International Journal of Social, Humanities and Life Sciences ISSN XXXX-XXXX
Vol. 1, No. 2, December, 2024, pp. 37-46

Cybersecurity and Information Assurance: Bridging the Gap

Nahid Neoaz

Wilmington University, USA

nahidneoaz@yahoo.com

Abstract

Both cyber security and information assurance have been more or less intertwined especially in the current society where innovation and technology has remained the core business of most organizations in the global v`=y. While cybersecurity is the protection of systems, networks and data against possible attack, information assurance will ensure confidentiality, availability and integrity of information in an unending fashion. However in practice, they are the components of that security strategy and although getting them integrated can pose some conceptual challenges, the process involves technical, organizational and cultural dimensions. In this paper I'm going to explain the differences between these two fields and how do they match – to what extent they have to 'perfectly fit' each other for the sake of constant functional threat-protection and data dependability warfare. More specifically, it points out that applying the structural-mapped techniques such as NIST, ISO 27001 or COBIT can guide on how to structure the methodologies to address the gap. Also, technological advancements such as artificial intelligence, block chain and IoT security are presented as potential solution to cybersecurity and assurance. Nonetheless, human and culture aspects are considered relevant to integration in the process. This is because challenges; structural silos, disparities in goals and objectives and lack of expertise reduce the likelihood of synergy between cybersecurity and information assurance. The means of addressing these barriers are through training that involves cross training, growing interdependency, and increasing security through leadership and delegation responsibilities. This is due to the application of frameworks together with emerging technologies and people in formulating a strategy with elements of both tactical and strategic cybersecurity.

Key words: *information security, guard, InfoSec, risk management, internal control, control, NIST, ISO, COBIT, artificial intelligence, big change thoughts, IoT security, departments, organization cultures, staff/I&W, data availability, availability, compliance, managerial support, collaboration, likely risks, readiness, confidence.*

1. Introduction

Technology has evolved in the current generation and thus; cybersecurity and information assurance are identical. However, it must be understand and noted that it is two subfields in the larger information system area even though both of them focuses on the protection of data and the network systems. The major function of cybersecurity therefore is centered on the maintaining the security of network and computer systems against intruders with malicious intents [1]. On the other hand information assurance is all about the managerial, technical and operations that is bound to ensuring that, the information in the physical media, virtual media or both that has been processed, is available, whole and intact, and its origin authentic, at every stage of its processing and storage. Due to the improvement of the challenges towards the risk environment, cyber security and information assurance has become more important than ever before. After all, as organizations become digitally smart to adopt advanced solutions on cloud, IoT and Artificial Intelligence the threat to its information intensified [2]. That change has led to the emergence of the need for the expanded, or a more complex security concept system, which replaces the known security in the form of threat control through technical means (cybersecurity) with the protection and dependability of information (information assurance). Failure in proper facilitation of such nodes can transform an organization into vulnerability to such threats as well as internal diseconomies [3].

This is because, the current and the future cybersecurity and information assurance dynamics are in dynamism of changes to the regulatory and industry demands. The best practice frameworks such as ISO 27001, NIST Cyber Security Framework and COBiT state that technical control shall be underpinned by written assurance over compliance, risk and business continuity. This alignment

is key important in areas such as the health, banking and other sensitive industries because incidents and downtimes cost a lot of money, reputation and legalities [4]. Nevertheless, the cybersecurity and information assurance have different positions in organizations and may work separately. Where information security tends to be focused to the current threat and safeguard of the net perimeters, information assurance is on planning and system reliability in this timeframe. It is thus an organizational division that denies necessary synergy, equal resource distribution and policy formulation hence creating potential flaws in an organizations security strategies [5].

Solving this issue is a function of perspective transformation leading to cybersecurity as a subfield of information assurance. It also presupposes the assertion that reliable defense is impossible without the combination of current reactive countermeasures with the general security guarantees for the data and its availability. Thus the technical, the organizational and more specifically the cultural everyday practices can be brought in line and do assist an organization to be prepared for new threats whilst at the same maintain the reliability and the significance of IS [6]. The authors of this article have also addressed the implication for practice, pedagogy and for research in the conclusion section. The next section of this article will include comparison between how and when this integration has been done, the issues and the possibilities, the strategies, the cases and the prospects [7].

