INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

Driving Technological Innovation for a Resilient Cybersecurity Landscape

***Muritala Aminu[1], Sunday Anawansedo[2], Yusuf Ademola Sodiq[3] and Oladayo Tosin Akinwande[4]**

[1]Master of Science in Information Technology, a Bachelor of Science in Physics, and an HND in Electrical and Electronics Engineering

[2]Master's degree in Electrical Engineering from the Southern University of Agriculture and Mechanical College

[3]Master's student at the prestigious University of Salford, Manchester, UK

[4]Assistant lecturer in Software Engineering department of Veritas University

***Corresponding Author**

DOI: https://doi.org/10.51583/IJLTEMAS.2024.130414

Received: 29 February 2024; Accepted: 09 March 2024; Published: 10 May 2024

Abstract: It is more important than ever to have a cybersecurity environment that is resilient and secure in this age of widespread digital connectivity. This research paper explores how developing technological innovation can serve as the foundation for building resilience in cyberspace. The study covers important aspects of cybersecurity, including its conceptual foundations, a wide range of applications, risk-reduction strategies, and the crucial role that policy regulation plays in the digital environment. In conclusion, the paper suggests that technological innovation is the driving force behind transformative change in cybersecurity. Policymakers, business executives, cybersecurity professionals, and researchers are all affected by the implications, which call for a coordinated and flexible strategy to meet the challenges of the digital frontier.

Keywords: cybersecurity, technological advancement, digital space, resilient cybersecurity, cyber threats

I. Introduction

The idea of resilience has become essential for protecting sensitive data and digital infrastructures in the rapidly evolving field of information security (Saeed et al., 2023). In the context of cybersecurity, resilience is the ability of a system to tolerate, adapt to, and recover from unanticipated challenges, such as intrusions, disruptions, and cyber attacks (Gould, 2018).Technological innovations are substantially supported by emerging technologies like cloud computing, blockchain, artificial intelligence, big data and analytics, the Internet of Things, and the industrial Internet of Things (Akter et al., 2020; Distor et al., 2023). These technologies utilized across organizations and other establishments are intensifying the drive toward digital transformation because of their many benefits. However, entities now face cybersecurity challenges,necessitating the security of their digital transformation resources to maintain continuity.

According to Cremer et al., (2022), the estimated cost of cybercrime to the world economy in 2020 was less than $1 trillion, a rise of more than 50% from 2018. The average amount of money paid out for cyber insurance claims increased from USD 145,000 in 2019 to USD 359,000 in 2020, indicating a growing need for standardized databases, public awareness campaigns, and improved cyber information sources. Furthermore, estimates by Smith et al., (2020), revealed that the global economy suffered damages from inadequate cybersecurity amounting to USD 945 billion, with an average of 2,200 cyberattacks daily, every 39 seconds and cybercrime projection costs of $8 trillion by 2023 (report by Astra Inc.). The impact of cyberspace as a basic and essential business requirement is impossible to overstate. Therefore, this phenomenon of growing integration presents new opportunities as well as risks. Cybersecurity is becoming a strategic issue at the core of the digital environment due to the growth of digital technologies, exponential data growth, and changing organizational needs (Abion et al., 2014; Kaur et al., 2023).

Resilience plays a role in ensuring that cybersecurity issues are addressed proactively (Safitra et al., 2023). However, Abdullayeva (2023) and Appiah et al., (2020) reported that while strengthening perimeters and preventing unauthorized access are common goals of conventional security systems and measures, resilience emphasizes that breaches will inevitably occur. In this regard, a transition may occur from a strategy that is only preventative to one that is more focused on recovery, response, and detection. Consequently, a resilient cybersecurity environment highlights that, in order to stay ahead of potential risks, cyber threats are dynamic and sophisticated, requiring constant adaptation and innovation (Safitra et al., 2023). Despitethe difficulty, resilience is essential because of the effects of cyber incidents and to ensure that organizations can perform vital functions. Though, resilience goes beyond simply responding to events; it also includes risk assessment, strategic planning, and the incorporation of cutting-edge technologies to improve overall cyber defense capabilities (Alrumaih et al., 2023).

