International Journal of Innovative Social & Science Education Research 13(1):42-46, Jan.-Mar., 2025

© SEAHI PUBLICATIONS, 2025 www.seahipublications.org ISSN: 2360-8978

doi:10.5281/zenodo.14780899

Cybersecurity and Occupational Health among Telecommunication Workers

[1]Gbarayege Mercy Barizorge & [2]Prof. Adedamola O Onyeaso

Department Of Health Promotion, Environmental and Safety Education
Faculty of Education
University of Port Harcourt, Port Harcourt, Nigeria
[1]gbarayegemercy@gmail.com/+2348036147903
[2]adedamola.onyeaso@gmail.com/+2348031189318

ABSTRACT

The study X-rayed cyber-security and occupational Health (OH) among tele-communication workers. The intersection of cybersecurity and occupational health is a critical concern for telecommunication workers. The demands of cybersecurity work can lead to physical, mental and social health effects, including muscular skeletal disorders, eye issue, stress, anxiety, depression and social isolations. Therefore, consistent precautionary strategies and safety measures are necessary. Some of the suggested safety measures were: management of telecommunication firms should organize intermittent training programmers for their workers, heads of telecommunication company should implement ergonomic design principles at work, policy-makers and regulators should develop and implement policies and regulations to protect the occupational health and safety of telecommunication workers, telecommunication workers should take proactive steps to promote their occupational health and safety such as prioritizing, selfcare, seeking support from colleagues and supervisors and reporting any health concern to OHS unit of the firm.

Keywords: Cyber security, occupational health, telecommunication workers, threat.

INTRODUCTION

The rapid growth of the telecommunication industry has led to an increased reliance on automated technologies, making cybersecurity a critical concern. Telecommunication workers are at the forefront of this automated transformation and their occupational health is being impacted by the demands of the cybersecurity (Ipalibo 2020). With a 51 percent risk in average weekly cyber attacks in 2021, the communications industry stood out as the third most vulnerable sector to cyber threats, following education and military industries, thus, firm and automated security strategies are needed to nip the situation in the bud.

Telecommunication operators store various data from social security numbers to credit card details. This wealth of sensitive data makes large-scale telecom forms appealing targets for bad actors. Following a successfully data breach hackers often resort to extortion, armed with compromised information, hackers can sell the data on the dark web or exploit their new- found leverage to demand ransom. The threat looms large, organization either pay a substantial sum to present the public disclosures or misuse of sensitive data or face the potential fall-out of reputational damage and legal consequence (Itoms,2022). These risks among others such as supporting interconnected networks and using legacy technology

underscore the growing need for reinforcing robust cybersecurity measures within the telecommunication sector.

In recent times, the battle field has shifted, adversities are no longer just on the other side of the physical borders but can strike from anywhere, at anytime through the vast and interconnected cyberspace. As such, cyber threats are on the rise and the bad actors behind them are becoming increasingly sophisticated, targeting individuals and exploiting weak points with alarming precisions (Ikem, 2023). The damage inflicted by these cyber threats is not confined to a company's finances or operations. The repercussions ripple outward, reaching the individuals at the heart of these organizations, those often fighting the digital war on the front lines are the employees.

Cybersecurity

Cybersecurity are those practices, technologies, and processes designed to protect digital information, computer systems, and networks from unauthorized access, use, disclosure, disruption, modification, or destruction. Types of cyber threats: Software designed to harm or exploit computer systems, social engineering attacks that trick users into revealing sensitive information, Malware that encrypts files and demands payment in exchange for the decryption key, Overwhelming a system with traffic to make it unavailable and intercepting communication between two parties to steal or modify data (Gibson 2021).

Cybersecurity Threats in Telecommunications

i. Network Intrusions_: Unauthorized access to telecommunications networks can compromise sensitive information and disrupt services.
ii. Malware and Ransomware_: Malicious software can compromise telecommunications systems, steal data, and demand ransom.
iii. Phishing and Social Engineering_: Telecommunications employees and customers may be targeted by phishing and social engineering attacks.
iv. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks_: Overwhelming telecommunications networks with traffic can disrupt services and impact customers (Ikiriko 2021).

Cybersecurity Measures for telecommunication workers

i. Network security systems that control incoming and outgoing traffic.
ii. Converting data into an unreadable format to protect it from unauthorized access.
iii. Programs that detect and remove malware.
iv. Using unique, complex passwords to protect accounts.
v. Keeping software and systems up-to-date with the latest security patches (Rael 2021).