2. A Review and Contrast of Similar Ideas

Cybersecurity and Information assurance cannot be discussed without basic similarities between these two fields and yet, each has its share in the world of information security. It is in any case important that organizations concerned with the development of a consistent overall security concept will be acquainted with these similarities and differences.

Core Principles of Cybersecurity: Cyber security is predominantly described as the process of protecting systems, networks and data against cybercrimes such as hacking, viruses, phishing and ransom ware. As clearly mentioned above, it enjoys a number of benefits in its implementation, its main goal is information security protection against access by unauthorized persons, leakage or system failure. Cyber security data security measures are; firewalls, intrusion detection systems; end point protection; encryption programs among others [8]. These steps pay most attention to the protection of the DSP, responding to threats as they are currently unfolding and decreasing vulnerabilities. To date, cybersecurity is still a very broad area of practice because the playing field is ever-shifting due to the threats. There is always the new private entry point; there are always the new threats; and the bad guys are always up to something, so it is impossible to just sit back and watch. Readers familiar with how security specialists work as they protect infrastructure in cyberspace may have come across the principle of confidentiality where some data should not be revealed to the public [9].

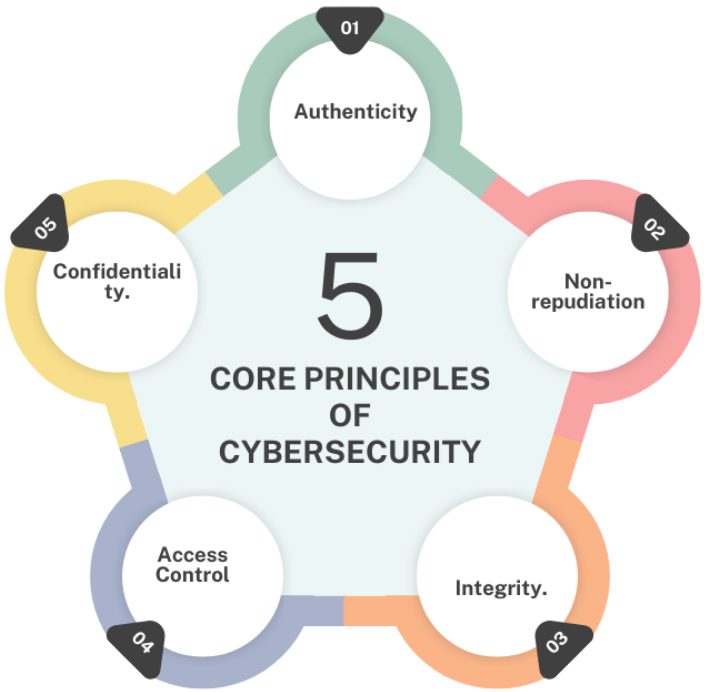

Figure: 1 showing core principles of cybersecurity

Core Principles of Information Assurance: Information assurance, on the other hand, is about the accessibility, and credibility of information from the time it is generated up to the time it is used. It proposes more general long-term objectives, which are data consistence, availability and believability, leading to the proposed solutions [10]. Where cybersecurity is about threat eradication at the first level, information assurance aims at protecting the data from outside threats and internal adversities, system failures, corrupted staff and policy breaches. Information assurance is therefore made up of risk management activity, compliance, checking, and disaster recovery. Concerns such as whether the organization can access core information when their system is offline, or whether the information inputting/outputting to the system is legally acceptable, are addressed by it. All these concerns place emphasis of massive on operational business continuity and organizational credibility [11].

Key Differences and Complementary Aspects: Thus the major difference between cybersecurity and information assurance can be identified based on the concentration areas and the endpoints. Cyber security is the functionality and for the most part - ad hoc, while information assurance is strategic, goal-oriented and comprises more than cyber threats [12]. However, there exist competition between these two fields but they are related in several ways. But when there is no cyber security then information assurance has no technical security measure in place to protect against the cartels. Conversely the lack of information assurance makes the cyber security efforts more of a short term drive and may for example lack objectives like the following: no conformance to standards, data file integrity, or insufficient disaster readiness structure [13]. This area of cybersecurity and information assurance presents such chances of enclosing the approaches and efforts towards information security. When Cyber Security is linked with Information Assurance concepts the organization is provided with both the technical competence and the vision of what is to come. Looking at such differences while utilizing the strength of both segments is the first line of action towards minimizing the existing gap between those two fields [14].

