Oluwafemi Mark Eke

S4215516

Fintech

FT7207

Human factor in Cybersecurity Assignment

Contents

[INTRODUCTION 3](#_Toc134659419)

[BODY 4](#_Toc134659420)

[BEHAVIOUR 5](#_Toc134659421)

[CYBERPSYCHOLOGY 5](#_Toc134659422)

[SOCIAL ENGINEERING 6](#_Toc134659423)

[PHISHING 6](#_Toc134659424)

[MITIGATION OF NON-MALICIOUS INSIDER THREAT 8](#_Toc134659425)

[CONCLUSION 9](#_Toc134659426)

[REFERENCES 10](#_Toc134659427)

# INTRODUCTION

The current era has made technology a necessity in the development of businesses by improving the ease of doing business (Susan & Novianti, 2019). The internet is one of the technological innovations that has affected every life, which has created significant potential and has led to the creation of new concepts such as e-commerce and e-business (Apăvăloaie, 2014). This technological innovation called the Internet currently hosts about 3 billion users and has raised billions of dollars annually for the global economy through its vast global network (Corallo et al., 2020; Li & Liu, 2021). Currently, the majority of economic, commercial, cultural, social, and governmental activities and interactions between countries, including those involving individuals, non-governmental organizations, and government institutions, take place in the virtual realm of cyberspace (Li & Liu, 2021).

The world is witnessing a significant expansion of cyberspace, and this rapid growth in information presents opportunities for those with malicious intentions (Arora, 2016). Consequently, it is essential to take action to protect against these threats, as they pose a serious and urgent danger (Arora, 2016). Cyber-attacks are on the rise such that the annual increase in cost related to cybercrime will reach 10 trillion dollars in 2025 (Jim Boehm et al., 2022). On average, there are approximately 2,200 cybersecurity attack incidents that occur per day, even a study from the University of Maryland shows that a cyberattack attempt occurs every 39 seconds (Ashley Watters, 2023). In 2022, the UK had the highest number of cybercrime victims per million internet users, with 4783, a 40% increase from 2020; the USA had the next highest number of victims per million internet users, with 1494, a 13% decrease from 2020, and both countries had significantly more victims compared to other countries, with the USA having 759% more victims in 2021 than the next-highest country, Canada (Charles Griffiths, 2023b). However, the good news is that the cybersecurity industry is not only keeping up with the learning rate of malicious actors but also growing, this growth provides hope for better protection against cyber threats (Ashley Watters, 2023).

The importance of cybersecurity cannot be overstated, as it involves ensuring the integrity, confidentiality, and availability (ICA) of an organization's computing assets, as well as those connected to other networks (Kaur & Ramkumar, 2022). Given the scale and complexity of cyber-attacks, significant investments are being made in cybersecurity to rectify or prevent cyber breaches. By the end of 2025, there will be an estimated 3.5 million unfilled cybersecurity jobs, yet the job market is predicted to grow 33% between 2021 and 2031, with the median average wage for a cybersecurity professional being $102,600 (Ashley Watters, 2023; Bureau of Labor Statistics, 2022). In 2022, the average cost of a cyber breach was $4.35 million due to investment in the prevention of cyber breaches, and cybercrime is estimated to have cost the global economy around $7 trillion, due to investment in the prevention of cyber breeches which is expected to rise to $10.5 trillion by 2025 (Charles Griffiths, 2023). According to Maddy Ell & Robbie Gallucci, ( 2022), out of the 39% of businesses that recognized being attacked, 83% of them experienced phishing attempts, while 21% experienced more advanced attack types such as denial of service, malware, or ransomware attacks.

