

Digital Agility: Assessing the Necessity of Data Literacy and Cybersecurity Training Across Non-Tech Sectors

Dr. Annapurna Sahoo^{1*} | Ms. Amisha Panda²

¹Assistant Professor of Commerce, Khallikote Unitary University, Berhampur.

²Student, Khallikote Unitary University, Berhampur.

*Corresponding Author: sahoannapurna2@gmail.com

Citation: Sahoo, A. (2026). Digital Agility: Assessing the Necessity of Data Literacy and Cybersecurity Training Across Non-Tech Sectors. *International Journal of Advanced Research in Commerce, Management & Social Science*, 09(02(II)), 115–120.

ABSTRACT

The tech industry's rapid advancements have emphasized the critical need for digital literacy and cybersecurity awareness, particularly among the workforce of non tech-sectors like healthcare, manufacturing and government. How fast an organisation adapts itself to the changing technological environment is termed Digital agility. Lack of data literacy among the employees of non tech sectors leads to slow growth and development. This study analyzes the critical essence of digital literacy and cybersecurity awareness in empowering individuals and enabling them to thrive in their workspace. The study focuses on digital literacy, cybersecurity education, and mentorship and community support. Digital literacy which equips employees with essential data literacy skills, AI skills, Machine learning, internet navigation, and understanding digital tools. Simultaneously the paper evaluates the role of cybersecurity education in mitigating risk related to AI driven and data driven threats among highly vulnerable non tech workforce. The study determines how mentorship and community support with a collaborative learning environment can encourage workforces to build confidence and address unique challenges. The study also highlights the broader impact of empowering the workforce of the non tech sectors including enhanced diversity, innovation, and equity. This research contributes to the fields of digital inclusion and cybersecurity by providing a deep analysis of replicable and scalable approaches to address systemic inequities. By equipping employees with the tools and knowledge to excel in the digital age, this study aligns with the broader goals of fostering workforce diversity and creating a more secure and inclusive tech ecosystem. This paper analyses how leveraging partnerships with tech companies, educational institutions, and community organizations and integrating accessible training programs, free resources, and hands-on workshops can bridge the digital divide.

Keywords: Digital Literacy, Cybersecurity Awareness, Tech Industry, Digital Inclusion, Cybersecurity Education, Workforce Diversity.

Introduction

The digital age encompasses both Knowledge Society 5.0 and Industry 5.0, a transformative period characterized by rapid technological progress and ubiquitous digital technologies (Henderikx and Stoffers, 2022; Phillips et al., 2017) which presents opportunities and challenges to both organizations and individuals (Hngoi et al., 2023). Industry 5.0, a human-centric extension of Industry 4.0 (Nousala and Metcalf, 2024), requires a workforce skilled in advanced digital technologies and a deep understanding of emerging technologies (Maddikunta et al., 2022). The modern economy will not reward routine manual or cognitive work, as it can be done through automation (Autor 2015; Goos, Manning, & Salomons, 2014). Rapid and accelerating digitization is likely to bring economic rather than environmental disruption, stemming from the fact that as computers get more powerful,

companies have less need for some kinds of workers (David H. Autor). Technological progress is going to leave behind some people, perhaps even a lot of people, as it races ahead (David H. Autor). The increasing number of internet use is also driving an upward trend for cybercrime on the internet. The National Cyber and Crypto Agency (BSSN) noted that during the Covid-19 pandemic, January 1 to April 12, 2020, cybercrime had reached 88,414,296 cases (Kompas.com 2020). As cybercrime increases, every organization must establish some policies to maintain and improve their information technology (Sumin, 2016). In today's hyper-connected digital landscape, businesses rely heavily on technology to operate efficiently and meet the demands of an ever-evolving market (Dawit Negussie Tolossa, 2023). However, this increased reliance on technology also exposes businesses to a growing number of cyber threats and security breaches. Cybercriminals continuously exploit vulnerabilities in systems and networks, putting sensitive data, financial assets, and even the reputation of companies at risk (Dawit Negussie Tolossa, 2023).

Literature review

Asa Romeo Asa , Johanna Pangeiko Nautwima , Helvi Nyete Johannes: Digital literacy has transformed from a basic technical skill to a complex, multifaceted competency which is critical for workforce readiness in the 21st century. The review also indicates that there remains a chronic and significant "digital skills gap" that is driven by an incessant pace of technological change and is increased by systematic barriers such as continuous digital divide and psychological barriers for individuals (Digital literacy for workforce Readiness: Bridging the skills Gap in 21st century DOI:10.18775/ijied.1849-7551-7020.2015.311.2001 URL: <https://doi.org/10.18775/ijied.1849-7551-7020.2015.311.2> <https://doi.org/10.18775/ijied.1849-7551-7020.2015.311.2>).

Dawit Negussie Tolossa : Cybersecurity awareness training for employees in business is not only essential but also highly effective in mitigating cyber risks. By equipping employees with the knowledge and skills to identify and respond to cyber threats, organizations can significantly reduce the likelihood of security incidents, data breaches, and reputational damage (Importance of cyber security awareness training for employees in business, <http://vidyajournal.org>).