The ability of an entity to continue operating is directly linked to its resilience therefore, cybersecurity-related issuescan have serious repercussions, such as damage to credibility and monetary losses (Perera et al., 2022). In conjunction with safeguarding sensitive data, a resilient cybersecurity environment also maintains stakeholders' and customers' trust. As a result, cybersecurity

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

measures must be of top priority as the adoption of relevant technological innovations becomes more accepted globally to ensure systems are safe from potential threats. As the digital world is becoming increasingly interconnected it is crucial to develop a robust cybersecurity environment.In this context, this study explores the advancement of technological innovation for developing resilient cybersecurity. The paper intends to contribute to the present debate on strengthening digital infrastructures against emerging cyber threats by examining cutting-edge technologies. Understanding the significance of resilience opens the opportunity for a comprehensive investigation into the various ways in which technological innovation can revolutionize cybersecurity and keep the digital environment flexible, strong, and ready for the demands of the digital age.

II. Concept of Cybersecurity

The concept of cyber resilience represents a fundamental paradigm shift of a proactive and flexible strategy for safeguarding digital infrastructures against constantly changing threats within theevolving field of cybersecurity (Safitra et al., 2023).A complex collection of guidelines and practices associated with cyber resilience are intended to enable an entity to withstand and recover from cyberattacks, but also continuously adjust and strengthen its defenses.Resilience is a multidisciplinary concept that incorporates definitions and perspectives from ecology, society, psychology, organizations, and engineering. Similarly, there are common themes and resilience features among these various disciplines, despite the multi-disciplinary conceptof resilience (Connelly et al., 2017).

Cyber resilience emphasizes continuity, adaptability, and quick recovery in the face of disruptions while acknowledging that breaches are unavoidable, in contrast to common cybersecurity approaches that primarily focus on prevention (Dupont et al., 2023). It is a comprehensive approach that combines organizational, technological, and human-centered components to produce a dynamic defense approach. This is attained by taking into account the interconnected hardware, software, and sensing components of cyberinfrastructure(Linkov, 2018). Based on known features of a system or network, the probability of a successful cyberattack can be empirically assessed and estimated suitably and accurately to some extent (Leslie et al., 2017). Assessment techniques are being developed for the cyber impact on a system (Kott et al., 2015). Current efforts evolve beyond quantifying risk in particular units (like the probability of failure) and towards risk-based decision-making using multi-criteria decision analysis because cyber threats are difficult to quantify (Ganin et al., 2016). The questions of how well a system can withstand a cyberattack and how quickly and fully it can recover from one are not addressed by the concept of risk, in contrast to the concept of resilience. There is always a residual risk even after hazards are recognized and mitigation measures are implemented. Therefore, part of the goal of resilience assessment and management is to address that residual known risk that has not been mitigated and to improve the system's overall capacity to respond to new or emerging threats.

In addition, robustness which refers to the ability of a system to tolerate unforeseen internal or external threats or changes without experiencing a decline in its functionality is another idea that is frequently misinterpreted with resilience(Liu et al., 2022).According to Bodeau et al., (2015), it is the degree to which a system performs as intended in the face of unusual inputs or demanding external conditions. The degree of damage usually determines how long recovery takes.There might also be a limit that recovery cannot occur past. Specifically, there is a relationship between resiliency which determines how quickly the system can recover from such damage, and robustness, whichevaluates how much damage is incurred in response to an unexpected disturbance. Therefore, a system with insufficient robustness will frequently fail past the point of recovery, providing minimal resilience.

Tariq et al., (2023),suggested that identifying and hardening the crucial system components that are most susceptible to failure is a crucial risk management approach. This strategy may be suitable for several isolated cyber systems; however, as previously mentioned, when the nature of the threat is unknown, it can be challenging to pinpoint all the vital parts and more costly to take precautionary measures to fortify or shield the entire system from threats (Ibrahim Kure & Islam, 2019). This therefore implies that as the world is becoming less and less isolated, it can be challenging to define and measure the extent of interdependency and interconnectedness, even while there is stagnation in investment and infrastructure, and societal systems are left largely unprepared for new and uncertain threats as risk mitigation plans become expensive and take longer to complete while seeking for funding.

III. Cybersecurity and Applications

Technology has advanced significantly over time, so numerous studies have been conducted on cybersecurity to better understand the problem and even provide an explanation of how it can be resolved.There are three categories of cyber threats, which make it easier to decide what security precautions to take and how best to respond. First, there is cyberterrorism, which has received more attention. It seeks to instill in the general public a fear of technology and panic (Weimann, 2014). It is employed by radicals who oppose technological advancements by using terror and panic to sabotage the smooth operation of society. Cyberattacks are primarily focused on political targets and the dissemination of private information. Finally, there is cybercrime, which targets different systems and is motivated by monetary gain and disruptions (Ablon, 2018). Although there are already some cyber threats that always emerge as technology develops(NIST, 2020).Every technological advancement is accompanied by changes in cyber threats.Cyber threats that are frequently encountered include ransomware, malware, and phishing.Since most security measures also call for physical cases to be installed in the devices or buildings where the information is being keyed in, such attacks require planning.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

