IMPLICATIONS OF PRIOTIZING A MORE HUMANISTIC APPROACH TO INFORMATON SECURITY AND TECHNIQUES TO ADAPT AND ADOPT A MORE HUMANISTIC APPROACH

By

OYEBOLA OYELOWO

Table of Contents

IMPLICATIONS OF PRIOTIZING A MORE HUMANISTIC APPROACH TO INFORMATON SECURITY AND TECHNIQUES TO ADAPT AND ADOPT A MORE HUMANISTIC APPROACH

1.1 Overview

The sociotechnical system is a complex organizational structure that involves the interaction between social and technical components, these components are independent and should be considered together for effective implementation to promoting change within the organization, the sociotechnical framework within an organization embodies six entwined independent elements, expanding the social and technical approach to information security, including people, tasks, structures, technology, physical infrastructure and cultural assumptions (Davis et al., 2014), the human factor, including the user-centered design, awareness and training and feedback evaluations are crucial element in the sociotechnical system that is often neglected due to ineffective leadership, prioritization of goals, lack of end-user involvement and ownership inadequate training which can pose a risk of poor decision making and struggle in establishing a contingency plan.

There has also been a steady rise in data breaches, and leaks, organization have been under cyber-attacks and information security threats such as denial of service, malware injection and social engineering attacks such as phishing, baiting and honey traps. It is therefore crucial to secure our information. To reduce the rate of cyberattacks, Organizations majorly introduced the technical approach to mitigating cybersecurity breaches such as encryption, data security protection, intrusion detection and prevention systems network security protocols and firewalls and paid less attention to another important aspect of a humanistic approach to information security despite the consistent evidence that people are the weakest link in an information security system.

According to (Dawson et al., 2018), the cyber domain comprises three crucial aspects; **the physical layer**, which includes the hardware and infrastructures that support the internet; **the logical layer**, including the network protocols and configurations; and **the social layer**, which consists of the human behavioural aspects of information security, there are more attention on the physical and logical layer of cybersecurity than the social layer which has created an unbalance in the effective protection of the cyber space. (Chen et al., 2013).

Consequently, new attack vectors such as malware, man-in-the-middle attack, phishing and social engineering are created to compromise their security but efforts to mitigate these information security breaches have been centered towards the technical approach to cybersecurity for detecting and preventing unauthorized access and data protection to safeguard security attacks are seen independently from the humanistic thereby find their root cause in human error, the human aspect has often been neglected even though most security attacks are rooted in human errors due to ignorance, mistakes and forgetfulness.

This paper presents the organization’s priority of the implementation of a technical approach to information and the need to adopt a humanistic approach to information. Additionally, the mitigation strategies of using a technical approach to information security from a more humanistic perspective and frameworks that support these measures.

1.2 Understanding Human

Humans are social beings whose behaviour is influenced by the perceptions around them (McAlaney et al., 2020) including their environment, psychology about a new environment and culture. These root causes can influence human behaviour within information security:

Human Psychology; Human psychology about information security is one of the complex and strongest driving forces influencing human behaviour that cannot be evaded. As humans, it is natural mindset to need time to adapt to a new environment and location especially when this new location is not like what they are used to. Similarly, the internet and technology constitute a new environment for humans that has been in evolution for more than a decade. Although the world has gradually adapted to the new era, humans are still taking baby steps to level up. We are living in cyberspace yet we are still excited and thrilled about this new environment without thinking of how to secure it, due to their fast innovative nature, there is more emphasis on campaigns promoting the innovation and functionality of the internet than on its security (Mary, 2019).

Culture; Culture refers to the way of life, the attitudes, values and behaviour that are prevalent within the organization and promote and protect information security practices among the employees. It is defined as the thought process, perception and daily activities and values that informs employees (Schlienger et al., 2002). Employees play a crucial role in fostering and maintaining a strong information security culture and demonstrate their commitment to responsibilities such as examining employee human behaviour and uniqueness, password management, policy and security awareness that focus on human responsibility towards protecting their information and understanding their level of risk appetite and effective communication, the outcome of protecting information security culture (Veiga et al., 2020).

