International Journal of Engineering Applied Sciences and Technology, 2024
Vol. 9, Issue 06, ISSN No. 2455-2143, Pages 140-144
Published Online October 2024 in IJEAST (http://www.ijeast.com)

INTEGRATING HUMAN FACTORS IN CYBER SECURITY FOR BETTER RISK MANAGEMENT

Amaefule I. A
Department of Computer Science,
Imo State University, Owerri.

Chilaka U.L
Department of Computer Science,
Kingsley Ozumba Mbadiwe University, Ideato.

Uka Kanayo Kizito, Ibebuogu C.C
Department of Computer Science,
Imo State University, Owerri.

Abstract - **Keeping a safe digital environment is essential, especially as businesses depend more and more on technology. In addition to growing more reliant on technology, society is also become more susceptible to cybercrimes. Since the human element is linked to numerous security events and data breaches, it becomes crucial to maintaining a secure cyberspace. A minor mistake made by an ignorant person could have serious consequences, including possible legal action, financial losses, reputational harm, and a breach of private information. The study intends to investigate a number of human elements, including awareness, behavior, training, and culture. It also provides important information and suggestions for enhancing security by reducing the risk associated with human activity.**

Keywords: **Cyber security, Training, Risk Management, Human Factor, Awareness, Integration,**

I. INTRODUCTION

A cybersecurity plan is not complete if it ignores the human element. A higher proportion of cybersecurity breaches involves human involvement, demonstrating the significance of people and behavior in guaranteeing the effectiveness of a cybersecurity plan. Human deployment and interface are necessary for technology and processes; in the recent past, employee connectivity has increased and the surface area vulnerable to cyberattacks has expanded. The need for employees to be vigilant against cyberattacks has never been greater; in addition to being aware of the risk, they must be empowered and driven to take immediate action to defend themselves.

The world of cybersecurity is dynamic and complicated, with new threats and vulnerabilities emerging practically every day. We have successfully implemented intrusion detection systems, firewalls, zero trust security systems, and advanced artificial intelligence (AI) algorithms to protect our organizations. It is shocking to learn, nevertheless, that human mistake frequently plays a role in security issues as well as sophisticated hacking strategies. Organizations' networks remain vulnerable due to human error, which includes falling for phishing emails, using weak passwords, leaking data accidentally, using obsolete software, not maintaining it properly, and generally lacking in security knowledge and training [1]. Contrary to popular belief, cyber security is not solely a technological problem [2], as most firms realize. Human elements and security culture receive minimal attention and financial support within businesses.

II. LITERATURE REVIEW

Human factors are leveraged by cybercriminals to gain illegal access, steal credentials, and introduce malware into systems; people are more likely to fall for scams when they are afraid, negligent, or lack knowledge in such circumstances.

[3] maintained that addressing cybersecurity solely through technological means is different and that a socio-technical strategy is actually needed to combat cyberattacks. They create a secure and safe digital environment, taking into account human aspects as one of the weakest and most elusive links. Experience, as well as training, age, and gender are examples of human characteristics that significantly affect cybersecurity overall.

[4], examine the idea of human aspects in cybersecurity from the viewpoints of end users. They provided statistical evidence to support the gender gap in cybersecurity expertise, showing that male staff within a business possess a greater understanding of cybersecurity than female employees. Additionally, they asserted that end user

behaviors make a big difference in preventing cyberattacks and that cybersecurity education alone is insufficient. emphasis on creating a well-thought-out and efficient end-user training program in cyber security is a way out to completely eradicate or drastically decrease human error to a manageable level.

In order to investigate the association between risk behavior, employees' attitudes in a work environment, internet addiction, and impulsivity, [5] polled 515 full- and part-time employees. [5] came to the conclusion that dangerous cybersecurity activities are largely influenced by impulsivity and internet addiction.