Cybersecurity Careers for telecommunication workers

i. Monitor and analyze security systems to identify vulnerabilities.
ii. Simulate cyber attacks to test an organization's defenses.
iii. Oversee an organization's overall cybersecurity strategy.
iv. Respond to and manage cybersecurity incidents.
v. Provide expert advice on cybersecurity best practices and risk management (Briggs 2021).

Cybersecurity Best Practices for Telecommunication workers

i. Tele communicational workers should avoid using easily guessable passwords.
ii. Tele communicational workers should add an extra layer of security to accounts.
iii. Tele communicational workers should regularly update operating systems, browsers, and software.
iv. Tele communicational workers should protect sensitive data with encryption.
v. Tele communicational workers should avoid suspicious emails and links to prevent phishing attacks(Harrold and Mickni 2022).

Cybersecurity Resources for Telecommunication workers

i. A trusted source for cybersecurity guidelines and best practices.
ii. A US government agency providing cybersecurity resources and guidance.

iii. A leading provider of cybersecurity training, research, and resources.
iv. A website providing up-to-date news and information on cybersecurity.
v. A non-profit organization providing resources and guidance on web application security (Ipalibo 2020).

Cybersecurity Certifications for Telecommunication workers

i. An entry-level certification covering security fundamentals.
ii. A certification covering risk management, vulnerability assessment, and incident response.
iii. An advanced certification covering security and risk management.
iv. A certification covering penetration testing and vulnerability assessment.
v. A certification covering information security management (Tyler and Adam 2021).

Cybersecurity Standards and Regulations in Telecommunications

i. A European Union regulation that protects personal data and imposes cybersecurity requirements on telecommunications companies.
ii. A United States regulation that protects sensitive healthcare information and imposes cybersecurity requirements on telecommunications companies.
iii. A standard that protects sensitive payment card information and imposes cybersecurity requirements on telecommunications companies (Briggs 2021).

Emerging Trends in Cybersecurity for Telecommunications

i. Using AI and ML to detect and respond to cybersecurity threats in real-time.
ii. Protecting IoT devices and networks from cybersecurity threats.
iii. Ensuring the security of 5G networks and devices.
iv. Protecting cloud-based telecommunications systems and data from cybersecurity threats (Krutz and Vines 2021).

Telecommunication Workers

Telecommunication workers are individuals employed in the telecommunications industry, which includes companies that provide communication services, such as television, phone, internet, and (Georg-will 2021). Their services are very essential for effective communication to take place.

Types of Telecommunication Workers

i. Telecom Engineers: They design, develop, and maintain telecommunications systems and networks.
ii. Network Administrators: They manage and maintain computer networks, including Local Area Networks (LANs), Wide Area Networks (WANs), and the Internet.
iii. Telecom Technicians: They install, maintain, and repair telecommunications equipment and networks.
iv. Customer Service Representatives: They provide customer support and services for telecommunications companies.
v. Sales Representatives: They sell telecommunications products and services to customers. (Ibunah 2021)

Work Environment of the Telecommunication worker

i. Office Settings: Many telecommunication workers work in office settings, such as call centers or administrative offices.
ii. Field Work: Some telecommunication workers, such as telecom technicians, may work in the field, installing and maintaining telecommunications equipment.
iii. Shift Work: Telecommunication workers may work varying shifts, including night shifts, weekends, and holidays. (Okobulo 2021)

Occupational Hazards of Telecommunication Workers

i. Physical Hazards: Telecommunication workers may be exposed to physical hazards, such as falls, electrical shock, and heavy lifting.

ii. Ergonomic Hazards: Telecommunication workers may be exposed to ergonomic hazards, such as repetitive strain injuries and musculoskeletal disorders.
iii. Psychosocial Hazards: Telecommunication workers may be exposed to psychosocial hazards, such as stress, anxiety, and burnout.
iv. Chemical Hazards: Workers may be exposed to chemicals, such as cleaning solvents or pesticides, when maintaining equipment or facilities.
v. Biological Hazards: Workers may be at risk of biological hazards, such as diseases transmitted through insect bites or contaminated water.
vi. Radiofrequency radiation: workers may be exposed to radiofrequency radiation from cell towers, antennas or other equipment.
vii. Electromagnetic fields: Workers may be exposed to electromagnetic fields from electrical equipment or transmission lines (Dinolo 2020).

Health and Safety Measures for Telecommunication workers

i. Personal Protective Device (PPD): Telecommunication workers should wear PPD, such as hard hats, safety glasses, and gloves, to protect themselves from physical hazards.
ii. Ergonomic Design: Telecommunication workers should work in ergonomically designed workspaces to reduce the risk of ergonomic hazards.
iii. Stress Management: Telecommunication workers should have access to stress management programs and resources to reduce the risk of psychosocial hazards. (Powa 2021).