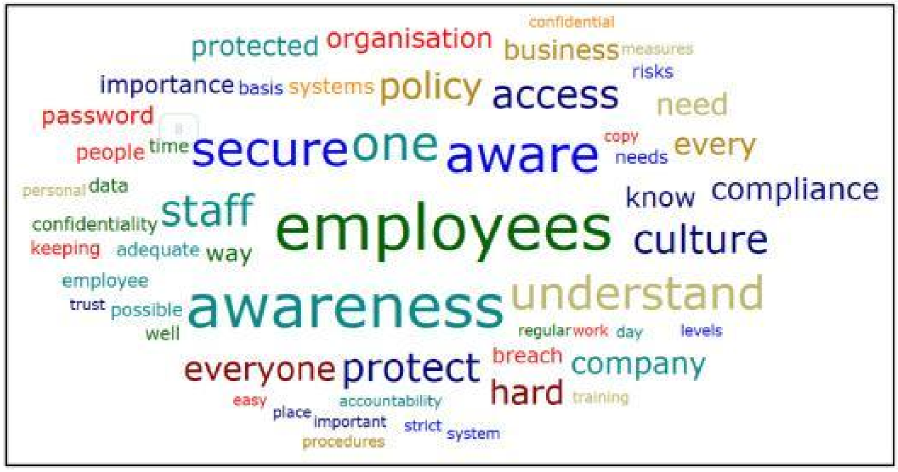

Fig 1: Information security culture (Veiga et al, 2020)

1.3 Human-Related Information Security Threats and Risks

According to Evans et al. (2019), 90.3% of errors related to human incidents are caused by incorrectly performing a task rather than not performing the task at all. Humans are considered the weakest link in the sociotechnical system and are also neglected even though most threats and risks are sourced from human error including (Sasse et al., 2001). This neglect and close mindedness of organizations to human approach and combating ways to address the information security is a big risk to the information security system.

Furthermore, humans are open to the risk of social engineering where attackers exploit human vulnerabilities through social interactions, persuasion and manipulations to get sensitive and gain unauthorized access to the organization's computer system, the goal is to attack the confidentiality, integrity and availability of the system (Wang et al., 2021). Since the 1970s, social engineering has been one of the most recognized attacks that has posed a substantial threat to organizations and is targeted towards human psychology and trust (Momoh et al., 2023). Social engineering is a big threat that targets the mind of individuals, manipulating them to gain unauthorized access to sensitive information by exploiting their trust and can lead to a data breach and compromise of confidential information.

Insider threats can pose a serious risk to an organization despite the huge investment toward protecting the security of the organization, they can either be intentional or unintentional threats that can be influenced by human behaviour and personality (Abdallah, 2023), insider threats can be unintentionally sourced from human negligence and ignorance to security policies and human error such as access to harmful websites, clicking phishing links and divulging confidential information unknowingly and intentionally sourced from malicious intent or personal game to deliberately cause harm to the organization's interests and assets. An insider threat is an intentional or unintentional unethical action that impacts the organization's information assets. Colwill (2009) recorded that 70% of fraudulent activities and 90% of security controls are accounted towards external threats. Insider threat is an abuse of individual's privileges and thieve of intellectual properties that can damage the organization's reputation.

In addition to that, as the information system moves towards a more sophisticated way of communication, phishing and vishing attacks are becoming a prevalent and easy way to manipulate human emotion, phishing is a deceptive strategy used by attackers to lure humans to divulge secret information (Mahfuth, 2019). It is done by sending a false link with intimidating or similar email content and an email address similar to an authorized address to lure employees into divulging sensitive information (Karamagi et al., 2022). Most of the time, attackers use voice calls, emails or instant messaging to send a false and manipulative link to their victims to gain unauthorized assets to secret data and personal information. Social applications such as Facebook, Instagram and LinkedIn are useful tools for developing phishing attacks because they include true information about identities such as academic and professional history displayed in these applications.

Another human-related threat is an unintentional data exposure to sensitive information, this is a situation where employees have access to classified information either intentionally or unintentionally. This can be due to human error, lack of awareness among employees, insider threats and malicious intentions. Individuals may inadvertently expose sensitive information through misconfiguring privacy settings and sending emails to the wrong recipients. This exposure can lead to theft of intellectual property, breach of privacy, confidentiality, financial loss, and integrity of the information and above all, reputational damage.