Phishing also includes the use of fraud, in which fraudsters send phony emails to obtain the information they require (Abdullahi et al., 2022).In this regard, the emails sent to the victims as a bait and switch resemble emails from reputable sources. Once the attackers have the stolen data, they can use it for financial fraud or identity theft, among other nefarious activities. Phishing attacks are a serious risk to people and businesses alike, which is why it's critical to identify telltale signs of phishing, like suspicious email requests or strange website URLs, so as to safeguard entities and prevent scams (Hussain et al., 2020).The term "ransomware" refers to the demand made for a ransom once the attacker gains access to data or system files. The process of introducing malware into a computer system is known as ransomware (Kennedy, 2017). Malware is the introduction of malicious software that either corrupts system files or allows access to the data they contain. Cybercriminals insert viruses or malicious software using a structured language query to obtain information. A malicious SQL statement is submitted by SQL, granting criminals access to the targeted database. There are more, such as denial-of-service attacks and man-in-the-middle attacks. A clearer picture of the potential danger of cyberattacks can be obtained by reviewing previous examples. The US Department of Justice charged a leader of an organized cybercrime unit in December 2019 with being responsible for the Dridex malware attack. The malware impacted infrastructure, the general public, and the government globally.

The thing about malware and the current level of connectivity is that it allows attackers to impact numerous users at once. Threats known as "zero-days," or attacks that surface without recognizable digital signatures, are on the rise right now (Al-Rushdan et al., 2019). Experts heavily rely on the digital signature that the hacker left behind after an attack to triangulate and obtain information about the hacker. It is difficult to defend against a threat if its digital signature cannot be detected. Notably, they triangulate and verify the vulnerabilities the hacker used in cases of existing threats when addressing cyber threats and improving cybersecurity. The usage of digital signatures clarifies the hackers' method of gaining access to the system files or network. They can now work on stopping these attacks by improving the security of the systems and eliminating any vulnerabilities found in the data. Hackers or even people wishing to harm the organization can launch cyberattacks. Even those that we have never suspected may be among them. Given that they are aware of the security applications and protocols in place in these situations, the issue becomes crucial. To prevent such attacks, security measures should be very strong and legitimate. Regretfully, risk management is implemented with an override for each safety measure. As a result, cybersecurity is relevant to so many different economic sectors, it is broken down into distinct sections. The following are the various components of cybersecurity:

Data Protection

Li & Liu (2021) revealed that it encompasses various departments and sectors within each context, which makes it simple to cover using the set of distinct divisions. One essential component in the world of technology is information. Every gadget purchased and every piece of technology used requires the provision of a certain amount of data. Sometimes the information is just the standard operating procedure; other times, it includes personal data that can be used to identify the product's owner. In these situations, it is important to store data securely to prevent it from falling into the wrong hands. This is where cybersecurity becomes crucial.

Security of Networks

Network security pertains to safeguarding the internet network, encompassing computer, phone, and other device usage. Network security does not exclude authorized users from accessing the device; malware, on the other hand, can corrupt or erase data (Alawida et al., 2022). The protection of the network infrastructure pertains to network security. Various cybersecurity measures fall under network security. There are many ways that network security can be compromised, and understanding this helps mitigate the resulting outcomes. denial-of-service A denial-of-service attack is a kind of cyberattack in which a perpetrator purposefully floods a network, server, or website with excessive traffic or data so as to deplete its resources and prevent users from accessing it (Conti et al., 2018). A denial-of-service attack aims to interfere with the target system or network's regular operation, resulting in malfunctions or outages (Schmittner & Macher, 2019). DoS attacks can be carried out in some ways, including flooding the target with a large number of network requests, taking advantage of holes in the target's infrastructure or software, or using botnets; networks of compromised computers to flood the target with traffic coming from several sources (Trautman & Ormerod, 2018). Organizations should have a clear incident response strategy in place to handle denial-of-service-related attacks. This strategy should make it easier to move quickly to lessen the impact of the attack and reduce possible harm (Afenyo& Caesar, 2023). Procedures for isolating impacted systems, promptly informing pertinent parties, and working with law enforcement agencies if required are possible essential elements (Alghazo et al., 2017).