3. Challenges in Integration

When it comes to defining the connection between cybersecurity and information assurance there are several problems, which have social, organizational, as well as technical and cultural implications. All of these issues can make it nearly impossible to put sound security policies into place and to mitigate current and future threats.

Figure: 2 showing challenges of integration

Organizational Silos: One of the major causes of many business integration failures is lack of Information integration within organizations brought about by the formation of organizations silos. At the current rate one finds many organizations having cybersecurity and InfoSec teams that are nearly completely detached [15]. This kind of division leads to some issues that include; integration difficulties like duplication of work, existence of uncoordinated polices or in some extreme; no harmonized objectives whatsoever. For instance, cybersecurity staff can focus on swift response to cyber threats; information assurance groups target compliance and risk management that can work in opposition [16].

Differences in Goals and Metrics: This last problem arises when the overall objectives and measurements are less compatible within such two domains. It is usually done quantitatively — the collection of information pertaining to the effectiveness of some st(-)initiatives in preventing or limiting the rate or type of such-and-such a threat — for examples, the rate of attack and the rate of visibly apparent vulnerability that has been prevented [17]. Whereas, information assurance methodology is judged on even more general note such as availability, governance compliance and organizational readiness. KPI thus may be somewhat divergent and this may complicate questions of co-ordination and of goal setting, not to mention resources distribution [18].

Skill and Knowledge Gaps: Information assurance and cybersecurity also positively interfaces and both also require experts who have international knowledge in the two subspecialties. However, a significant number of organizations responding to the challenges of complex processes management do not have employees with interdisciplinary experience and knowledge. Some of the strategic risks and regulatory issues may not be well understood by information assurance professionals and currents threats and securities may be ill-understood by cybersecurity specialists [19]. This has made it hard to establish a connected team and develop a plan of action that a team shapes. However, time and efforts should be made on orientation specifically with reference to decoupling goal coordination and of which training was most significant across faculties. All these can be addressed by working together, benchmarking metrics that are familiar with all the teams and building teams that are highly differentiated in their respective specialties to assist in creating a support and development of the one stop security and information assurance stop shop [20].

4. Frameworks and Standards

CS and IA is a sister discipline and depends on the frameworks and standards of security currently in existence. These frameworks provide systematic guide/routine in establishing and setting standard that any organization can follow to manage their risks, compliance and safeguard their information & application assets [21]. Nevertheless, there is a special problem in the harmonization of these frameworks to meet goals and requirements related to cybersecurity and information assurance.

Cybersecurity Standards: The technical aspect of information protection is countered by such organizational controls standards as NIST Cybersecurity Frames, and ISO/IEC 27001. These above frameworks focus on the identification, prevention, alert, and recovery from the cyber threats. For example, NIST CSF is guided on the improvement and dynamic protection structure of an organization in order to address new generation threats [22]. Similarly, ISO/IEC is a set of guidelines for information protection, which contains a description of the risk identification factors and the measures for their mitigation. While these standards are fine for establishing ideal, precise templates to capture the nature of technical solutions and countermeasures to threat potential, they are weak for something like long-term data authenticity, business continuance in the face of incidents, and legal admissible evidence, which are elements of Information assurance [23].

