local and global scale. In reality, teachers have the most important job in the world. Those who have an impact on the children of society have the power to change lives. Oweikpodor, Temienor & Nnorom, (2025); and Olowonefa & Ogunode (2021) observed that teachers are fundamental to the effective delivery of the teaching programme in educational institutions. The teachers' place in educational institutions cannot be replaced. The teacher plans the lesson, organizes the instructional resources and delivers the lesson. The teachers ensure the students learn the right knowledge and skills through the process of teaching and learning. Teachers are found in all educational institutions.

Teachers can act as a support system that is lacking elsewhere in students' lives. They can be a role model and an inspiration to go further and to dream bigger. They hold students accountable for their successes and failures and good teachers won't let their talented students get away with not living up to their full potential. Teachers of all walks of life and subjects have the ability to shape opinions and help form ideas about society, life and personal goals. Teachers can also expand students' limits and push their creativity. In the roles of the teachers in the schools, the teachers are regarded as the implementer of the school curriculum. The job of the teachers includes; implementation of curriculum, planning of lesson notes, lesson plan, organization of instructional resources, assessment of students via continuous assessment and examination, marking of students' scripts and provision of feedback to parents on students' academic performance (Ogunode, Olowonefa, & Ayoko, 2023).

Cyber Security awareness is the knowledge and understanding individuals have about protecting digital systems and data. It involves recognizing cyber threats, understanding associated risks, and adopting safe practices. This awareness aims to defend both individuals and organizations from cyber incidents, typically nurtured through training and ongoing education.

This preparation is crucial in education since school are a treasure trove of personal data about staff, students, and their parents, making them a prime target for data breaches. Most School administrator and teachers are learning about several new technological platforms to perform their administrative and teaching job, from teaching to grading and communicating with parents. It is based on this that this paper seeks to discuss the benefits of Cybersecurity Awareness Training for School Administrators and teachers for School Administrators for Sustainable School System in Nigeria.

1.2 Purpose of the study

The purpose of this is to examine the benefits of Cybersecurity Awareness Training for School Administrators and teachers for School Administrators for Sustainable School System in Nigeria. The specific objectives include;

1. To find out the benefits of Cybersecurity Awareness Training for School Administrators for Sustainable School System
2. To find out the benefits of Cybersecurity Awareness Training for Teachers for Sustainable School System

Literature Review

2.1 Concept of Cyber Security

Cyber security, Nwachukwu (2021), viewed cybersecurity to encompasses a set of policies, security concepts, tools, security safeguards, risk management approaches, guidelines, actions, best practices, training, assurance, and technologies that can be used to protect the cyber environment, organization, and user's assets. Organization and user assets include connected computing devices, personnel, applications, infrastructure, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security attempts to ensure the accomplishment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

Cyber-security is the body of guidelines or templates put in place for the protection of cyberspace. But as individuals, organizations, and even states become more dependent on cyberspace, they undoubtedly face new risks. Cybercrime can also be referred to as a series of organized crimes attacking both cyberspace and cyber security (Ukhami, & Abdulsalam, 2024).

Cybersecurity is an important information security principle that aims to protect computer systems, networks, and data from unauthorized access, data breaches, and other cyber threats. It involves implementing measures, protocols, and technologies to ensure the confidentiality, integrity, and availability of digital information. Cybersecurity is a categorical concept that encompasses various aspects related to protecting computer systems, networks, and information from unauthorized access, theft, damage, or disruption. It involves implementing measures to safeguard digital assets, technologies, and data, as well as mitigating risks associated with cyber threats (Khodzhanovna 2023). Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment - the internet (Steffani, 2006)

Cybersecurity includes various practices and techniques that help organizations and individuals to defend against cyberattacks. This may involve the use of firewalls, antivirus software, encryption, intrusion detection systems, and other security tools. It also includes strategies such as regular security updates, training and awareness programs, network segmentation, and incident response plans. The importance of cybersecurity has grown significantly with the increasing reliance on digital technologies and the rise in cybercrime (Khodzhanovna 2023). Cyber Security can also be described as the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access (Thilla, 2012).

2.2 Concept of Cybersecurity Awareness Training

Cybersecurity awareness training according to Editorial Team (2024) is a resourceful approach that companies often use to help staff members develop their knowledge and awareness of best practices and methods for keeping sensitive data secure. Cybersecurity awareness training can extend beyond the IT department and encourage colleagues across different teams to improve their approaches to accessing and using company data. Some companies may also use training to support policy development regarding cybersecurity practices. Completing a workshop or training program can be a beneficial way to develop the skills necessary to manage digital information.