Application Security

It is evident that different applications are used on a variety of devices for different purposes. In order for the apps to function and recognize the user, the personal information of the user must be provided. Certain apps demand more factual information than others and are therefore more critical than others. For example, certain keys are needed for apps that are linked to banks because the data is vital. For this reason, it is imperative that users make sure they have installed the appropriate security measures for the different apps (Thames & Schaefer, 2017). In the past, some hackers have depended on the applications installed on their intended targets' devices to obtain the data they require in order to take advantage of them. Usually, it offers security protocols for these programs even before they are made widely available (Li & Liu, 2021). Therefore, due to the diversity of cybersecurity, each component must be addressed to the best of its ability even as individuals deal with these kinds of threats, especially in light of the rapidly expanding Internet of Things.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

IV. Strategies to Reduce Cybersecurity Risks

4.1 Establishing Intrusion Detection Systems and Firewalls

A firewall is a type of network security device that monitors all incoming and outgoing network traffic and decides which traffic to allow or block based on security rules that have been predefined. Businesses can protect sensitive data by separating their internal network from the public internet by using firewalls (Haitham Nobanee et al., 2023). Organizations should install intrusion detection systems (IDS) in addition to firewalls. IDS monitors network traffic for suspicious and malicious activity, identifying anomalies and possible security breaches. When an intrusion is discovered, IDS notifies system administrators or security personnel, allowing for prompt action (Bokan & Santos, 2021). Together, firewalls and intrusion detection systems (IDS) can detect and stop possible threats, adding another line of defense against online attacks. Organizations can dramatically lower the risk of cybersecurity threats by limiting network access and taking appropriate action in the event of suspicious activity (Faruk et al., 2022). For complete cybersecurity, though, installing firewalls and intrusion detection systems by themselves is not enough. Additionally, businesses should implement a multi-layered security strategy that includes data backups, software patches, employee training, encryption for sensitive data, and strong passwords (Jang-Jaccard & Nepal, 2019). Thus, organizations can greatly reduce their susceptibility to cybersecurity threats by implementing a multi-layered security approach, integrating firewalls and intrusion detection systems.

4.2 Consistent Software Updates

Regular software and security patch updates are among the best ways to reduce cybersecurity threats. Software developers make sure users have the most recent security measures in place by releasing updates to fix bugs and vulnerabilities that hackers might exploit (Housen-Couriel, 2015). Cybercriminals are always changing their methods and strategies as they search for holes in widely used software, operating systems, and plugins to exploit. Users who don't update their software are more susceptible to new threats, but regular updates keep you ahead of hackers and plug security holes (Jang-Jaccard & Nepal, 2019). Frequent software upgrades prevent system failures and data loss brought on by outdated or incompatible software by fixing bugs, addressing security flaws, and enhancing system performance(Ma & McKinnon, 2020). The software can be easily updated via manual software settings checks or automatic updates. To guarantee that the software is always up to date without requiring active user involvement, it is advised to enable automatic updates (Samtani et al., 2019). It is essential to update the operating system, web browsers, antivirus software, and other apps regularly in addition to software updates. Users who disregard these updates are at risk of known security vulnerabilities that have already been fixed by developers (Thomasian&Adashi, 2021).

4.3 Planning for Incident Response

An organization's approach to handling cybersecurity issues is regarded as an incident response plan (Dave et al., 2023). This entails locating, containing, and assessing the incident's extent through investigation. The plan also directs the proper courses of action, including data recovery, alerting pertinent parties, and putting safety measures in place to stop similar incidents in the future (Babate et al., 2015). Organizations may minimize the impact of cybersecurity breaches and stop additional harm by responding quickly and effectively to these events when they have a well-developed incident response plan in place. Clear guidelines for responding to various incident types should be provided, along with an explanation of roles, responsibilities, and communication channels. To keep a plan effective, testing and updates must be done regularly (Trautman & Ormerod, 2018).

V. Strategies for Enhancing Cyber Resilience

A variety of variables affect thenetwork of a system or organization's resilience in a complicated and frequently contradictory way(Linkov, 2018). A few of these variables and how to utilize or manage them to increase resilience arefurther explored and a description of a set of frameworks, technologies, and analytical techniques by Bodeau&Graubart (2016) can be employed to enhance the cyber resilience of systems and missions.