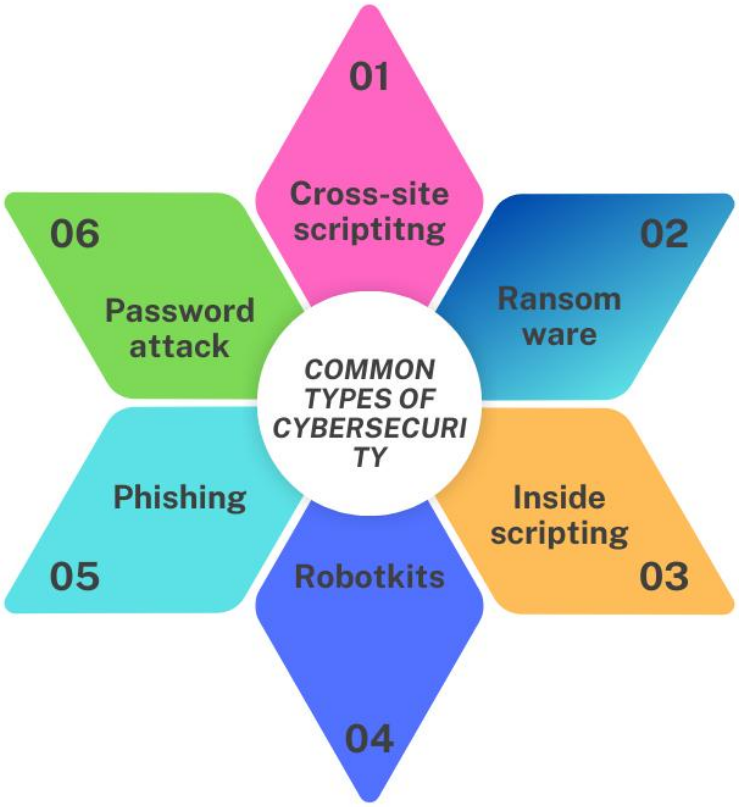

Figure: 3 showing types of cyber security

Information Assurance Frameworks: COBIT and ITIL, Information Technology Infrastructure Library information assurance frameworks focus on the governance, risk and control and processes. These frameworks aimed at assisting an organization in answering some affirmative questions such as whether its information systems support organizational goals and objectives, and whether or not they are stable, conforming to legal requirements and security [24]. For instance, COBIT has enshrine guidelines for linking IT processes to enterprise objectives, risk and compliance, on the other hand ITIL addresses issues pertaining to service quality, availability [25].

Toward Unified Approaches: For this reason only is it possible to combine these frameworks in order to (wage) fight in terms of cyber security threats while at the same time looking at strategic objectives. Efforts have been made recently to integrate the both the technological integration alongside with the operational ones with NIST RMF as well as the CMMC. Systems like these makes organizations better equipped to look for holistic strategies for security and resilience problems [26]. So, comparing two frameworks that describe cybersecurity and information assurance, it is possible to create a perspective on integrating cybersecurity and information assurance approaches to obtain the adequate and harmonized perspective of the security. It also enables them to manage risks and sustain operations and compliance that they will in the process earn gigantic returns [27].

5. Technological Intersections

The integration of both cybersecurity and information assurance is quite affected by the innovative technologies that provide connections between both fields. These technologies assist organizations in acquiring improved strategies for managing perpetual cyber threats and guaranteeing the validity and reliability of organizational information over time [28]. By means of these developments the general security drive of any organization can be improved, and actions in the sphere of cyber protection be aligned with the objectives discussed in the sphere of information protection [29].

Role of Artificial Intelligence and Machine Learning: The fields of AI and ML are applied in the approaches through which organizations can identify and mitigate cybersecurity threats. These technologies enhance means of automating threat detection, anomaly detection and response to incidents enhancing fight against cybercrimes [30]. However, AI and ML can enable information assurance to identify the unlawful usage of data, oversee the precision of the data before using it; and streamline the

compliance check procedure. For instance, it helps the applied systems of AI to check the honesty and genuineness of key information bids in real time, put into practice goals most connected with information assurance [31].

Block chain for Enhanced Assurance: Information assurance also has a very close relation with cybersecurity and one of the greatest links is block chain technology. Because of decentralized nature of the solution and because block-chain is fixed the solution provides certainty of authenticity, integrity and traceability implying that the data is protected. All these factors can be safeguarded by the block chain technology if they will be cached in supply chain, financial and/or digital identity data [32]. Taking into account security and reliability challenges block chain is the most vivid example of how implementing information technology align engulfs comprehending cyber security and information assurance [33].