Phishing attacks are the most common type of cyber threat, which serve as a gateway for more devastating attacks like ransomware, as success in these initial attacks can provide hackers with the means to escalate their efforts by having users follow malicious links to spoof websites or download malware (Charles Griffiths, 2023a). Phishing is the most frequent cybercrime, with around 3.4 billion spam emails sent daily, and despite Google's cyber security measures blocking 99.9% of phishing attempts, 48% of all emails sent in 2022 were spam and around 50% of global cybercrime victims in 2021 were victims of phishing attacks (Charles Griffiths, 2023). In 2021, Asian organizations were mostly targeted by phishing attacks, which are the most prevalent form of cyber-attack, and a data breach against an organization has an average cost exceeding $4 million.(Charles Griffiths, 2023a). Though many of these cyber breaches are caused by human error rather than technology failures (Ashley Watters, 2023). Ofir Hason, (2018) stated the human factor is the weakest link in cyber breach mitigation and prevention, insisting on the education of people on security policies, tools, and technology. ISACA and the CMMI Institute, (2018) also noted humans as essential in any organization's cybersecurity management strategy. 94% of organizations experienced insider data breaches in 2020, with human error being the top cause of serious incidents according to 84% of IT leaders surveyed, noting phishing attacks as the cause of 73% of data breaches (Egress, 2021).

This study aims to analyse the non-malicious insider threat in an organization, specifically in the context of phishing. It will explore why unintentional insider threat through phishing is becoming more prevalent. This study seeks to evaluate this by dissecting the concept of cybersecurity into main themes such as behaviour, cyberpsychology, social engineering and phishing to be able to analyse the link between this concept in describing the root cause of non-malicious insider threat in regard to phishing and how it can be mitigated.

# BODY

Cybersecurity attacks can be internal or external, but when comparing both, most internal attacks are more difficult to detect and prevent due to the difficulty in distinguishing between non-malicious use cases to malicious attacks (Schulze, 2019). To properly understand the threat insiders, pose to an organization, it is important to have a precise definition of what insider threat is which will be inclusive of the areas being affected by this type of cyber-attack. There is some form of consensus in the definition of insider threat regarding its scope in an organization. According to Schulze insider threat report, (2019) insider threats are security threats that do not originate from malicious outsiders or malware but from trusted insiders with access to sensitive data and systems - both malicious insiders and negligent insiders. It is the possibility that a person who has been granted or previously had permission to access an organization's essential resources may use their access, either deliberately or accidentally, to engage in actions that may have adverse effects on the organization (Costa Daniel, 2017). It is the intentional or unintentional attempt by an insider through authorized access to cause harm to the organization's resources, information, personnel, equipment, networks, or systems using their access (Cybersecurity and Infrastructure Security Agency., n.d.). There are two types of insider threats, which are categorized malicious insiders and non-malicious or unintentional insiders whose activities endanger the confidentiality, integrity and availability of the business (Mazzarolo & Jurcut Delia, 2019). While this study focuses on non-malicious insider threats, Cybersecurity and Infrastructure Security Agency (n.d.) links insider threat to behaviour as the route through which it becomes an attack.

## BEHAVIOUR

Human behaviour plays a significant role in determining a person's actions and can offer valuable insights that aid in anticipating their future behaviour (Mazzarolo & Jurcut Delia, 2019). Studies suggest that there is a connection between human behaviour and cybersecurity attacks, indicating that an organization's susceptibility to an attack is contingent on the behavioural patterns of insiders. Studies further show that behavioural patterns are linked to motives (Kim et al., 2023) and personality traits or characteristics (Dupuis & Khadeer, 2016; Harms et al., 2022). Over the years there have been several approaches to identifying these behavioural patterns and being more proactive in preventing insider threats or attacks. Some of these common approaches are, behavioural analysis (M. Singh et al., 2020; Zargar et al., 2016), machine learning (Le et al., 2020; Mayhew et al., 2015; Tuor et al., 2017; Zhang et al., 2018) and taxonomies (Homoliak et al., 2019; Posey et al., 2013). Behavioural patterns including the motives and personality characteristics are better explained by investigating the psychology behind it, this is where the concept of cyberpsychology comes in.