Moreover, Vulnerabilities like unpatched software and system updates are other human threats and risks that can arise due to human negligence. This is an instance where the software running on a computer or operating system has not been updated with the latest updates released by the software vendor or security patches (Anjum et al., 2023). Unpatched software leaves a weakness in the software thereby giving room for attackers to compromise the system. The neglect to update and patch software and systems leaves vulnerabilities for exploit by malicious actors. This leads to unauthorized access and malware infection.

Lastly, Another analysis from American telecommunication giant Verizon showed that 90% of successful data breaches resulted from exploiting users who used default or weak passwords (Halevi et al., 2016). A weak password is a human-related information security threat that involves employees using easily guessed passwords such as date of birth, name and surname and phone numbers to secure their information system (Strigini et al., 2022). These passwords can easily be brute forced by hackers and access can be granted without authorization and could also put at risk other devices with the same passwords.

1.4 Current Gaps Associated with Human Factor in Cybersecurity and Sociotechnical Systems

Organizations lacks sufficient knowledge and implementation for security culture and its impact on the security behavior within the organization. Human behavior is complex in itself, the budget allocated for information security is little to influence a good information security culture (Rohan et al., 2021), It is crucial to understand how human behavior influences individual's beliefs and decision making and it is an intentional effort for organizations to put techniques in place, thereby creating an effective security culture.

Moreover, the gap in security awareness and knowledge within the organization is another critical observation within the organization. Individuals are not adequately informed about the latest threats, best practices and the importance of information security, this inadequacy has increased human risk and vulnerabilities such as social engineering, Phishing and insider threat and hence, security incidents such as data breaches and lack of confidentiality (Scott et al., 2021).

2.1 Organizational Approaches To Human Information Security Vs Technical Security

The dynamics between an organization's human security and technical information security approaches are essential to effective information security:

2.1.1 Human Information Security Approach:

Organizations provide well-detailed Security Policies and procedures to inform employees and assets of acceptable practice. Security policies are set of rules and laws developed within an organization to characterize and specify acceptable use of assets in an organization, what is permitted and not permitted, These security policies are foundational documents for guiding employees in safeguarding organization data including security information, the approach of security policies is to raise good and acceptable security behaviour and curb bad human behaviour to information security (Alissa et al., 2018). Every organizations adhere to established standards that guides the use of security policies helps in fostering an acceptable standards and use of organizational assets.

Additionally, Awareness and Training is another humanistic approach to information security that organizations imbibe. It involves the use of regular awareness and training sessions that enhance the awareness of security and instils a security discipline among employees within the organization, a larger percentage rate of information security incidents accounted for humans both directly and indirectly, thus, Information Security Awareness in an organization is one of the core aspects of protecting acceptable security behaviour (Khando et al., 2021).

Furthermore, Access Control Permission is implemented to ensure that employees have access to information based on their job roles. It is a mechanism to closely monitor the level of access to resources and information within the organization and ensure that only authorized access is allowed to certain information, this ensures the mitigation of unauthorized access and breaches (Qiu et al., 2020). Tailoring access control permissions to job responsibilities both respect unique roles and only ensures assess to limited information based on assigned roles.

2.1.2 Technical Security Approach

Encryption is one of the techniques securing data for providing an additional layer of security to information against unauthorized access. Encryption is a technique for encoding information to prevent unauthorized access or theft. It converts texts to hidden text by encoding them to provide security. Encryption is done with a key and it is designed to make the decryption almost impossible without the help of the key used in encryption.

Furthermore, Authentication and Authorization is another approach to information security as it provides an extra layer of security to information, it involves the use of three-factor authentication, the use of multifactor authentication and strong authorization to ensure access control and protection against unauthorized access. Authorization is the technique of permitting how much access an individual has towards information while Authentication is a process of protecting the authorized individual, once a user enters his login details, authentication is established and authorization is determined (Chandra et al., 2019).