Emerging Technologies and IoT Security: The prevalence of the 'Things' in the Internet network domain has populated new ideas in cybersecurity/ information assurance streams. On the same nut as the IoT devices for example, most of the devices are associated with many a times with better risks bearing in mind the poor security measures developed [34]. Nonetheless, the edge computing with further the so called secure by design approaches are good to reply to those challenges because both progress at the same time the security of the device and the data accurate. Therefore, technologies like the containerization and the micro services that characterize cloud-native are solutions for addressing massive volumes of data and prevention or assurance [35].

Challenges in Adoption: However, the application of these technologies has benefit which among them are; complexity, cost and skilled personnel. It also signifies a great need for organizations to scrutinize their technological spending on security and assurance against a new introduction of other risks [36]. By these technological corollaries, organizations can seamlessly integrate cybersecurity for information assurance with relation to the dynamic innovative systems and data systems to offer reliability, robustness [37].

6. Human and Cultural Factors

Information assurance and, in particular, cybersecurity as the specialized branch is usually regarded as the branch that relies on the technology most, while still, people and perceiving cultural factors are required to integrate the technological conditions into the real environment. It was not simply a security of technology problem, but a behavior, awareness, collaborative and culture problem. It is important for counteracting those factors for creating the proper and integrated concept of security provision [38].

Training and Awareness for Unified Practices: However, perhaps the most continuing problem area regarding cybersecurity and information assurance is the ignorant bliss employee. Most of the time, hackers attack are due to negligence by employees and these include: Schemes, wrong settings, and neglecting the rules of security. It is therefore important that workers do at least know enough about cybersecurity so that they are able to observe the short term measures and follow the long term assurance activities [39]. Training should therefore go beyond what constitutes cyber hygiene for example the next phase could be data integrity, data availability and compliance. He added further that Cybersecurity and information assurance are also cross-trained also since the two fields are very interrelated. When professionals from these fields are aware of the role and aim of the other, they can then work in unity towards achieving the abovementioned objective of offering a broad viewpoint security [40].

Behavioral Impacts on Security Practices: Roles and implication of Human behavior, consequently, remain central to the effectiveness or otherwise of any security initiatives. For example, the employees may for instance neglect to use the security controls that they deem pedestrian or confining [41]. Likewise, the corporate culture in an organization, which a number of authors stress has a strong influence on security practices, can also defeat security objectives: there may be the fear of change, lack of responsibility and so on. Leadership has to get involved in integrating security to the organizational culture for which leadership has to set good examples and practices good security measures, deserting employees who breach it while on the same note, all employees are supposed to talk about security standards an/or incidents [42].