According to Qi & Mei (2024), the resilience of a system or network is largely determined by the complexity of its links. In this regard, highly complex links may potentially result in interactions that the system's designer is unable to predict or prevent, which causes catastrophic system failures. Hidden pathways, which are difficult for the designer to understand due to the large number of diverse, often implicit links, can circumvent a system's resilience measures. Kott & Abdelzaher (2016) argued that this problem is especially significant in multi-genre networks, which are networks that integrate multiple genres, such as social and cognitive networks, networks of physical resources, communication networks, and information networks. The paths connecting the network's elements are far more complex when considering a complete multi-genre network rather than just one of its heterogeneous, single-genre sub-networks. However, increased network complexity can also result in a decrease in the network's resilience. For instance, active agents might be more susceptible to unexpected side effects brought on by hidden paths within the network, or they might be discouraged in their restoration efforts due to the network's intricacy (Linkov, 2018). By increasing the number of ways that a failed component may contribute to the failure of another, and by concealing this fact from the developer, complexity may also result in lower resilience. Therefore, unless it directly supports resilience functions, more complicated structures should generally be avoided whenever possible.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

Additionally, Li & Liu, (2021) suggested that systems should be designed for reversibility such that when a system component fails or is compromised, it should be designed so that it can return to a safe mode. This indicates that to recover the system, the failed component, other system components, or the environment must not be damaged,and it must allow the component to be reversed back to its original state. This is becausecertain features set it apart from strictly logical systems (like databases), where rollback from failure is more practical and less expensive. However, traditional fail-safe design techniques might not be compatible with the requirement that the system absorb failure, which could reduce resilience. For instance, a system administrator discovers that malware has infected a system. Disconnecting the system might be a sensible fail-safe measure. However, if the computer is required to support other components that carry out damage-absorbing actions, this could be harmful to the system's overall resilience.

Furthermore, transmission should be regulated in a way that the system developer should take precautions against cascading failures to improve the system's capacity to withstand the effects of a cyberattack. Since each of these failures is not independent (Riggs et al., 2023). Large "domino effect" networks are likely to suffer significant damage in response to even small disturbances, which severely restricts the range of situations in which resilient operation and effective absorption and recovery are still feasible.

VI. Policy Regulation in the Digital Environment

Despite the swiftly evolving digital landscape, enterprises encounter a confluence of obstacles and prospects when it comes to fulfilling regulatory obligations. Since regulations must adapt to new technologies and cyber threats, the regulatory landscape is constantly changing. Keeping up with these changes and guaranteeing adherence to an ever-growing list of requirements present a challenge for organizations. The stakes for organizations protecting sensitive data are higher due to the proliferation of data and the rise in cyber threats.Adherence to data protection laws becomes crucial, necessitating strong cybersecurity defenses and privacy-focused procedures (Milch et al., 2019).

Regulations are often failing to keep up with digital innovations. Research can flourish in this dynamic tension between innovation and regulation, particularly in fields where digital technologies have significant societal ramifications. Firstly, organizations can anticipate potential regulatory roadblocks by identifying areas where policy was unable to maintain technological advancements. Additionally, it can help legislators concentrate their efforts (Cohent&Sundararajantt, 2019). Furthermore, it can be difficult to strike a balance between encouraging innovation and guaranteeing the welfare of society. Comprehending the dynamic between digital innovations and the legal structure will be essential to creating a more balanced and favourable atmosphere for new ideas to thrive.

VII. Conclusion

This study has explored the complex landscape of technological innovation in safeguarding information to create a safe and resilient cyber landscape.Through a review of fundamental concepts like cybersecurity, a range of applications, risk mitigation techniques, and the need for resilience,a thorough overview of the opportunities and challenges present in the modern digital landscape have been compiled. One particularly important foundational pillar in strengthening cybersecurity protection is the evolution of technological innovation. Technological developments are a driving force behind the continuous fight against cyber threats. Consequently, emerging technologies are driving global digital transformation while raising cybersecurity risks for companies going through it.

The study also emphasizes that the process of advancing technological innovation necessitates an understanding of emerging technologies and the security risks they pose. Therefore, users must make sure the right safeguards are in place to protect data and networks from malicious activity and unauthorized access as they shift their core operations to IT solutions.The findings indicate the importance of regulatory frameworks in establishing standardsensuring adherence, and creating an environment that is favourable to innovation and cybersecurity. In addition, it requires much more than technology to advance technological innovation for a resilient cybersecurity environment;it also requires a comprehensive approach that includes strategic planning,and dedication to adapting to the changing threat landscape.