[6] carried out a survey where students were given different definitions of cyberthreats and asked to score how familiar they were with them. Then, based on their experience, expertise, and amount of internet usage, they were divided into three groups. [6] stated that knowledge of cyberthreats is thought to be a predictor of internet attitudes and security practices.

III. COMMON CYBER THREAT TYPES

Cyber-attacks are when someone gains illegal access to a system or network. These are a few examples of frequent cyberattacks.

1. **Man-in-the-Middle (MITM) Attacks:** These allow cyber criminals to secretly intercepts data that is being sent between computers, networks, or end users.
2. **Ransomware:** This is a malicious software used by perpetrator to locks down and encrypts the victim's personal files, then requests a ransom to unlock them (decrypt).
3. **SQL Injection:** Malicious code is inserted into a SQL-using server by an attacker, forcing the server to divulge information that it would not ordinarily.
4. **Zero-Day Exploit:** Attackers target the revealed vulnerability within this window of time, which happens after a network vulnerability has been uncovered but before an update or solution is put into place.
5. **Denial-of-Service Attack:** The attackers overload the network or system servers with traffic in an attempt to deplete its resources and bandwidth, which prevents the system from responding to valid requests. To carry out these assaults, attackers may potentially leverage a number of compromised devices.
6. **Phishing:** Through the use of phony communications that seem to be from a legitimate source, distinctively emails, the attacker hopes to obtain sensitive details like login identifications, credit card numbers and or send malware to the victim's computer.
7. **Insider Threat:** Consists of an insider rather than a third party. In this instance, it can be an employee of the organization who has enormously knowledge about the organization. They have the capacity to launch several attacks and inflict great harm.
8. **Malware Attacks:** Among the most frequent kinds of online attacks are these ones. It describes viruses that infect software maliciously, such as trojans, worms, spyware, ransomware, and adware. A vulnerability allows malware to enter a network. An email attachment may download or a virus-ridden pen drive may be used when the user clicks on a risky link.

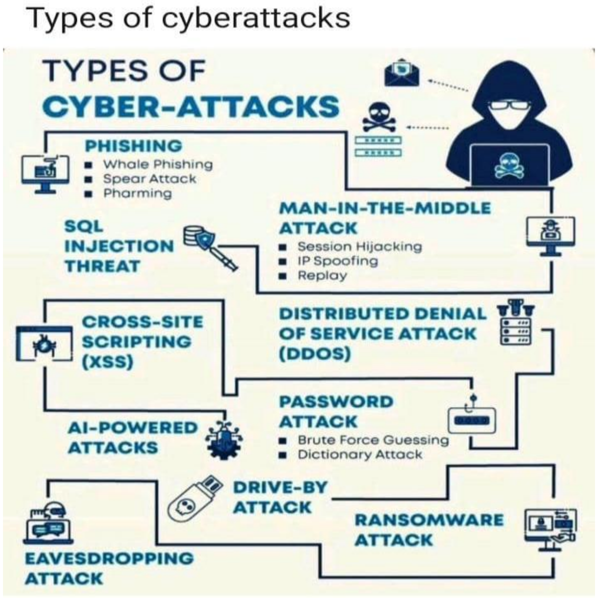

Figure 1: Types of Cyber Attacks.

[7]: Adapted from LinkedIn (Cyber Attacks: Be Cyber Safe)

IV. APPROACHES TO BETTER RISK MANAGEMENT

Building a strong cybersecurity architecture that is better equipped to respond to threats and avert hazards before they materialize requires being able to recognize and quantify the human aspect. Information security managers can identify potential human-driven threats by comprehending the role that human risk plays in the human component of cybersecurity. Here, focus is on Awareness, Training, Culture and Behavior.