Endpoint Protection addresses the safeguarding of end devices like computers through deploying antivirus software, endpoint detection and response tools to address the threats at end devices. It also protects against unauthorized access including malware and viruses. Overall, strong security protection is a strategy that necessitates both human and technical approaches to information security including both policies and technology. As endpoint protection and encryption are crucial, policies, awareness and training are equally crucial to information security.

2.2 Implications of Prioritizing Technical Approaches to Information Security

Prioritizing a technical approach against a more humanistic approach to information security may lead to a neglect of human factor in the propagation of information security within the organization including a **knowledge gap** IT Professionals and other individuals within the organization, it focuses on programming languages and algorithms to secure a network leaving behind human error, user education and awareness, effective communication of security practices, policies and procedures (Dawson et al., 2018).

Additionally, Organizations that validate more technical skilled personnel can led to a **lack of security awareness** amidst the employees including social engineering training and discernments, hence, vulnerable to human-related risks and threats (Rahman et al., 2021). The dismissal of security awareness influences human behavior to information security has limited the scope of the organization's research exploration in other aspects including human psychology and effective solution that considers human factors are limited compared to the overall information security. Incorporating a more humanistic approach creates a balance in security of the organization.

Organizations prioritized a technological approach creates a false sense of information security and user resistance. Deploying firewalls and encryption which are mostly automated and regularly used in organizations makes individuals within the organization focus less on anomaly behaviour, when an unpredictable behavioural pattern occurs, technical controls may not solely find it easy to adapt to such changes and may not be able to deliver an efficient task to address human-related security including training, security policies and procedures (Rajivan et al., 2017). This paper would suggest that while automation is useful for the comfortability of the organization, individuals should also be trained on effective use and security including incidence response.

The constantly evolving information security threats and risks in the information system have necessitated preferring solutions needed to mitigate the landscape, this paper suggests that creating a largely technical approach can lead to an incomplete information security of the system and combining both technical and humanistic approach will bring about an effective way of protecting information security.

2.3 Human Cybersecurity Mitigation Methods, Practices, Protocols

Organizations should state and implement a well concise and detailed security policies which outline the acceptable use of the organization's information resources, Bring Your Device and Access Control policies, Security policies can vary based on different organizations it also includes security frameworks and industry standards like International Organization for

Standardization (ISO), National Institute of Standards and Technology (NIST), etc. The goal is to protect the confidentiality, integrity and availability of the organization's information (Paananen et al., 2020; Bhaharin et al., 2019).

Additionally, regular and continuous employee training and awareness are crucial to information security. Employees should be trained on being sensitive to social engineering in and out of the organization, how to detect different types of phishing attacks including vishing, spear phishing and other cyberattacks and threats and how to protect themselves from them, the training should also include the use of materials on how to protect their data (Vernon, 2023). This paper would suggest that although training helps users aware of information security, aligning these training to their daily activity and open communication goes a long way.

Furthermore, risk management is another crucial mitigation method. It is a proactive approach to protecting information within the organization. Risk management involves identifying potential risks and vulnerabilities, assessing the impact of the risk identified, Risk management aims to monitor information assets and ensure their protection. Employees should be trained in the practice of risk management and safeguarding of their digital assets (Grishaeva et al., 2020).

Access control and Authentication should be implemented and monitored. a strong password is a complex unguessed and easy to memorize (Paananen et al., 2020). Organizations should enable appropriate and effective password management policies, even though password policies can vary for different organizations, that allow for complex passwords and passphrases that are lengthy and unique. Periodically change their passwords. An organization should implement Multi-Factor Authentication (MFA), MFA adds an extra layer of security beyond passwords and unauthorized access should be denied at all layers.

Conclusively, a secured communication protocol is a significant mitigation technique that is aimed at protecting the confidentiality, integrity, availability and authenticity of information that is exchanged within the organization. Organizations should implement the use of a secure shell, SSH, for securing communication and encryption for securing messaging applications and emails. Also, organizations should isolate sensitive communications from other communications. Employees should be aware of the importance of effective communication with the use of human-human and human-machine communication protocols like Hypertext Transfer Protocol Secure (HTTPS), Secure/ Multipurpose Internet Mail Extensions (S/MIME) and Virtual Private Network (VPN) for secure remote access and conduct a periodic security audit on the communication channels.