References

1. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. Electronics, 11(2), 198. https://doi.org/10.3390/electronics11020198
2. Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. Results in Control and Optimization, 12(1), 100268. https://doi.org/10.1016/j.rico.2023.100268
3. Abion, L., Libicki, M. C., & Golay, A. A. (2014). M Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar. Apps.dtic.mil; RAND CORP ARLINGTON VA NATIONAL SECURITY RESEARCH DIV. https://apps.dtic.mil/sti/citations/ADA603661
4. Ablon, L. (2018). The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf
5. Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

6. Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2020). Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. Annals of Operations Research, 308(1). https://link.springer.com/article/10.1007/s10479-020-03620-w
7. Al-athwari, B., & Azam, H. M. (2020). Resource allocation in the integration of IoT, Fog, and Cloud computing: state-of-the-art and open challenges. In: International Conference on Smart Computing and Cyber Security: Strategic Foresight, Security Challenges and Innovation, Springer, Cham, 247–257.
8. Al-Rushdan, H., Shurman, M., Alnabelsi, S. H., & Althebyan, Q. (2019). Zero-Day Attack Detection and Prevention in Software-Defined Networks. 2019 International Arab Conference on Information Technology (ACIT). https://doi.org/10.1109/acit47987.2019.8991124
9. Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003
10. Alghazo, J. M., Kazmi, Z., & Latif, G. (2017, November 1). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. IEEE Xplore. https://doi.org/10.1109/ICETAS.2017.8277910
11. Alrumaih, T. N. I., Alenazi, M. J. F., Al Sowaygh, N. A., Humayed, A. A., & Alablani, I. A. (2023). Cyber resilience in industrial networks: A state of the art, challenges, and future directions. Journal of King Saud University - Computer and Information Sciences, 35(9), 101781. https://doi.org/10.1016/j.jksuci.2023.101781
12. Appiah, G., Amankwah-Amoah, J., & Lui, Y.-L. (2020). Organizational Architecture, Resilience, and Cyberattacks. IEEE Transactions on Engineering Management, 1–16. https://doi.org/10.1109/tem.2020.3004610
13. Babate, A., Musa, M., Kida, A., &Saidu, M. (2015). State of cyber security: Emerging trends landscape. " International Journal of Advanced Research in Computer Science & Technology, 3(1), 113–119. https://www.academia.edu/11947469/state_of_cyber_security_Emerging_trends_landscape
14. Bodeau, D., &Graubart, R. (2016). Cyber Resilience Metrics: Key Observations Cyber Resilience Metrics: Key Observations Cyber Resilience Metrics: Key Observations Cyber Resilience Metrics: Key Observations. https://apps.dtic.mil/sti/trecms/pdf/AD1107819.pdf
15. Bodeau, D., Graubart, R., Heinbockel, W., Laderman, E., & Bedford, M. (2015). Cyber Resiliency Engineering Aid - The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques. https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf
16. Bokan, B., & Santos, J. (2021, April 1). Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures. IEEE Xplore. https://doi.org/10.1109/SIEDS52267.2021.9483736
17. Cohent, M., & Sundararajantt, A. (2019). Self-Regulation and Innovation in the Peer-to-Peer Sharing Economy. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1039&context=uclrev_online
18. Connelly, E. B., Allen, C. R., Hatfield, K., Palma-Oliveira, J. M., Woods, D. D., &Linkov, I. (2017). Features of resilience. Environment Systems and Decisions, 37(1), 46–50. https://doi.org/10.1007/s10669-017-9634-9
19. Conti, M., Dargahi, T., &Dehghantanha, A. (2018). Cyber Threat Intelligence: Challenges and Opportunities. Advances in Information Security, 70, 1–6. https://doi.org/10.1007/978-3-319-73951-9_1
20. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., &Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3). https://doi.org/10.1057/s41288-022-00266-6
21. Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., &Khut, D. (2023). The New Frontier of Cybersecurity: Emerging Threats and Innovations. https://arxiv.org/ftp/arxiv/papers/2311/2311.02630.pdf
22. Department of Justice . (2019). https://www.justice.gov/opa/pr/russian-national-charged-dec%20ade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.%20Accessed%20Dec%202020
23. Distor, C. B., Inês Campos Ruas, TupokigweIsagah, &Soumaya Ben Dhaou. (2023). Emerging technologies in Africa: Artificial Intelligence, Blockchain, and Internet of Things applications and way forward. https://doi.org/10.1145/3614321.3614326
24. Dupont, B., Shearing, C., Bernier, M., &Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. Computers & Security, 132, 103372. https://doi.org/10.1016/j.cose.2023.103372
25. Faruk, M. J. H., Tahora, S., Tasnim, M., Shahriar, H., &Sakib, N. (2022). A review of quantum cybersecurity: threats, risks and opportunities. In 1st International Conference on AI in Cybersecurity (ICAIC).
26. Ganin, A. A., Massaro, E., Gutfraind, A., Steen, N., Keisler, J. M., Kott, A., Mangoubi, R., &Linkov, I. (2016). Operational resilience: concepts, design and analysis. Scientific Reports, 6(1), 1–12. https://doi.org/10.1038/srep19540
27. Gould, D. (2018). Organizational Resilience Approaches to Cyber Security. International Journal of Smart Education and Urban Society, 9(4), 53–62. https://doi.org/10.4018/ijseus.2018100105
28. Haitham Nobanee, Ahmad Yuosef Alodat, Reem Bajodah, Al-Ali, M., & Alyazia Al Darmaki. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. Journal of Financial Crime. https://doi.org/10.1108/jfc-11-2022-0287
29. Housen-Couriel, D. (2015). "Cybersecurity and anti-satellite capabilities (asat) new threats and new legal responses. Journal of Law & Cyber Warfare, 4(3), 116–149.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