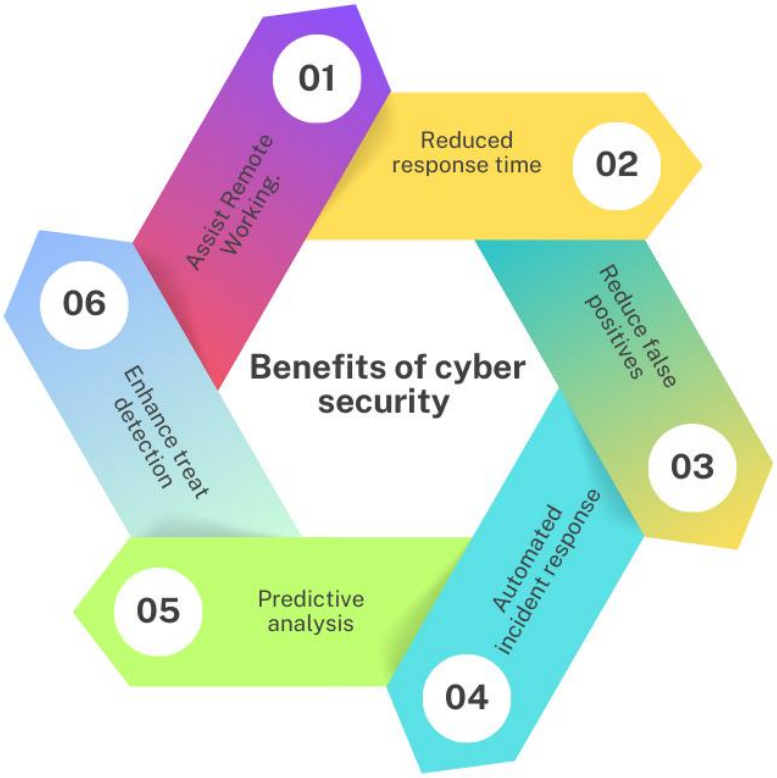

Figure: 4 showing benefits of cyber security

Overcoming Organizational Barriers: Due to the following cultural barriers in organizations, a room for disintegration of the cybersecurity and information assurance was created. These two domains are usually managed by two different departments – one operates with its own goals and objectives. On the other hand, to get over the mentioned silos, people should foster cooperation and have similar goals. This can be achieved by cooperation in formation of both disciplinary committees, formulation of mutual polices and indicators that represent both the goals in cybersecurity and assurance [43]. For example an organization may deem success as being realize not only in terms of the number of cyber-attacks averred in the organization, but also in instances where data access is improved or where there is deeper compliance established.

Leadership's Role in Bridging the Gap: People and culture represent the most important factors that leadership can either manage or cannot manage. The management systems of the top executive should find ways of integrating security in a company's organizational culture more specifically by employing resources for training purposes, purchasing support tools and participating in programs that address issues of corporate security and information assurance. Organizational leaders who set a positive perception are the ones who make their followers at any level of the organization adhere to the laid down security measures [44]. As the conceptual models presented inform, human and cultural factors are needed to bridge the divide between cybersecurity and information assurance. In Training, Collaboration Encouragement and Achieving Accountability form the unification platform to protect data and systems in organizations.

7. Conclusion

A clear distinction between cybersecurity and information assurance cannot be drawn up to date because they work hand in hand. Cybersecurity is aimed to prevent possible attacks to a system and networks where information assurance is dedicated to protecting data from degradation and unauthorized changes as time passes. In aggregate, these domains supply a sound and broad framework for security but, to overcome the gap between them, the considerations of both technology and organization are necessary. As elaborated in this discussion, the differences and similarities between cybersecurity and Information assurance stress on their interconnectedness. While cybersecurity focuses on bringing in the technical solutions needed to protect against the threats targeting the organization in immediate ways, information assurance provides a theoretical approach to protect against similar threats, avoid problems in compliance, and support data reliability. While the goals of these fields seem quite aligned, there are

numerous barriers to integration such as; lack of cooperation due to factors such as silos, commitment of different goals and objectives, and lack of cross-disciplinary proficiency.

Frameworks and standards have a large role to play in the link between cybersecurity and information assurance. Using guidelines I mentioned above NIST, ISO 27001, and COBIT used security technologies as well as the method for long-term data management and governance will be united. AI, block chain, and IoT security technological enhancements also facilitate this integration provide unique approaches to safeguard and handle data following the threat dynamics caused by increased innovation. But, technology can only go a long way. More so, the human and cultural factors have an important role in guaranteeing the success of these efforts. Attitude, knowledge, and perception should be cultivated to enable the collaboration between cyber-security and information assurance, de-soloing and cultivating for ownership. Leadership must first model the types of behaviors required, as well as provide the support that will foster on the creation of these alignment and interdisciplinary working. To close the gap between cybersecurity and IA, there is a need to have a detailed approach on technical solution, planning, and organizational culture. In the light of these dimensions, one can find a way on protecting organization's systems and data against both current and future cyber threats. In fact, this integrated approach can be regarded not only as a requirement for the developing modern enterprise but as the key to establishing the trust and sustainable business environment in the conditions of the digital world economy.