## CYBERPSYCHOLOGY

The way we communicate and share information has changed with the growth of technology becoming interrelated, creating technological intimacy, and causing the emergence of cyberpsychology (Ancis, 2020). Research has shown that human behaviour has experienced some negative influences from technology which are labelled as digital anxiety and digital addiction (A. K. Singh & Singh, 2019), which can easily be taken advantage of by cyber attackers. The concept of cyberpsychology is the understanding of all aspects of human behaviour in relation to technology (Attrill-Smith et al., 2018). Psychological factors in cyber behaviour which can provide valuable insight to cybersecurity researchers, practitioners, and decision-makers, helping them understand motivations and vulnerabilities and develop effective tools, measures, policies, and laws (Crooks, 2022). This is important because it is well known now that attackers can manipulate people's minds rather than the computer systems themselves using social engineering (tricking people to gain information like passwords) and cognitive hacking (spreading false information) to hack into a computer network or system (Cybenko et al., 2002; Thompson, 2004; McAlaney et al., 2015; King et al., 2018; Fraunholz et al., 2019). This further explains why humans are regarded as the weak link.

## SOCIAL ENGINEERING

There is a high usage of the internet due to how it makes life easier and better, with shopping, banking and telecommunication which involves the use of social media, all this involves upload of personal data of which cyber attackers have developed techniques such as social engineering and phishing in order to obtain this information (Syed  Mohammed Adib, 2021). Social Network Sites (SNSs), mobile communication, the Industrial Internet and the Internet of Things (IoT) gather a lot of information about people and devices, thereby increasing the attack channel and bigger attack surface (Wang et al., 2021). Cyber attackers have shifted from the use of technicality to access systems into the use of psychology and techniques to focus on the weak link which is the user behind the system, by playing on the negligence of the users to create vulnerabilities around systems through the means of infecting systems, stealing credentials and transferring funds. Social engineering is a technique developed by attackers to exploit human weakness in achieving malicious aims (Breda et al., 2017a, 2017b; Syed  Mohammed Adib, 2021), by manipulation, influence, persuasion, and inducing (Butavicius et al., 2015). Several researchers have developed models to describe social engineering. One of such models was created to describe the main perspectives in social engineering, which are the attacker perspective, the victim perspective, the perspective of principle and explaining (Butavicius et al., 2015; Wang et al., 2021). Breda et al, (2017) further categorized social engineering into hunting and farming. Social engineering is also known to be in four phases known as the research, hook, play and exit phase(Breda et al., 2017). Cyber attackers are also motivated by several factors such as financial gain, espionage, entertainment, ego and challenge to dismantle the weak link using social engineering to collect confidential information from users behind the system by exploiting the greed, fear and curiosity of users (Syed Mohammed Adib, 2021), which is explored by using a popular technique known as phishing.

## PHISHING

Phishing is a subset of social engineering and one of the most commonly used social engineering technique used in manipulating users to giving cyber attackers personal or confidential information like passwords and bank details by clicking on suspicious links and downloading malware (Cisco, n.d; Graphus, 2022). Phishing is described as a form of social engineering that uses email, websites and identity theft to manipulate or coerce the victim into revealing personal data or confidential information(Cisco, n.d; CISA, 2021; Graphus, 2022). (Cisco, n.d) There are several types of phishing attack which have different functions such as spear phishing (focuses on specific individuals) and whale phishing(targets top executives in an organization) and it can be done in the form of smirching or vishing (CISA, 2021). Social engineering attack is increasing in sophistication and efficiency, in way not too long from now might be the predominant threat in cyber security (Breda et al., 2017). According to CyberTalk, (2022) report, 1 in 99 emails is phishing while 90% of data breaches occur in the account of phishing. Tessian, (2023) listed some of the biggest phishing attacks:

1. $100 Million Google and Facebook Spear Phishing Scam
2. Persuasive email phishing attack imitates US Department of Labor
3. Russian hacking group targets Ukraine with spear phishing
4. Deepfake Attack on UK Energy Company
5. $60 Million CEO Fraud Lands CEO In Court
6. Microsoft 365 phishing scam steals user credentials
7. Singapore bank phishing saga like ‘fighting a war’
8. Ransomware gang hijacks victim’s email account
9. Phishing scam uses HTML tables to evade traditional email security
10. Sacramento phishing attack exposes health information
11. Google Drive collaboration scam
12. Sharepoint phishing fraud targets home workers
13. $75 Million Belgian Bank Whaling Attack
14. High-Profile Twitters Users’ Accounts Compromised After Vishing Scam
15. Texas Attorney-General Warns of Delivery Company Smishing Scam

From analysing these phishing attacks, it is clear that it is targeted at the non-malicious insider. Using spear phishing attack to understand the behaviour and cyberpsychology of the victim, while engaging in social engineering to manipulate and gather confidential information for malicious purposes. This does not only point at the fact that cybercriminals are going after the weak link but also reveals an unintentional threat within an organization, called the non-malicious insider threat by literature. Desolda et al., (2021) systematic literature review, reveals 5 factors that are considered from a human perspective (given the established point that the human factor is the weak link), as the factors that are addressed by literature in evaluating human-centred threats in an organization, which will help in creating mitigation strategies:

1. Lack of knowledge
2. Lack of resources
3. Lack of awareness
4. Norms
5. Complacency

This factors are addressed and applied in creating mitigation strategies for non malicious insider threat.

## MITIGATION NON-MALICIOUS INSIDER THREAT

Cyber Security Culture

Cybersecurity culture is the reflection of people’s knowledge, beliefs, perceptions, attitudes, assumptions, norms and values in cybersecurity and how they are manifested in people’s behaviour in relation to information technology (ENISA, 2017). The main objective of the cybersecurity culture is to create an established ground for social and psychological support in cybersecurity (Alvarez-Dionisi Emilo Luis & Urrego-Baquero Nelly, 2019; Uchendu et al., 2021). The enactment of cyberculture has to be spearheaded by the leadership of the organization, through policies and routines till it becomes a culture (Uchendu et al., 2021). Alshaikh, (2020) highlighted five initiatives for creating a cybersecurity culture:

1. identifying key cyber security behaviours,
2. establishing a 'cyber security champion' network,
3. developing a brand for the cyber team,
4. building a cyber security hub,
5. aligning security awareness activities with internal and external campaigns

This will help in influencing employees’ attitudes and behaviour toward cybersecurity

Cyber Hygiene

Cyber hygiene can be an effective tool for mitigating non-malicious insider threats in organizations. By establishing strong cybersecurity practices and policies, organizations can reduce the risk of insider threats caused by human error or negligence. For instance, by ensuring that employees are trained in best practices for password management, data handling, and network security, organizations can reduce the likelihood of employees inadvertently leaking sensitive information or falling prey to phishing attacks. Similarly, by regularly updating software and systems, implementing access controls and monitoring systems, and establishing incident response plans, organizations can better detect and respond to insider threats before they can cause significant damage. Overall, a comprehensive approach to cyber hygiene that includes employee training, technical controls, and incident response planning can go a long way toward mitigating the risk of non-malicious insider threats in organizations.

Cybersecurity Awareness

Cyber security awareness is the knowledge and understanding of the potential threats and risks that exist in the online environment and how to prevent or respond to them. Cyber security awareness can help mitigate non-malicious insider threat, which is the risk of an employee or contractor unintentionally causing harm or damage to an organization’s information or systems due to negligence, error, or ignorance (Infosecurity Magazine, 2021; NPSA, n.d.; CSO Online, 2021). By raising cyber security awareness among employees, organizations can educate them on the best practices and policies for cybersecurity, such as using strong passwords, updating software and antivirus programs, avoiding suspicious links and attachments, backing up data, and encrypting sensitive information (NPSA, n.d.; cyber.uk, n.d.). Cybersecurity awareness can also help employees recognize and report any suspicious or unusual activities or incidents that may indicate a cyberattack or a breach (CSO Online, 2021; NPSA, n.d.). By increasing cyber security awareness, organizations can reduce the likelihood of non-malicious insider threat and enhance their overall cybersecurity posture (Infosecurity Magazine, 2021; NPSA, n.d.).