2.4 Models And Frameworks That Support Understanding An Organization's Human Cyber Behavior

NIST Cybersecurity Framework: the NIST Framework is a recognized cybersecurity framework developed by the National Institute of Information Security Technology in the United State. it consists of five (5) core interacting components (Handri et al., 2023); **Identify**, understand the organizational assets including employees and data and identify risks associated with them: **Protect,** develop and implement strategies to Protect the organization's critical assets including employees understanding their roles and responsibilities in security, providing security policies, procedure and employees awareness programs and training such as phishing awareness, strong password practice and behavioural best practice for effective and efficient delivery of acceptable use and safety of critical infrastructure and services; **Detect,** develop and implement measures to identify any cybersecurity incidents that may occur, these measures include anomaly human behavior in among the employees, the use of Security Information event management (SIEM) tools for continuous monitoring, intrusion Detection/Prevention System (ID/PS) for anomaly detection and periodic auditing; **Respond,** includes strategies and measures in place for immediate response to cybersecurity incident detected which includes eradication of the root cause of incidence and containing the impact of the incident and through human error; **Recover,** implementing activities that restore and recover services and data that were impaired due to the incidents, This includes a recovery plan, communication and incident documentation and reporting. This serves as a comprehensive guide to building and protecting information security within an organization.

SANS Security Awareness Maturity Model framework provides a structural approach to assess and improve organization's maturity level by evaluating and enhancing security awareness within an organization. According to Schneider et al. (2020), SANS Model approach focuses on **Role-Based Trainings,** which focuses on the different employees role and how level of security training different from one another**,** for instance, an IT role require a balance between technical and human training for a balanced security culture and an HR role require a more non-technical training such as social engineering, phishing awareness training, risk management and policy awareness; **Behavioural Change Focus,** requires an understanding that an organization desired achievement is a growth behavioural mindset which includes leveraging on tools for and trainings that guides employees and users towards a positive security mindset; **and Effective Security Awareness Training Delivery**, there should be a consistent and periodic security awareness programs, it provides 5 steps to guide organization's security culture such as onboarding security training for new employees and less frequent general security training and more specific trainings. While role-based training is good, this paper would suggest the organization explores diversities in roles due to the unique difference in behavior and roles, this can be done through informal experimentations and observations, more so, humans generally actively pay attention to whatever has a price, organizations should rewards security conscious employees within an organization

Factor Analysis of Information Risk (FAIR) is another framework that can qualitatively analyses the information security risk of an organization including human factors. It analysis risks according to their financial implication and informs making decision by making systematic and structured approached to individually define risk scalability and appetite according to specific needs which ranges from low to high by setting currency corresponding to risks identified. An asset is vulnerable if the capacity of the attacker is higher than the organization's asset can contain (Anderson, 2018). FAIR analysis core taxonomy include (Freund et al., 2014) ; **Assets:** these are items within an organization including people, information and endpoint devices; **Risk,** which is defined as the 'loss Exposure' is the probability of exposure to vulnerability and the loss it might incur; **Loss Event Frequency (LEF**), estimates the rate of threat potential occurrence**; Loss Magnitude (LM**), which can also be called Risk assessment, is the potential financial consequences associated with the risk estimated within a time frame, it could be 'Primary and Secondary' Losses; **Vulnerability**, the weakness that can be exploited by threat agents the weak which can be 'Threat Capability' and 'Resistance Strength' **Threat Event Frequency,** is the time taken for a threat agent to exploit a vulnerability and some exploitation may result in loss. While these frameworks are aids to inform better decision towards evaluating risks of asset within an organization but most human factors such as social engineering, phishing attacks cannot be accurately evaluated, therefor periodic awareness and training cannot be overemphasized and human-focused risk management should also be assessed regularly.