Lee, J. J., & Meng, J. (2021): Skill sets and knowledge in cognitive analytics, data management, technology literacy, sense making skills for digital transformation and digital competencies in crisis management are desired and necessary (Digital competencies in communication management: a conceptual framework of readiness for industry 4.0 for communication professionals in the workplace. Journal of Communication Management, 25(4), 417-436 <https://doi.org/10.1108/JCOM-10-2020-0116>).

Mun Yah Zahiroh (2020): Although cybersecurity awareness does not have a significant effect, it positively correlates with Change Readiness in Digital Banking Employees who are aware of cybercrime will minimize the risk to the company's technology security, especially the banking business, which operationally must apply the principle of prudence because it is related to the management of very large third party funds belonging to the public (Cybersecurity Awareness and Digital Skills on Readiness For Change in Digital Banking, <http://dx.doi.org/10.31332/lifalah.v5i2.2271>)

Research Objective

The study aims to assess the critical requirement of digital literacy and cybersecurity awareness to empower individuals, enabling them to thrive in their workspace. To determine the essence of data literacy skills such as machine learning, AI skills, etc. It focuses on evaluating the role of cybersecurity education in mitigating risk related to AI driven and data driven threats among highly vulnerable non tech workforce. It focuses on how mentorship and community support with a collaborative learning environment can encourage workforces to build confidence and address unique challenges. It aims to highlight the broader impact of empowering the workforce of the non tech sectors including enhanced diversity, innovation, and equity.

Methodology

This study employed the literature review method where the existing literature is scrutinized around the major research question of digital literacy and cybersecurity awareness. The findings of the earlier research are examined for the identification of consistent and repetitive themes. A sequential literature search was made in the database of Google Scholar and Scribd. For smoother research, duplicate papers were manually excluded to derive authentic results. At this stage, we kept 26 papers. Further exclusion criteria were applied. Thus, only full-text items written in English were

selected, and in doing so, three papers were excluded (no full text available), and one other paper was excluded because it was not written in English, but in Spanish. Therefore, we investigated a total number of 22 papers.

Results and Key Findings

Consequences of the Skills Gap for Businesses

The digital skills gap is an economic issue and at the same time it has also negative impacts on industries and businesses (Falck, Heimisch, & Wiederhold, 2021; OECD, 2019). Businesses are facing difficulties in acquiring the right talent with sufficient digital skills. Consequently, various critical posts remain vacant for elongated periods resulting in heavy financial costs (Goos, Konings, & Rademakers, 2016). These digital talent gaps are having a direct effect on the innovations, as businesses could not create new digital products, services and models (Goos, Konings, & Rademakers, 2016). Moreover, the existing labor force's lack of digital competence challenges the adoption and use of new technologies, and in many cases, technological investments do not yield the expected returns (Attewell, 1994; Bresnahan, Brynjolfsson, & Hitt, 2002; Nautwima et al., 2025). Lack of sufficient digital skills consequently erode a firm's competitive position (Vial, 2019). Companies having slow digitization growth because of lack of appropriate skills will start losing revenue to digitally mature competitors, which ultimately affects a company's bottom line and sustainability in the marketplace (Vial, 2019).

Identifying the requirement of Digital Skills

Multiple academic studies and industry reports have identified a growing demand for both foundational and advanced digital skills (Bejaković & Mrnjavac, 2020; van Laar et al., 2017). Research by the World Economic Forum indicates that AI and machine learning, data analysis, and digital marketing are among the most sought-after skills by employers (World Economic Forum, 2023). Beyond these advanced competencies, there is also significant demand for proficiency in collaboration tools, cloud computing environments, and data visualization tools (Brynjolfsson & McAfee, 2014). These digital skills align with sector-specific needs: for instance, healthcare requires expertise in Electronic Health Records (EHR) and telemedicine, while advanced manufacturing calls for highly specialized skills in robotics and IoT (Brynjolfsson & McAfee, 2014). The increasing diversity in required digital skill areas presents challenges for implementing a one-size-fits-all approach to digital literacy programs (van Laar et al., 2020). Several of these skills are discussed below.

- **Information and Data Literacy**

This basic capability is more than just finding information; it also involves critical appraisal, analysis and synthesising of data in a systematic way (Covello, 2006; Dey, 2022; Metzger, 2007). Employees must be able to find out the credible sources of information which is away from biases, misinformation and caricatured information (Covello, 2006; Dey, 2022; Metzger, 2007). This will help in conducting authenticated market research analyzing and utilising data efficiently and ethically which could lead to strategic decision making (Mandinach & Gummer, 2016). It further requires what scholars term "data-driven thinking"—the ability of employees to interpret the meaning behind metrics and leverage that data to address business questions (Mandinach & Gummer, 2016). This competency is critical, as today's workforce must navigate and manage complex datasets effectively (Hatlevik & Christophersen, 2023). This is important because workers are required to manage complex data effectively (Hatlevik & Christophersen, 2023).