30. Hussain, A., Mohamed, A., & Razali, S. (2020). A Review on Cybersecurity. Proceedings of the 3rd International Conference on Networking, Information Systems & Security. https://doi.org/10.1145/3386723.3387847
31. Ibrahim Kure, H., & Islam, S. (2019). An Assets Focus Risk Management Framework for Critical Infrastructure Cyber Security Risk Management. IET Cyber-Physical Systems: Theory & Applications, 4(4). https://doi.org/10.1049/iet-cps.2018.5079
32. Jang-Jaccard, J., & Nepal, S. (2019). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. Sciencedirect. https://doi.org/10.1016/j.jcss.2014.02.005
33. Kaur, R., Gabrijelčič, D., &Klobučar, T. (2023). Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. Information Fusion, 97, 101804. sciencedirect. https://doi.org/10.1016/j.inffus.2023.101804
34. Kennedy, C. (2017). New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles. Michigan Telecommunications and Technology Law Review, 23(2), 343–356.
35. Kott, A., &Abdelzaher, T. (2014). Resiliency and robustness of complex systems and networks. Adaptive Dynamic and Resilient Systems, 67, 67–86.
36. Kott, A., &Abdelzaher, T. F. (2016). Resiliency and Robustness of Complex, Multi-Genre Networks. ArXiv (Cornell University).
37. Kott, A., Alberts, D. S., & Wang, C. (2015). Will Cybersecurity Dictate the Outcome of Future Wars? Computer, 48(12), 98–101. https://doi.org/10.1109/mc.2015.359
38. Leslie, N. O., Harang, R. E., Knachel, L. P., & Kott, A. (2017). Statistical models for the number of successful cyber intrusions. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 15(1), 49–63. https://doi.org/10.1177/1548512917715342
39. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. Energy Reports, 7(7), 8176–8186. Sciencedirect. https://doi.org/10.1016/j.egyr.2021.08.126
40. Linkov, I. (2018). Fundamental Concepts of Cyber Resilience: Introduction and Overview Motivation: Why Cyber Resilience? Springer. https://arxiv.org/pdf/1806.02852.pdf
41. Liu, X., Li, D., Ma, M., Szymanski, B. K., Stanley, H. E., & Gao, J. (2022). Network resilience. Physics Reports, 971, 1–108. https://doi.org/10.1016/j.physrep.2022.04.002
42. Ma, K., & McKinnon, T. (2020). COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic. SSRN Electronic Journal, 29(2). https://doi.org/10.2139/ssrn.3718845
43. Milch, R. S., Pernice, I., Romanosky, S., von Lewinski, K., Shackelford, S. J., Rosenzweig, P., Christakis, T., Swire, P., Healey, J., Herpig, S., Pohle, J., Zatko, S., & Wenger, E. (2019). Building Common Approaches for Cybersecurity and Privacy in a Globalized World. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3508933
44. Mohamed, K. S. (2019). IoT Physical Layer: Sensors, Actuators, Controllers and Programming. The Era of Internet of Things. https://www.semanticscholar.org/paper/IoT-Physical-Layer%3A-Sensors%2C-Actuators%2C-Controllers-Mohamed/118dcef9e64e0185e5227f094bac13a1f199070c
45. Mufti, T., Saleem, N., &Sohail, S. (2020). Blockchain: A detailed survey to explore innovative implementation of disruptive technology. EAI Endorsed Transactions on Smart Cities, 4(10), 164858. https://doi.org/10.4108/eai.13-7-2018.164858
46. NIST. (2020). social engineering - Glossary | CSRC. Csrc.nist.gov. https://csrc.nist.gov/glossary/term/social_engineering
47. Perera, S., Jin, X., Maurushat, A., & Opoku, D.-G. J. (2022). Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. Informatics, 9(1), 28. https://doi.org/10.3390/informatics9010028
48. Qi, X., & Mei, G. (2024). Network Resilience: Definitions, approaches, and applications. Journal of King Saud University - Computer and Information Sciences, 36(1), 101882–101882. https://doi.org/10.1016/j.jksuci.2023.101882
49. Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors, 23(8), 4060. https://doi.org/10.3390/s23084060
50. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., &Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors, 23(15). https://doi.org/10.3390/s23156666
51. Safitra, M. F., Lubis, M., &Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. Sustainability, 15(18), 13369. https://doi.org/10.3390/su151813369
52. Samtani, S., Abate, M., Benjamin, V., & Li, W. (2019). Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1–20. https://doi.org/10.1007/978-3-319-90307-1_8-1
53. Sanskriti , J. (2022, December 19). 160 Cybersecurity Statistics: Updated Report 2024. Astra IT, Inc. https://www.getastra.com/blog/security-audit/cyber-security-statistics/#:~:text=160%20Cybersecurity%20Statistics%202024%20%5BUpdated%5D&text=Cybersecurity%20statistics%20indicate%20that%20there