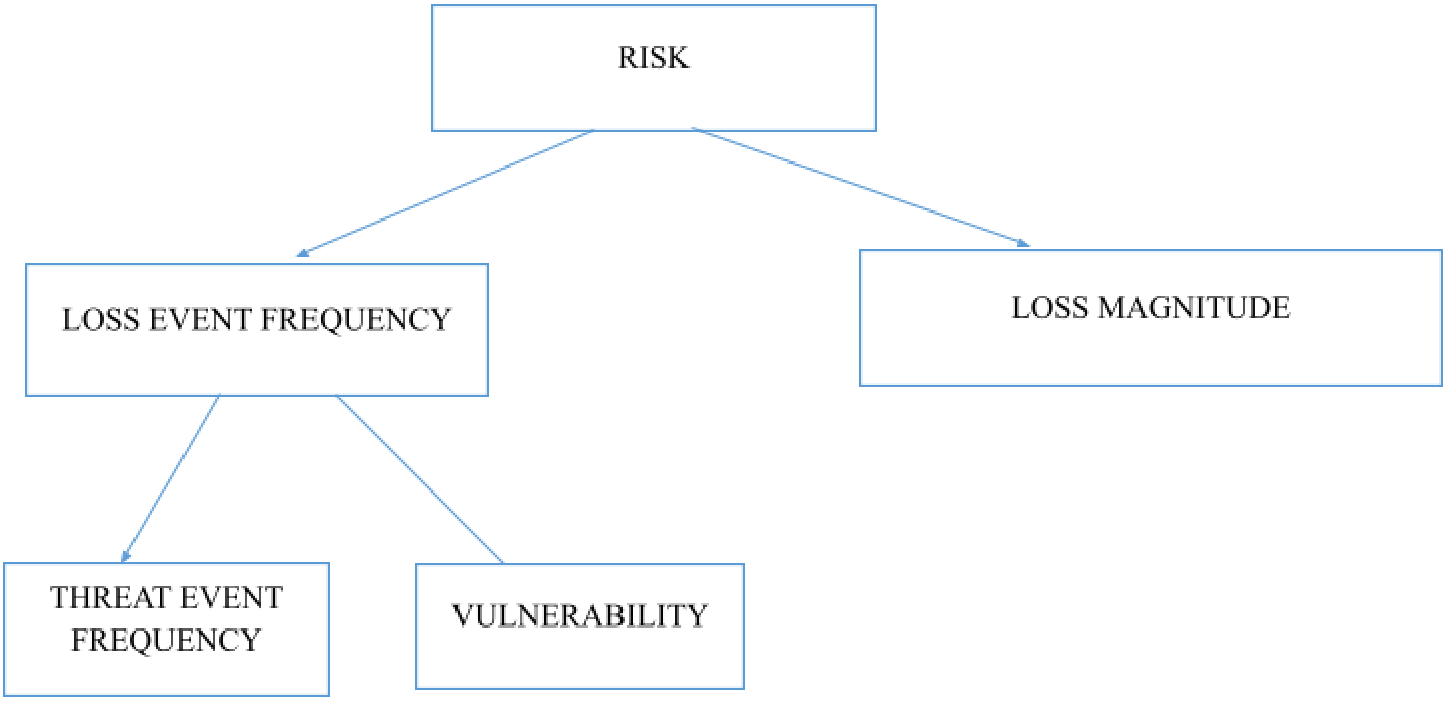

Fig 2 : Fair Loss Event Ontology (Freund et al., 2014)

Adaptation and Adoption Techniques and Practices

Adapting and Adopting techniques and practices are significant against the infiltration of security incidents, organizations need to preserve and protect their information security. To achieve this, the goal of the organization is to ensure a positive security awareness consciousness in the mind of the employees including;

Adaptation Techniques

Organizations should ensure continuous and regular Training and Development among every employee within the organization. Regular training and development are important as they make users aware of the attacks and the threats associated with information systems, understand their principles and how they work and recognize them when they see them through their behavioural characteristics and patterns (Grassegger et al., 2021; McEvoyet al., 2019). For instance, organizations should conduct a periodic phishing awareness training program for their employees, this is also an effective way to recognize and prevent social engineering attacks

Risk Management is another adaptation technique that organizations should imbibe within an organization, risk management is the practice of identifying, qualifying and controlling risks associated with information systems, it involves the identification of the risk associated with the information system, assess the risk to understand the likelihood of the risk and the risk appetite and a step to take to mitigate the risk either by avoiding it, transferring or accepting risk (McIlwraith et al., 2021).