Security Access

Security access is the control and management of who can access what information or systems within an organization. Security access can help mitigate non malicious insider threat, which is when an employee or contractor unintentionally causes harm or damage to an organization’s information or systems due to negligence, error, or ignorance. By implementing security access measures, such as access levels, passwords, authentication, authorization, encryption, and logging, organizations can reduce the exposure and impact of non malicious insider threat. Security access can also help monitor and audit the activities and behaviors of employees and contractors, and detect and respond to any anomalies or incidents that may indicate a non-malicious insider threat. By applying security access principles, organizations can protect their information and systems from unauthorized or accidental access by insiders.

Employee monitoring

Employee monitoring can be used as a mitigation strategy for non-malicious insider threats. Employee monitoring involves the use of technology to track and analyze employee activities and behaviours, such as computer usage, network access, and communication patterns. By monitoring employee behavior, organizations can detect potential insider threats before they cause significant harm or damage. However, it is important to balance the need for monitoring with employee privacy and ethical considerations. Organizations should clearly communicate their employee monitoring policies and obtain informed consent from employees before implementing any monitoring measures.

# CONCLUSION

In conclusion, this study has shown that non-malicious insider threats pose a significant risk to organizations' cybersecurity. Understanding user behavior and cyberpsychology is crucial in developing effective strategies to mitigate these threats. Social engineering and phishing attacks are commonly used by attackers to exploit human vulnerabilities and gain access to sensitive information or systems. To counter these attacks, organizations should focus on improving cybersecurity culture, promoting cyber hygiene, raising cybersecurity awareness, implementing security access measures and monitoring employees. By adopting a comprehensive approach that combines technical controls and employee education and training, organizations can reduce the risk of non-malicious insider threats and enhance their overall cybersecurity posture. It is essential to recognize that cybersecurity is not solely a technical issue, but a people issue as well, and organizations must invest in creating a security-aware culture that encourages safe and secure behaviour among their employees.