School stakeholders are at the forefront of any school and are simultaneously one of the biggest targets and threats to a company's cybersecurity. There are numerous different cyber threats that

can impact on a company ranging from technological failure and human error to cybercrimes. Increases in remote working has also brought new and increased risks to businesses, as employers have less control over the security systems surrounding an employees workstation when it is out with an office setting (Mitigo 2024). Security awareness training is a strategic approach IT and security professionals take to educate employees and stakeholders on the importance of Cybersecurity and data privacy. The ultimate objective is to enhance security awareness among employees and reduce the risks associated with cyber threats (Yasar, & Pratt, 2024).

Cyber security training is the type of technological training given to staff in an organization to equip the staff to be able to identify, report, recognize and mitigate cyber risks, cyber threats, imparting the knowledge and skills cyber vigilance and cyber resilience on the staff for the safe keeping of institution assets or information. Cybersecurity awereness training deals with the transferring of skills and knowledge to staff on how to protect their personal data, institutional data and assets against attacks and prevent and militate against data attack that may result to financial loses in the institutions (Ogunode, 2025).

The terms *security awareness* and *security training* are closely intertwined but have noticeable differences according to Yasar, & Pratt, (2024) Security awareness is the process of educating and directing an employee's attention to security-related issues inside an organization. Employees who are aware of security concerns are more inclined to feel accountable for maintaining security, understand its importance, and are aware of the consequences and disciplinary actions for noncompliance. Security training on the other hand, focuses on imparting specialized knowledge and skills to staff members so they can improve their capacity to recognize and effectively address security issues. The main goal of security training is to provide useful advice on security best practices, including how to handle sensitive information appropriately, spot phishing emails and develop secure browsing habits.

There are several common areas security training can cover, according to Editorial Team (2024) including practices like:

Data and record management

One important aspect of cybersecurity awareness training is that it teaches teams how to monitor and manage company data securely. Processes like secure file setup and data transfer are often part of security training, where teams learn and apply best practices for storing and accessing information. Documentation and incident reports are also essential to security training, as reporting is integral to addressing and mitigating risks like viruses and malware.

Installation protocols

Software and application installations are often necessary for many organizations to maintain business information and communicate with staff, shareholders and customers. Cybersecurity awareness teaches teams how to install third-party applications and software programs safely on company computers. Security training can also give direction on the types of programs suitable to install on shared networks and deepen teams' understanding of the risk of installing unlicensed software.

Password safety

Password security is another key concept cybersecurity awareness teaches. Training helps teams learn how to create stronger passwords for different applications, including email accounts, secure data files and social media platforms. Cybersecurity awareness also helps teams understand the importance of updating passwords regularly to maintain secure networks and accounts.

Alert response procedures

Cybersecurity awareness training often teaches response procedures for addressing and managing risks to computer systems. Teams can learn how to identify threats like cyber attacks, data hacks and phishing activities, along with the protocols for assessing the risk level, reporting the incident and fixing the issue. This aspect of training can also cover how to identify different types of security threats so staff can apply mitigation strategies according to the specific alert or security notification.

Internet, email and mobile use

Secure internet use and online interactions are also integral to cybersecurity awareness. Security training often teaches employees best practices and security protocols for communicating through email, managing social media accounts and accessing sensitive business data from mobile devices. Several key concepts teams may learn regarding this area of cybersecurity include identifying and avoiding malicious emails, developing social media and mobile device policies for secure interactions, communication and data use.

Policy standards and implementation

Cybersecurity awareness training also supports the development of standards of practice that companies can use to establish policies for data management and internet use within company networks. Teams can develop their understanding of industry standards and use these cybersecurity criteria to create protocols outlining a risk mitigation strategies, emergency response plans and best practices for protecting sensitive data. Training in cybersecurity can also help support technology teams by encouraging nontechnical staff to follow the policies IT personnel establish.

Phishing Simulation Exercises

Phishing simulations are a more interactive form of cybersecurity training as it allows employers to see that employees have understood their awareness training and are putting the methods learned into practice. Phishing simulations are often conducted internally within a company whereby a fake email is sent to employees containing an attachment, embedded link or a request for personal information. The idea is to test and teacher’s awareness at identifying the key markers that should create suspicion around a dodgy email. It also demonstrates how a teacher will react when they receive such an email (i.e. reporting it to management) as phishing scams are one of the most common cyber threats to a business in modern society.