Education and Training for Telecommunication workers

i. Formal Education: Telecommunication workers typically require a post-secondary education, such as a diploma or degree, in a field related to telecommunications.
ii. On-the-Job Training: Telecommunication workers typically receive on-the-job training to learn specific skills and procedures.
iii. Certification Programs: Telecommunication workers can obtain certification through programs, such as the Certified Telecommunications Professional (CTP) program. (Sulter, 2021).

Career Advancement for Telecommunication workers

i. Promotions: Telecommunication workers can advance to supervisory or management positions.
ii. Specialization: Telecommunication workers can specialize in a particular area, such as network administration or cybersecurity.
iii. Entrepreneurship_: Telecommunication workers can start their own businesses, providing telecommunications services or products. (Kelah and Abdulrahmen 2021).

Occupational health of Telecommunication workers

Occupational health of Telecommunication workers refers to the promotion and maintenance of physical, mental, and social well-being of workers in the telecommunication industry. Some of the importance of occupational health to telecommunication workers include:

i. Prevents Work-Related Injuries and Illnesses: Occupational health programs help identify and mitigate workplace hazards.
ii. Improves Productivity_: Healthy workers are more productive, efficient, and effective.

Challenges faced by Telecommunication workers

i. Limited Resources_: Insufficient funding, equipment, and personnel.
ii. Lack of Awareness_: Limited understanding of occupational health among workers, employers, and healthcare providers.
iii. Cultural and Language Barriers_: Challenges in communicating occupational health information to diverse worker populations (singer and Alen 2021).

CONCLUSION

The intersection of cybersecurity and occupational health is a critical concern for telecommunication workers. The demands of cybersecurity work can lead to physical, mental and social health effects, including musculoskeletal disorders, eyes issue, stress, anxiety, depression and social isolations.

SUGGESTIONS

i. Management of telecommunications firms should organize intermittent training programmers for their workers.
ii. Heads of telecommunications company should implement ergonomic design principles at work.
iii. Policy-makers and regulators should develop and implement policies and regulations to protect the occupational health and safety of telecommunication workers.
iv. Telecommunication workers should take proactive steps to promote their occupational health and safety such as prioritizing, selfcare, seeking support from colleagues and supervisors and reporting any health concern to OHS unit of the firm.

REFERENCES

Briggs, O. (2021). Principal of Computers Security. Ikeja. Guida publishers.
Dinolo, J. (2022). Issue with telecoms. Port Harcourt. TOC printing press.
Eric, C. Seith, M. and Joshua, F. (2021) CISSP study guide. Owerri. Spring publishers Ltd.
Georgewill, N. (2021). Operational guidelines in telecoms. Owerri. Springfield publishers ltd.
Gibson, D. (2021). Principle of computer security. Lagos. Alpha book Publisher.
Harold, F T. and Mickni K, (2022). Information Security Management Handbook. Owerri . Standard publishers.
Ibuniah, Q. (2021). Cyber and tech threats. Lagos. Alpha book publishers.
Ikem, P. (2023). Essential of Cybersecurity. Lagos. Bounty Press Ltd.
Ikiriko, H. (2021). Computer Security: Art and Science. Abeokuta. Pabcode pub listing.
Ipalibo, K. (2020). Cyber Security for dummies. Benin. Evens brothers Nigeria publishers.
Itoms, K. (2022). Cybersecurity Innovation Anka. Fides Media.
Kelah, K. and Abdulrahman, A (2021). Cyber-security: An integrated approach. Ikeja. Parressa publishers Ltd.
Krutz, L. and Vines R D (2021). Cyber-Security A business solution. Benin. Cogent
books Nigeria's.
Matts, B. (2020). Introduction to computer security. Benin. Macadams publishers.
Okobulo, Y. (2021). Hazard in the tele-communication environment. Makurdi.
Aboki publisher.
Pova, L. (2021. Introduction to cyber-crime. Port Harcourt. Ikah printing press.
Real, M. (2021). Cyber-Security for beginners. Lagos. publishers express Ltd.
Singer P W, and Allen F (2021). Cyber-security and cyberwar, what every-one needs to know. Jos. Plateau publishing co-operation.
Sulter, J. (2021). Cyber-security: A very short introduction. Minna. AMAB books and publishing company.
Tyler, M and Adam S, (2021). Cyber-security. Protecting critical infrastructures from cyber-attack. Makurdi. Aboki publishers.