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIII, Issue IV, April 2024

54. Schmittner, C., &Macher, G. (2019). Automotive Cybersecurity Standards - Relation and Overview (A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, & F. Bitsch, Eds.). Springer Link; Springer International Publishing. https://doi.org/10.1007/978-3-030-26250-1_12
55. Smith, Z., Lostri, E., & Lewis, J. (2020). The Hidden Costs of Cybercrime. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.
56. Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A critical cybersecurity analysis and future research directions for the internet of things: A comprehensive review. Sensors, 23(8). https://doi.org/10.3390/s23084117
57. Thames, L., & Schaefer, D. (2017). an overview of key benefits, technologies, and challenges. In: Cybersecurity for Industry 4.0. In L. Thames & D. Schaefer (Eds.), Springer Series in Advanced Manufacturing. Springer International Publishing. https://doi.org/10.1007/978-3-319-50660-9
58. Thomasian, N. M., & Adashi, E. Y. (2021). Cybersecurity in the Internet of medical things. Health Policy Technology, 10(3).
59. Trautman, L. J., & Ormerod, P. (2018). Wannacry, Ransomware, and the Emerging Threat to Corporations. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3238293
60. Weimann, G. (2014). Cyberterrorism: How Real Is the Threat? United States Institute of Peace. https://www.usip.org/sites/default/files/sr119.pdf

Biographies of the Authors

1. **Muritala Aminu** is an experienced DevOps and infrastructure specialist with a focus on DevSecOps and Site Reliability Engineering (SRE). His career spans various roles where he has demonstrated proficiency in driving digital transformation and enhancing software delivery processes.With expertise in cloud architecture, Kubernetes orchestration, Linux system administration, and cybersecurity protocols, Muritala brings a comprehensive skill set to his work. His commitment to continuous improvement and collaboration makes him a valuable asset in any team. Additionally, his educational background includes a Master of Science in Information Technology, a Bachelor of Science in Physics, and an HND in Electrical and Electronics Engineering.

2. **Sunday Anawansedo** is a seasoned expert in cybersecurity and telecommunications, specializing in driving technological innovation for a resilient cybersecurity landscape. He earned his Master's degree in Electrical Engineering from the Southern University of Agriculture and Mechanical College, where he honed his skills and knowledge in cutting-edge technologies. With over 10 years of hands-on experience in the field, Sunday has established himself as a prominent figure, contributing significantly to the advancement of cybersecurity solutions.

3. **Yusuf Ademola Sodiq**, is a Master's student at the prestigious University of Salford, Manchester, UK, specializing in Cyber Security Threat Intelligence and Forensics. With a rich tapestry of experience spanning over 8 years in system administration, Yusuf seamlessly blends his profound academic pursuits with hands-on expertise.

4. **OladayoTosin Akinwande**is an Assistant lecturer in Software Engineering department of Veritas University, Abuja. He is currently pursuing his Ph.D in Computer Science specialising in Explainable Artificial Intelligence(XAI). He Holds a Master’s degree in Computer Science and Bachelor’s Degree in Computer Science, both from Federal University of Technology, Minna. He is an experienced, competent and well-trained researcher in the fields relating to computing with expertise in Machine Learning and Artificial Intelligence. He is a member of Nigeria Computer Society (NCS).