3.0 Method

This paper takes a stance. Secondary data was used in the paper. Print and internet publications provided the secondary data. The literature used in the paper was chosen using content analysis. International publications including CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib SAGE, Nebraska, and Springer are typically included as references for the literature. This essay takes a stance. Secondary data was used in the paper. Print and internet publications provided the secondary data. The literature used in the paper was chosen using content analysis. International publications including CEON, Elsevier, Hindawi, JSTOR, IEEE, Learn Techlib SAGE, Nebraska, and Springer are typically among the literature's sources (adopted from Ogunode, Akpakwu, & Ochai, 2025).

4.0 Result and Discussion on Benefits of Cyber security training Awareness for School administrators and School Teacher

A) School administrators

In today's digital age, the importance of cybersecurity cannot be underestimated. With the growing threat of cyber attacks and data breaches, it is essential for schools to prioritize

cybersecurity awareness training for their administrators. This training not only helps to protect sensitive data and personal information, but it also teaches administrators the necessary skills to identify and prevent potential cyber threats. By investing in cybersecurity awareness training, schools can not only safeguard their own systems, but also help to create a safer online environment for students and staff. From understanding basic security protocols to identifying phishing attempts, this training equips school administrators with the necessary knowledge and tools to protect their school's digital assets. It is crucial for schools to recognize the value of cybersecurity awareness training and make it a priority in order to ensure the safety and security of their digital infrastructure (Khodzhanovna, 2023).

Cybersecurity Awareness Training for School Administrators

In recent years, cyber attacks have become increasingly prevalent, targeting individuals, businesses, and even schools. As educational institutions become more reliant on technology, the need for cybersecurity awareness and training among school administrators has become imperative. This article outlines the essential components of a comprehensive cybersecurity awareness training program for school administrators.

In order to effectively safeguard sensitive data and protect against cyber threats, school administrators must have a thorough understanding of cybersecurity principles and best practices. This training program is designed to equip school administrators with the knowledge and skills necessary to identify potential risks and take proactive measures to mitigate them (Saxena, 2024).

The benefits of cyber security training for school administrators include:

1. Understanding Cybersecurity: This section will provide an overview of cybersecurity, discussing the types of threats schools may face and the potential impact of a cyber attack.
2. Best Practices for Data Protection: School administrators will learn how to protect sensitive data by implementing strong password policies, using encryption, and regularly backing up data.
3. Identifying and Responding to Suspicious Activity: This section will cover how to identify and respond to potential cyber threats, including phishing scams, malware, and ransomware attacks.
4. Creating a Culture of Cybersecurity: School administrators will learn how to create a culture of cybersecurity within their institutions, promoting best practices among staff and students.
5. Compliance Requirements: This section will outline important compliance requirements, such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Internet Protection Act (CIPA), that schools must adhere to when handling sensitive data.
6. Crisis Management: In the event of a cyber attack, school administrators must be prepared to respond quickly and effectively. This section will cover crisis management strategies to minimize the impact of an attack.

School Teachers

Cybersecurity Awareness Training for Teachers is a critical aspect of ensuring the security of educational institutions and their data. This training provides teachers with the necessary knowledge and skills to identify and respond to potential cyber threats, ultimately protecting the sensitive information of students and staff.

The Cybersecurity Awareness Training for Teachers outlines the necessary steps and information for educators to effectively teach cybersecurity to their students. The training covers a wide range of topics such as recognizing and avoiding cyber threats, data protection, and safe online behavior. It also includes hands-on exercises and simulations to increase practical understanding and

application of cybersecurity concepts. The training is designed to be easily accessible and engaging for teachers of all levels and backgrounds. By the end of the training, teachers will have a solid understanding of cybersecurity principles and be equipped to teach their students how to stay safe in the digital world.

Benefits of Cybersecurity Awareness Training for Teachers:

1. Prevention of Data Breaches: Teachers handle a significant amount of sensitive information, including student records, financial data, and confidential school information. Cybersecurity Awareness Training equips them with the knowledge to identify potential threats and secure their devices and networks, reducing the risk of data breaches.
2. Protection Against Cyber Attacks: Educational institutions are prime targets for cyber attacks due to the valuable information they hold. Cybersecurity Awareness Training helps teachers understand the different types of cyber attacks and how to prevent and respond to them effectively. This ultimately protects the institution from potential financial and reputational damage.
3. Improved Security Culture: By educating teachers on the importance of cybersecurity, they become advocates for security within the institution. They are more likely to follow security protocols and identify potential risks, promoting a culture of security awareness within the school.
4. Cost Savings: In the long run, Cybersecurity Awareness Training can save educational institutions money. The cost of recovering from a cyber attack can be significant, both in terms of financial resources and time. By preventing these attacks, the institution saves money that would have been spent on recovery efforts.
5. Compliance with Regulations: Educational institutions are subject to various regulations, such as the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA). Cybersecurity Awareness Training ensures that teachers are aware of these regulations and understand their responsibilities in safeguarding sensitive information, ensuring compliance.