Adoption Techniques

Incentives is an effective adoption technique used to encourage individuals within an organization to comply with the security policies and practices within the organization. Incentives are rewards or recognition given to an individual within an organization to motivate them to comply with the information security practice within the organization. They are designed to encourage a positive security culture and practice within the organization. When incentives are strategically adopted, it will contribute to the growth of the adoption of security practice within the organization.

Furthermore, Feedback provides valuable insights into the information security in identifying individual strengths and weaknesses. Feedback is information about the performance of a system situation and individuals towards identifying the situation of the current information awareness, promoting learning and improvement in information security culture. It could be both positive and negative feedback, the overall goal of feedback is to encourage acceptable and desired behaviour and identify the areas of improvements and solutions to protect information security.

Providing a both adaptation and adoption techniques and practice ensures that organizations maintain a flexible and effective security culture while maintaining their organization.

Conclusion

The human factor is a critical component in the socio-technical system that encompasses training and awareness, user-centered design and techniques used to improve the behavior, motivation of individuals within an organization towards security. As organizations develop their business continuity plan, they should include different approaches to securing information assets and incident response and recovery plans against incidents, it is equally important to understand and address human behavior in cybersecurity to fortify their defense mechanism to information security. The emerging challenges of social engineering attacks and evolution of human-computer interaction signifies the continuous evolution of these considerations. To mitigate against security threats, organizations should cultivate a cybersecurity culture that encompasses benefit, cost, risk and security. Organizations should consider the dynamics of security threats and the evolving the vulnerabilities in human factor landscape, adaptability, continuous and regular assessments and training to create a resilient cybersecurity culture.

3.0 REFERENCE

1. Abdallah, W., 2023. A Systematic Literature Review: Human Factor as Insider threat in Organizations. *International Journal of Computer Science and Information Security (IJCSIS)*, *21*(6).
2. Aiken, M., 2019. *Life in Cyberspace (Volume 5)*. European Investment Bank.
3. Al-Slais, Y. and El-Medany, W.M., 2022. User-centric adaptive password policies to combat password fatigue. *Int. Arab J. Inf. Technol.*, *19*(1), pp.55-62.
4. Alenezi, M.N., Alabdulrazzaq, H. and Mohammad, N.Q., 2020. Symmetric encryption algorithms: Review and evaluation study. *International Journal of Communication Networks and Information Security*, *12*(2), pp.256-272.
5. Alissa, K.A., Alshehri, H.A., Dahdouh, S.A., Alsubaie, B.M., Alghamdi, A.M., Alharby, A. and Almubairik, N.A., 2018, April. An instrument to measure human behavior toward cyber security policies. In *2018 21st Saudi Computer Society National Computer Conference (NCC)* (pp. 1-6). IEEE.
6. Anderson, B., 2018. FAIR Vulnerability Determined using Attack Graphs. In *Proceedings of the International Conference on Security and Management (SAM)* (pp. 285-286). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
7. Andrade, R. et al. (2018) "2018 Ieee 8th Annual Computing and Communication Workshop and Conference (ccwc)," in Management of Information Security Indicators Under a Cognitive Security Model. IEEE, pp. 478–483. doi: 10.1109/CCWC.2018.8301745.
8. Anjum, M., Singhal, S., Kapur, P.K., Khatri, S.K. and Panwar, S., 2023. Analysis of vulnerability fixing process in the presence of incorrect patches. *Journal of Systems and Software*, *195*, p.111525.
9. Bhaharin, S.H., Asma'Mokhtar, U., Sulaiman, R. and Yusof, M.M., 2019, December. Issues and trends in information security policy compliance. In *2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
10. Chandra, J.V., Challa, N. and Pasupuletti, S.K., 2019. Authentication and authorization mechanism for cloud security. *International Journal of Engineering and Advanced Technology*, *8*(6), pp.2072-2078.
11. Chen, L.C. and Cotoranu, A., 2013. Enhancing the Interdisciplinary Curriculum in Cybersecurity by Engaging High-Impact Educational Practices.