8. References

1. Steve Morgan, "Official Annual Cybercrime Report," Herjavec Group, 2023.
2. S. Redman, K. Yaxley and K. Joiner, " Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?" Creative Education, 2020.
3. S. T. Zubair, L. Saheed, O. I. Yusuf and A. M. Bello, "A review of artificial intelligence on the internet of things," International Journal of Research in Engineering, vol. 4, no. 1, pp. 8-12, 2022.
4. D. Mouheb, S. Abbas and M. Merabti, Cyberecurity Curriculum Design, Transactions on Edutainment, 2019.
5. T. Smith, A. Koohang and R. Behling, "Formulating an Effective Cybersecurity curriculum," Issues in Information Systems, vol. xi, pp. 410-416, 2010.
6. H. Santos, T. Pereira and I. Mendes, "Challenges and reflections in designing Cyber security curriculum," in IEEE World Engineering Education Conference (EDUNINE), Santos, Brazil, 2017.
7. Bicak, X. M. Liu and D. Murphy, "Cybersecurity curriculum development: Introducing specialties in a graduate program. Information Systems Education Journal," Information Systems Education Journal, vol. vol 13, pp. 99-110, 2015.
8. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI's Revolutionary Role in Cyber Defense and Social Engineering. *International Journal of Multidisciplinary Sciences and Arts*, *3*(4), 57-66.
9. J. Marquardson and A. Elnoshokaty, "Skills, Certifications, or Degrees: What Companies Demand for Entry-Level Cybersecurity Jobs," Information Systems Education Journal, vol. 18, no. 1, pp. 22-28, 2020.
10. K. J. Knapp, C. Maurer and M. Plachikinova, "Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance," Journal of Information Systems Education (JISE), vol. 28, pp. 101-114, 2017.
11. National Institute of Standards and Technology, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication, 2020.
12. International Organization for Standardization, "Information technology - Security techniques - Guidelines for cybersecurity education," 2012.
13. UNION, African Union Convention on Cyber Security and Personal Data Protection, Ethopia, 2021.
14. M. Erickson and P. Kim, "Designing cybersecurity curriculum: Exploring the need for industry certifications and experiential learning," International Association for Computer Information Systems, vol. 22, no. 4, pp. 9-20, 2021.
15. N. S. Clair and J. Girard, "Judging Competencies in Recent Cybersecurity Graduates," vol. 8, 2020.
16. J. K. Nelson and B. L. Donham, "Partnership to Prepare Students for Careers in the Emerging Field of Cybersecurity," in ASEE Virtual Annual Conference, 2020.
17. W. A. Conklin, R. E. Cline and T. Roosa, "Reengineering Cybersecurity Education in the US: An Analysis of the Critical Factors," in 47th Hawaii International Conference on System Science, 2014.
18. C. D. Ramirez and G. A. Rioux, "Advancing curricula development for homeland security education through a survey of DHS personnel," Journal of Homeland Security Education, vol. 6, 2012.
19. Beveridge, R. (2021) Addressing the Gender Gap in the Cybersecurity Workforce. International Journal of Cyber Research and Education, 3, 54-61. https://doi.org/10.4018/ijcre.2021070105