Conclusion and Recommendations

Cybersecurity awareness training is essential for school administrators and school teachers to protect sensitive data and ensure the safety of their institutions. Cybersecurity Awareness Training for both school administrators and teachers provides numerous benefits, such as preventing data breaches, protecting against cyber attacks, promoting a security culture, cost savings, and compliance with regulations. It is an essential tool in safeguarding the sensitive information of students and staff, making it a necessary investment for all educational institutions. By implementing the key concepts outlined in this program, school administrators and school teachers can enhance their understanding of cybersecurity and take proactive measures to safeguard their schools against cyber attacks. With the rising threat of cyber attacks, investing in cybersecurity awareness training is crucial for the safety and security of in the Nigerian educational institutions.

References

1. Editorial Team (2024). Cyber security training https://www.indeed.com/career-advice/finding-a-job/cyber-security-training

2. Keepnet (2024). Why-is-cybersecurity-awareness-important-in-k-12-and-higher-education https://keepnetlabs.com/blog/why-is-cybersecurity-awareness-important-in-k-12-and-higher-education

3. Khodzhanovna, S, K (2023).cybersecurity is an important information security principle. *Best journal of innovation in science, research and development,02(07), 136-169.*
4. Mitigo (2024)**.** What is cyber security training? https://mitigogroup.com/cyber-security-wiki/what-is-cybersecurity-training/#:~:text=Cybersecurity%20training%20is%20used%20to,)%2C%20networks%20and%20cloud%20services.
5. Muhammed, T. U. (2018). Importance Cybersecurity Awareness Training for Teachers https://www.toolbot.ai/apps/AI%20Abstracteer?desc=A%20tool%20that%20generates%20academic%20abstracts%20from%20user%20input&placeholder=Enter%20a%20topic%20for%20your%20abstract%20
6. Nwachukwu, (2021). "Nigeria: A Failing State Teetering on the Brink." The Punch News. 19 May.
7. Mohammed, H., Ogunode, N. J. & Yahaya D. M. (2021) Challenges facing administrators of public secondary schools in Nigeria and the way forward. *Middle European Scientific Bulletin,* (19), 58-67.
8. Ogunode, N,. J (2025). Cyber Security and Schools in Nigeria: Implication for Administrative Decision. *Best Journal Of Innovation In Science, Research And Development,* 4 (3),146-152.
9. Onafowope, M. A., Egwunyenga, E. J. & Oweikpodor, V. G. (2023) Administrative Strategies to enhance teachers' commitment in Delta State Public and Private Secondary Schools. *European Journal of Alternative Education Studies*. 8: (1) 48- 61.
10. Oweikpodor, V. G., Temienor E. & Nnorom, J. N. (2025) Insecurity on Teachers' Job Performance and Security Management Strategies Available for Principals of Public Secondary Schools in Abuja, Nigeria. *American Journal of Management Practice*. 2:(5) 16-22
11. Saxena, A. (2024). What is Cybersecurity and Why is It Important?. https://sprinto.com/blog/importance-of-cyber-security/
12. Steffani, H. (2006). Do bad boys really get the girls? Delinquency as a cause and consequence of dating behavior among adolescents. *Justice Quarterly* 21 (2), 355–389.
13. Skolera (undated). Role of administrator in school. https://blog.skolera.com/role-of-administrator-in-school/
14. Thilla, D. (2012) The economics of crime and punishment: an analysis of optimal penalty. *Economics Letters* 68 (2), 191–196.
15. Ukhami, E,. I. & Abdulsalam, D. (2024). Globalisation and national security: perspectives on Cybersecurity threats in Nigeria. *Journal of political discourse,* 2, 1,(2),274-286.
16. Raghave foundation (2023). School staff training. https://raghavfoundation.org.in/blog/school-staff-training/
17. Yasar, K & Pratt, M, K (2024). Security awareness training
18. Yemi, R. T. (2021), Benefits of cybersecurity Awareness Training for School Administrators https://www.toolbot.ai/apps/AI%20Abstracteer?desc=A%20tool%20that%20generates%20academic%20abstracts%20from%20user%20input&placeholder=Enter%20a%20topic%20for%20your%20abstract%20