1. **Awareness:** The idea behind security awareness is to be highly conscious of work-related habits and their possible effects on the organization [8]. It also emphasizes taking processes more carefully and thinking comprehensively. One of the main reasons for cybersecurity vulnerabilities is frequently distractions. Employees are more likely to open a hacked email or become a target to a scammer if they are handling multiple duties at once. Security awareness may limit risk, improve best practices, and lessen disarray. In order to support their staff and promote a security-aware culture, organization security managers can take proactive steps such as implementing multiple-factor authentication and strong passwords, updating software frequently, encouraging email safety by double-checking the identity of the sender, grammar, spelling, and vocabulary, and refraining from opening file attachments and clicking hyperlinks. Protecting networks, preventing intrusions, detecting and eliminating malware, backing up crucial data on a regular basis, and maintaining a virtual private network (VPN) are all part of maintaining firewalls and antivirus programs.

2. **Behavior:** Establishing a secure digital environment requires a strong understanding of cybersecurity psychology. [9] It can aid in reducing the risks associated with our progressively more digital lives. Human behavior and its impact on technology interactions. Numerous studies have demonstrated that people prefer easy-to-remember passwords to complicated, hard-to-guess ones. This behavioral vulnerability is easily exploited by hackers. One other habit is the propensity to open attachments and click on links without first confirming the source, which can result in infections with malware, phishing scams, and other internet risks. By taking a thorough and all-encompassing strategy and setting up training programs to teach users how to recognize phishing attacks and other online hazards, as well as standard procedures for password management, organizations can stop this weak habit in its tracks. On the other hand, multi-factor authentication and frequent software updates are examples of standards and rules that should be put into place to promote safe conduct.

3. **Training:** To help employees comprehend the risk and threat related to cyber-attacks, frequent awareness training as well as education on a wide range of cybersecurity topics, such as the most recent cyber threat, phishing methods, password management, and safe internet practices, is essential. Businesses may drastically lower the chance of being the target of an assault [10] by giving their staff members the abilities and information to recognize any online dangers. Through methods such as social engineering and phishing emails, hackers often target unaware staff. One of the most significant developments in security awareness training is the ability to identify such strategies and react appropriately, which can help businesses reduce their chances of being adversely affected by online crimes.

4. **Culture:** The resilience and sustainability of cybersecurity depend heavily on the culture of the organization. Not only is risk reduction important, but fostering an atmosphere in which safe behavior is not taken for granted. [11] Employee empowerment, increased awareness, a proactive strategy to cybersecurity, and a reduction in crisis response time are all facilitated by a robust cybersecurity culture. The unwritten guidelines and common ideals serve as a direction for decisions and actions aimed at improving security. Strong password practice, frequent security awareness and training sessions, strict controls on access, threat evaluations, response to incidents strategies, and safety rules should all be part of the company's security procedures. However, CEOs, senior managers, and board members play a crucial part in establishing the standard for cybersecurity in companies, which instills trust in individuals by letting them concentrate on the organization's needs rather than their own security.

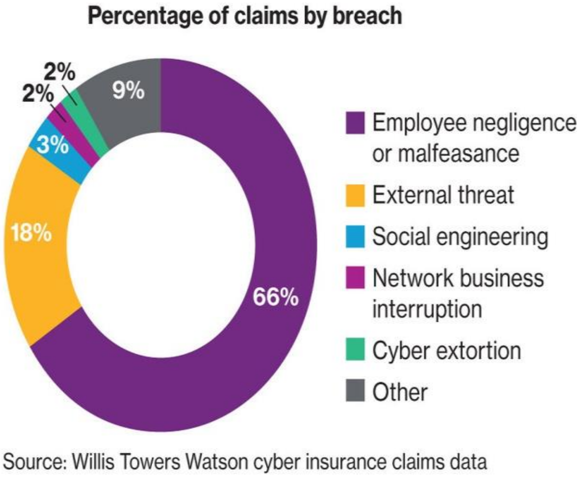

Figure 2: Percentage of Claims by breach [12]

V. SUMMARIZED CYBER SECURITY MEASURES

[13], provided ten (10) essential resources, to reduce threats and fix flaws in an organization. These resources consist of:

1. Keeping a precise inventory of all control system hardware and making sure that none of it is exposed to outside networks.
2. Putting firewalls and network segmentation into practice.
3. Make use of safe remote entry techniques.
4. Putting in place system logs and role-based access control.
5. Consider alternative access control measures, change default passwords, and use only strong passwords.
6. Stay informed about vulnerabilities and apply any required patches and upgrades.
7. Create and implement mobile device policies.
8. Establish a cybersecurity education program for staff members.
9. Involves leaders and upper management in cybersecurity.
10. Establish protocols for identifying breaches and create an incident response strategy for cyber security.

VI. CONCLUSION

It is reasonable to think that working in high-tech, high-risk businesses like finance will increase awareness of security issues, but assumptions should be avoided. Any business's cybersecurity depends heavily on its human resources. The primary line of defense may involve taking the time to comprehend what personnel do, what they require, and how they respond to cybersecurity products. Through cybersecurity awareness programs, people can lower workplace cyber risk and make wise cybersecurity decisions. Training staff is a major step in the right direction; the secret is to integrate technology and education. It appears that human input is necessary for cybersecurity and data protection; otherwise, human mistake will render in-depth defense technology useless. Finally, in minimizing the human element in cybersecurity for better risk management is for organizations to instill a tenable prospect of threat in their staff members through cybersecurity awareness training, access rights and privilege limitations, and regular data backups and good cyber hygiene.

VII. REFERENCES

[1] Mazhar Hamayun (2023). The Human Factor of Cyber Security. Office of the CTO Check Point Software Technology. https://blog.checkpoint.com/security/the-human-factor-of-cyber-security/

[2] Limba, T., et al., (2017). Cyber security management model for critical infrastructure. Entrepreneurship and Sustainability Issues, 2017. 4(4): p. 559-573. DOI: 10.9770/jesi.2017.4.4(12).

[3] Safa, N.S., R.v. Solms, and L. Futcher (2016): Human aspects of information security in organizations. Computer Fraud & Security, (2): p. 15-18. https://doi.org/10.1016/S1361-3723(16)30017-3

[4] Cain, A.A., M.E. Edwards, and J.D. Still (2018): An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications. 42: p. 36-45. https://doi.org/10.1016/j.jisa.2018.08.002

[5] Hadlington, L., (2017): Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 2017. 3(7): p. e00346. DOI: 10.1016/j.heliyon. 2017.e00346

[6] Jeske, D. and P. van Schaik (2017): Familiarity with Internet threats: Beyond awareness. Computers & Security, 66: p. 129-141. https://doi.org/10.1016/j.cose.2017.01.010

[7] Vinay Ratra (2023): Cyber Attacks: Be Cyber Safe. https://www.linkedin.com/pulse/cyber-attacks-safe-2023-vinay-ratra

[8] Jay Reid, Joseph Alterholt, Anthony Cellini (2023). The Human Factor in Cybersecurity; https://www.crowe-com/insight/the-human-factor-in-cybersecurity.

[9] Razz Security Academy (2023) The Human Factor in Cybersecurity: Understanding the Psychology Behind Cyber Threats

[10] The Importance of Cyber Security Awareness Training for Employees. (2024): https://www.elev8me.com/insights/the-importance-of-cyber-security-awareness-training-for-employees

[11] Inc. Africa (2024): Unpack the model's five levels to leverage the power of culture to fortify cyber-

defenses. https://www.incafrica.com/library/inc-masters-the-security-culture-maturity-model-for-cyber-resilience

[12] Willis Towers Watson (2017): cyber insurance claims data https:// assets.weforum.org/ editor/piKG1JyhHEF2u_ cIL5jbm9CuoCCfFSsIiVZm-JBwmiY.jpg

[13] Water ISAC – Security Information Center (2016): 10 Basic Cybersecurity Measures: Best Practices to Reduce Exploitable Weakness and Attacks.