20. Radu, C. and Smaili, N. (2021) Board Gender Diversity and Corporate Response to Cyber Risk: Evidence from Cybersecurity Related Disclosure. Journal of Business Ethics, 177, 351-374. https://doi.org/10.1007/s10551-020-04717-9
21. Berríos, N. (2019) Increasing the Participation of Young Women in Cybersecurity. 1-12. http://hdl.handle.net/20.500.12475/311
22. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566-578.
23. Merayo, N. and Ayuso, A. (2022) Analysis of Barriers, Supports and Gender Gap in the Choice of STEM Studies in Secondary Education. International Journal of Technology and Design Education, 33, 1471-1498. https://doi.org/10.1007/s10798-022-09776-9
24. Moghaddam, Y., Kwan, S., Freund, L. and Russell, M.G. (2021) A Proposed Roadmap to Close the Gap between Undergraduate Education and STEM Employment across Industry Sectors. In:
25. Leitner, C., Ganz, W., Satterfield, D. and Bassano, C., Eds., Advances in the Human Side of Service Engineering. AHFE 2021. Lecture Notes in Networks and Systems, Vol. 266, Springer, Cham, 363-373. https://doi.org/10.1007/978-3-030-80840-2_42
26. Maraj, A., Sutherland, C. and Butler, W. (2021) Studying the Challenges and Factors Encouraging Girls in Cybersecurity: A Case Study. European Conference on Cyber Warfare and Security, 24-25 June 2021, 269-277.
27. Montañez, R., Golob, E. and Xu, S. (2020) Human Cognition through the Lens of Social Engineering Cyberattacks. Frontiers in Psychology, 11, Article 1755. https://doi.org/10.3389/fpsyg.2020.01755
28. Hunt, V., Prince, S., Dixon-Fyle, S. and Dolan, K. (2020) Diversity Wins: How Inclusion Matters. http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/1340/1/McKinsey%20Repo Y. Asiry DOI: 10.4236/jis.2024.151002 23 Journal of Information Security rt%20-%20Diversity-wins-How-inclusion-matters.pdf
29. Böhm, S., Linnyk, O., Kohl, J., Weber, T., Teetz, I., Bandurka, K. and Kersting, M. (2020) Analysing Gender Bias in IT Job Postings. Proceedings of the 2020 on Computers and People Research Conference, Nuremberg, 19-21 June 2020, 72-80. https://doi.org/10.1145/3378539.3393862
30. Turner, R. and M'manga, A. (2022) Requirements for a Platform That Improves the Number of Young Women Entering Cybersecurity. The 35th International BCS Human-Computer Interaction Conference, Keele, Staffordshire, 11-13 July 2022, 1-4. https://doi.org/10.14236/ewic/HCI2022.41
31. Kshetri, N., Chhetri, M. and Kshetri, N. (2022) Gender Asymmetry in Cybersecurity: Socioeconomic Causes and Consequences. Computer, 55, 72-77. https://doi.org/10.1109/mc.2021.3127992
32. Lyon, V. (2020) Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals. Ph.D. Thesis, Walden University, Minneapolis. https://search.proquest.com/openview/86d84d20c21827e82b25cc2a5261205d/1?pqorigsite=gscholar&cbl=18750&diss=y
33. El Arnaout, N., Chehab, R. F., Rafii, B. and Alameddine, M. (2019) Gender Equity in Planning, Development and Management of Human Resources for Health: A Scoping Review. Human Resources for Health, 17, Article No. 52. https://doi.org/10.1186/s12960-019-0391-3
34. Breese, J.L., Conforti, M. and Peslak, A. (2020) An Exploration of Gender Bias in Information Technology Job Advertisements. Issues in Information Systems, 21, 189-199. https://iacis.org/iis/2020/3_iis_2020_189-199
35. Gaucher, D., Friesen, J. and Kay, A.C. (2011) Evidence That Gendered Wording in Job Advertisements Exists and Sustains Gender Inequality. Journal of Personality and Social Psychology, 101, 109-128. https://doi.org/10.1037/a0022530
36. Son Hing, L.S., Sakr, N., Sorenson, J.B., Stamarski, C.S., Caniera, K. and Colaco, C. (2023) Gender Inequities in the Workplace: A Holistic Review of Organizational Processes and Practices. Human Resource Management Review, 33, Article ID: 100968. https://doi.org/10.1016/j.hrmr.2023.100968
37. McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Lillie, M. (2018). The effect of resilience and job stress on information security awareness. Information and Computer Security, 26(3), 277–289.
38. Moody, G. D., Galletta, D. F., & Lowry, P. B. (2014). When trust and distrust collide online: The engenderment and role of consumer ambivalence in online consumer behavior. Electronic Commerce Research and Applications, 13(4), 266–282.
39. Pervez, M. A. (2010). Impact of emotions on employee's job performance: An evidence from organizations of Pakistan. OIDA International Journal of Sustainable Development, 1(5), 11–16.

40. 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), 1189–1210.
41. Preacher, K. J., Rucker, D. D., & Hayes, A. F. (2007). Addressing moderated mediation hypotheses: Theory, methods, and prescriptions. Multivariate Behavioral Research, 42(1), 185–227.
42. Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations1. MIS Quarterly, 34(3), 487–502.
43. Snyman, D. P., Kruger, H., & Kearney, W. D. (2018). I shall, we shall, and all others will: paradoxical information security behaviour. Information and Computer Security, 26(3), 290–305.
44. Spanaki, K., Gürgüç, Z., Mulligan, C., & Lupu, E. (2019). Organizational cloud security and control: a proactive approach. Information Technology and People, 32(3), 516–537.