# REFERENCES

1. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*, 102003. https://doi.org/10.1016/j.cose.2020.102003
2. Alvarez-Dionisi Emilo Luis, & Urrego-Baquero Nelly. (2019, March 15). *Implementing a Cybersecurity Culture*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture
3. Ancis, J. R. (2020). The age of cyberpsychology: An overview. *Technology, Mind, and Behavior*, *1*(1). https://doi.org/10.1037/TMB0000009
4. Apăvăloaie, E.-I. (2014). The Impact of the Internet on the Business Environment. *Procedia Economics and Finance*, *15*, 951–958. https://doi.org/10.1016/S2212-5671(14)00654-6
5. Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, *8*, 540–542. https://doi.org/10.1016/J.PISC.2016.06.014
6. Ashley Watters. (2023, January 27). *Top 50 Cyber Security Statistics and Facts | CompTIA*. Comptia. https://connect.comptia.org/blog/cyber-security-stats-facts
7. Attrill-Smith, A., Fullwood Chris, Keep Melanie, & Kuss Daria J. (2018). The Oxford Handbook of Cyberpsychology. *The Oxford Handbook of Cyberpsychology*. https://doi.org/10.1093/OXFORDHB/9780198812746.001.0001
8. Breda, F., Barbosa, H., & Morais, T. (2017a). SOCIAL ENGINEERING AND CYBER SECURITY. *INTED2017 Proceedings*, *1*, 4204–4211. https://doi.org/10.21125/INTED.2017.1008
9. Breda, F., Barbosa, H., & Morais, T. (2017b). SOCIAL ENGINEERING AND CYBER SECURITY. *INTED2017 Proceedings*, *1*, 4204–4211. https://doi.org/10.21125/INTED.2017.1008
10. Bureau of Labor Statistics. (2022, September 8). *Occupational Outlook Handbook, Information Security Analysts*. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
11. Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2015). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *ACIS 2015 Proceedings - 26th Australasian Conference on Information Systems*.
12. Charles Griffiths. (2023a, April 6). *Cyber Crime Statistics*. The Latest Cyber Crime Statistics (Updated April 2023) | AAG IT Support. https://aag-it.com/the-latest-cyber-crime-statistics/
13. Charles Griffiths. (2023b, April 6). *The Latest Phishing Statistics* . AAG IT Support. https://aag-it.com/the-latest-phishing-statistics/
14. Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, *114*, 103165. https://doi.org/10.1016/J.COMPIND.2019.103165
15. Costa Daniel. (2017, March 7). *CERT Definition of Insider Threat*. SEI Blog. https://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/
16. Crooks, C. (2022). *Cyberpsychology & Future of Cybersecurity Research*. https://smartech.gatech.edu/handle/1853/66379
17. Cybenko G., Giani A., Thompson P. (2002). Cognitive hacking: a battle for the mind.
18. Cybersecurity and Infrastructure Security Agency. (n.d.). *Defining Insider Threats* . Retrieved April 27, 2023, from https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
19. CyberTalk. (2022, March 30). *Top 15 phishing attack statistics*. https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/
20. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021). Human Factors in Phishing Attacks: A Systematic Literature Review. *ACM Computing Surveys (CSUR)*, *54*(8). https://doi.org/10.1145/3469886
21. Dupuis, M., & Khadeer, S. (2016). Curiosity Killed the Organization: A Psychological Comparison between Malicious and Non-Malicious Insiders and the Insider Threat. *RIIT 2016 - Proceedings of the 5th Annual Conference on Research in Information Technology*, 35–40. https://doi.org/10.1145/2978178.2978185
22. Egress. (2021). *Insider Data Breach Survey 2021*.
23. ENISA. (2017). *Cyber Security Culture in organisations* . https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations
24. Fraunholz D., Anton S. D., Lipps C., Reti D., Krohmer D., Pohl F., et al. (2019). Demystifying deception technology: a survey. arXiv [Preprint] arXiv:1804.06196
25. Graphus. (2022). Is Phishing a Social Engineering Attack? Retrieved from https://www.graphus.ai/blog/is-phishing-a-social-engineering-attack/
26. Harms, P. D., Marbut, A., Johnston, A. C., Lester, P., & Fezzey, T. (2022). Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats. *Journal of Information Security and Applications*, *71*. https://doi.org/10.1016/j.jisa.2022.103378
27. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. In *ACM Computing Surveys* (Vol. 52, Issue 2). <https://doi.org/10.1145/3303771>
28. Infosecurity Magazine. (2021). How to mitigate non-malicious insider risk (and why employee awareness is key). https://securityitsummit.co.uk/briefing/how-to-mitigate-non-malicious-insider-risk-and-why-employee-awareness-is-key/
29. ISACA and the CMMI Institute. (2018). *Narrowing the culture gap for better business RESULTS*. https://hbr.org/2012/04/the-new-science-of-building-great-teams