12. Da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M., 2020. Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security*, *92*, p.101713.
13. Davis, M.C., Challenger, R., Jayewardene, D.N. and Clegg, C.W., 2014. Advancing socio-technical systems thinking: A call for bravery. *Applied ergonomics*, *45*(2), pp.171-180.
14. Dawson, J. and Thomson, R., 2018. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in psychology*, *9*, p.744.
15. El-kenawy, E.S., Saber, M. and Arnous, R., 2019. An integrated framework to ensure information security over the internet. *International Journal of Computer Applications*, *975*, p.8887.
16. Evans, M., He, Y., Maglaras, L. and Janicke, H., 2019. HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, pp.74-89.
17. Freund, J. and Jones, J., 2014. *Measuring and managing information risk: a FAIR approach*. Butterworth-Heinemann.
18. Grassegger, T. and Nedbal, D., 2021. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, pp.59-66.
19. Grishaeva, S.A. and Borzov, V.I., 2020, September. Information security risk management. In *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 96-98). IEEE.
20. Handri, E.Y., Putro, P.A.W. and Sensuse, D.I., 2023, August. Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government. In *2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (pp. 82-87). IEEE.
21. Karamagi, R., 2022. A Review of Factors Affecting the Effectiveness of Phishing. *Computer and Information Science*, *15*(1).
22. Khando, K., Gao, S., Islam, S.M. and Salman, A., 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, *106*, p.102267.
23. Kim, H., Kwon, H. J. and Kim, K. K. (2019) "Modified Cyber Kill Chain Model for Multimedia Service Environments," Multimedia Tools and Applications : An International Journal, 78(3), pp. 3153–3170. doi: 10.1007/s11042-018-5897-5.
24. Levin, I. and Mamlok, D., 2021. Culture and society in the digital age. *Information*, *12*(2), p.68.
25. Mahfuth, A., 2019. Human factor as insider threat in organizations. *International Journal of Computer Science and Information Security (IJCSIS)*, *17*(12), pp.December-2019.
26. McAlaney, J. and Benson, V., 2020. Cybersecurity as a social phenomenon. In *Cyber influence and cognitive threats* (pp. 1-8). Academic Press.
27. McEvoy, T.R. and Kowalski, S.J., 2019. Deriving cyber security risks from human and organizational factors–a socio-technical approach. *Complex Systems Informatics and Modeling Quarterly*, (18), pp.47-64.

28. McIlwraith, A., 2021. *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.
29. Momoh, I., Adelaja, G. and Ejiwumi, G., 2023. Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution.
30. Paananen, H., Lapke, M. and Siponen, M., 2020. State of the art in information security policy development. *Computers & Security*, *88*, p.101608.
31. Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, *7*(6), pp.4682-4696.
32. Rahman, T., Rohan, R., Pal, D. and Kanthamanon, P., 2021, June. Human factors in cybersecurity: a scoping review. In *The 12th International Conference on Advances in Information Technology* (pp. 1-11).
33. Rohan, R., Funilkul, S., Pal, D. and Chutimaskul, W., 2021, December. Understanding of human factors in cybersecurity: A systematic literature review. In *2021 International Conference on Computational Performance Evaluation (ComPE)* (pp. 133-140). IEEE.
34. Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), pp.122-131.
35. Schneider, B., Asprion, P.M., Androvicsova, S. and Azan, W., 2020. A Practical Guideline for Developing a Managerial Information Security Awareness Program.
36. Scott, J. and Kyobe, M., 2021, December. Trends in cybersecurity management issues related to human behaviour and machine learning. In *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)* (pp. 1-8). IEEE.
37. Sony, M. and Naik, S., 2020. Industry 4.0 integration with socio-technical systems theory: A systematic review and proposed theoretical model. *Technology in society*, *61*, p.101248.
38. Strigini, L. and Gadala, M., 2020, February. Human Factors Standards and the Hard Human Factor Problems: Observations on Medical Usability Standards. In *Proceedings of the 13th International Joint Conference on Biomedical Engineering Systems and Technologies* (pp. 766-773). SCITEPRESS.
39. Tahaei, M. and Vaniea, K., 2019, June. A survey on developer-centred security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 129-138). IEEE.
40. Vernon, N., 2023. EMPLOYEE AWARENESS AND TRAINING. *EDPACS*, *68*(4), pp.26-37.
41. Wang, Z., Zhu, H. and Sun, L., 2021. Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, pp.11895-11910.