30. Jim Boehm, Dennis Dias, Charlie Lewis, Kathleen Li, & Daniel Wallance. (2022). *Cybersecurity trends: Looking over the horizon | McKinsey*. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon
31. Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*, *34*(8), 5766–5781. https://doi.org/10.1016/J.JKSUCI.2021.01.018
32. Kim, D. W., Shin, G. Y., & Han, M. M. (2023). Anomaly Detection Based on Discrete Wavelet Transformation for Insider Threat Classification. *Computer Systems Science and Engineering*, *46*(1). https://doi.org/10.32604/csse.2023.034589
33. King Z. M., Henshel D. S., Flora L., Cains M. G., Hoffman B., Sample C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Front. Psychol. 9:39. 10.3389/fpsyg.2018.00039.
34. Le, D. C., Zincir-Heywood, N., & Heywood, M. I. (2020). Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning. *IEEE Transactions on Network and Service Management*, *17*(1). https://doi.org/10.1109/TNSM.2020.2967721
35. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/J.EGYR.2021.08.126
36. Maddy Ell, & Robbie Gallucci. (2022). Cyber Security Breaches Survey 2022 - GOV.UK. In *GOV.UK*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
37. Mayhew, M., Atighetchi, M., Adler, A., & Greenstadt, R. (2015). Use of machine learning in big data analytics for insider threat detection. *Proceedings - IEEE Military Communications Conference MILCOM*, *2015-December*. https://doi.org/10.1109/MILCOM.2015.7357562
38. Mazzarolo, G., & Jurcut Delia, A. (2019). Insider threats in Cyber Security: The enemy within the gates. *Arxiv*, *11*.
39. McAlaney J., Taylor J., Faily S. (2015). The social psychology of cybersecurity.
40. NPSA. (n.d.). Reducing insider risk. https://www.npsa.gov.uk/reducing-insider-risk
41. Ofir Hason. (2018). *The Human-Factor in Cybersecurity Training: Why Adopting a Holistic Approach Is Most Valuable - CPO Magazine*. CPO Magazine. https://www.cpomagazine.com/cyber-security/the-human-factor-in-cybersecurity-training-why-adopting-a-holistic-approach-is-most-valuable/
42. Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders’ protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly: Management Information Systems*, *37*(4). https://doi.org/10.25300/MISQ/2013/37.4.09
43. Schulze, H. (2019). *Insider Threat Report*.
44. Singh, A. K., & Singh, P. K. (2019). The study of psychological factors in cyber behavior can provide valuable insight to cybersecurity researchers, practitioners, and decision makers, helping them understand motivations and vulnerabilities and develop effective tools, measures, policies, and laws. *Library Philosophy and Practice (e-Journal). 2656*.
45. Singh, M., Mehtre, B. M., & Sangeetha, S. (2020). Insider Threat Detection Based on User Behaviour Analysis. *Communications in Computer and Information Science*, *1241 CCIS*. https://doi.org/10.1007/978-981-15-6318-8\_45
46. Susan, A., & Novianti, W. (2019). Benefits of Technology for Business. *IOP Conference Series: Materials Science and Engineering*, *662*(3). https://doi.org/10.1088/1757-899X/662/3/032036
47. Syed  Mohammed Adib. (2021, June). *Social engineering: Concepts, Techniques and Security Countermeasures*. https://www.researchgate.net/publication/353567848\_Social\_engineering\_Concepts\_Techniques\_and\_Security\_Countermeasures
48. Tessian. (2023). 15 Examples of Real Social Engineering Attacks - Updated 2023. Retrieved from https://www.tessian.com/blog/examples-of-social-engineering-attacks/
49. Thompson P. (2004). Cognitive hacking and intelligence and security informatics. Proc. SPIE 5423 142–151.
50. Tuor, A., Kaplan, S., Hutchinson, B., Nichols, N., & Robinson, S. (2017). Deep learning for unsupervised insider threat detection in structured cybersecurity data streams. *AAAI Workshop - Technical Report*, *WS-17-01-WS-17-15*.
51. Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387
52. Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access*, *9*, 11895–11910. https://doi.org/10.1109/ACCESS.2021.3051633
53. Zargar, A., Nowroozi, A., & Jalili, R. (2016). XABA: A zero-knowledge anomaly-based behavioral analysis method to detect insider threats. *13th International ISC Conference on Information Security and Cryptology, ISCISC 2016*. https://doi.org/10.1109/ISCISC.2016.7736447
54. Zhang, D., Zheng, Y., Wen, Y., Xu, Y., Wang, J., Yu, Y., & Meng, D. (2018). Role-based log analysis applying deep learning for insider threat detection. *Proceedings of the ACM Conference on Computer and Communications Security*. https://doi.org/10.1145/3267494.3267495