- **Communication and Collaboration**

In the current time, the workspaces are collaborating digitally, and communication skills through digital platform requires some more digital efficiency along with communication skills, effective teamwork and management is becoming increasingly sophisticated and require (e.g., Slack, Microsoft Teams, and Asana) to develop increasingly sophisticated abilities in digital communication (Heine, Krepf & König, 2023; Lee & Meng, 2021). This generates the foundational know-how of communication through various digital channels and social media platforms (e.g., formal email versus informal chat), maintaining a professional digital presence on sites like LinkedIn, and engaging successfully in video meetings (Heine, Krepf & König, 2023; Lee & Meng, 2021). This involves collaborating on projects and documents, accessing shared files, and being a productive member of distributed or remote teams, which have become essential in post-pandemic work settings (García-Peñalvo, 2021; Wang et al., 2021).

- **Digital Content Creation**

Digital content creation whether for marketing purposes or advertising is a basic skill requirement for employees nowadays which could involve clear edited contents.(Redecker, 2017). From making effective presentation slides to produce short videos and creative reports, effective and concise blog writing skills and social media vlog posting skills are the basic capability. (Scott, 2015). This competency also requires basic knowledge of intellectual property, requiring employees to properly attribute sources, that is, follow copyright law and use Creative Commons licenses when borrowing existing content into a new product (Revuelta-Domínguez et al., 2022).

- **Cybersecurity education in mitigating risk**

- **Role of Employees in Cybersecurity:** The data consistently emphasized that employees play an essential role in an organization's cybersecurity posture. They are often the first line of defense against cyber threats, but they can also unintentionally become a weak link, leading to data breaches and security incidents.
- **Impact of Cybersecurity Awareness Training:** The majority of the reviewed studies reported positive outcomes associated with cybersecurity awareness training. Organizations that implemented regular and comprehensive training programs experienced a noticeable decrease in security-related incidents, such as phishing attacks, malware infections, and data breaches.
- **Building a Cybersecurity-Conscious Culture:** The data emphasized that cybersecurity awareness training not only enhances employees' knowledge about cyber risks but also influences their attitudes and behavior towards security. Employees who received proper training were more likely to adopt secure practices, report potential security incidents, and be proactive in safeguarding sensitive information.

Mentorships and learning solutions

- **The Role of Educational Institutions**

The most effective approaches extend beyond mere computer labs and fully engage with a cohesive, across-the-board approach to computing literacy across the curriculum (Saleh, 2019). This approach ensures that students learn to employ digital skills in applied, discipline-specific settings; for example, students using data analysis software for a science class or a collaborative digital platform for a history project (Georgopoulou et al., 2025). The emergence of interdisciplinary experiences, such as computational social science or digital humanities, highlights this trend, whereby technical and applied domain skills converge with disciplinary knowledge (Georgopoulou et al., 2025).

- **Vocational and Alternative Training Models**

Awareness that the traditional four-year degree is not the only pathway to a meaningful career has led to the development of a diverse ecosystem of alternative training models in the United States(Gerdeman, 2022). For example, vocational training programs and coding bootcamps emphasize intensive, short-term, and targeted training to master specific and relevant technical proficiencies, such as data analytics or web development(Gerdeman, 2022). Hence, research suggests that these options can benefit employment outcomes, particularly for career changers (Gerdeman, 2022). At the same time, the vast number of massive open online courses (MOOCs) offered through platforms such as Coursera and edX, which provide open access to high-quality educational content offered by leading universities and organizations (Kaplan & Haenlein, 2016), provides another alternative and pathway for engagement in the learning process.

- **Corporate and Lifelong Learning Initiatives**

The rapid pace of technological change demands lifelong learning, and companies are increasingly taking the initiative in employees' ongoing development. Upskilling and reskilling practices are regarded as strategic imperatives for companies that want to retain talent and navigate digital transformation(Li, 2022). These range from subscriptions to online library-learning materials to creating custom in-house training academies (Li, 2022). The most critical aspect of success in such programs is fostering a "learning culture" (Senge, 2006). This relies not just on courses but also on leader board support, committed learning time, and management practices, making it a priority to institutionalize learning by rewarding experimentation, sharing, and knowledge (Senge, 2006). When employees feel

well supported and able to engage in continuous skill development, the entire organization shifts, becoming agile, innovative, and more adaptable to change (Senge, 2006).

- **The Importance of Public-Private Partnerships (PPPs)**

The sprawling scale and complexity of the digital skills gap means that no sector can address it alone, making public-private partnerships (PPPs) an imperative approach (Languille, 2017). PPPs leverage the unique benefits of each stakeholder: education providers must lend pedagogical knowledge; industries should provide insight and opportunities for authentic experiential education; and governments should provide financial support, policy structure, and scale (Languille, 2017). Preferred examples, such as dual vocational education training in Germany and Pathways in Technology Early College High School (P-TECH) in the United States, highlight the value of deep collaboration (Boudard, 2021; Schwartz, 2017). In dual vocational education, this pathway was characterized as co-designing the curriculum with educators and industries for relevance, weaving learning between the classroom and the workplace (Boudard, 2021; Schwartz, 2017).

Implications and Recommendations

This study provides several implications and recommendations for various stakeholders, as elaborated below (Boudard, 2021; Schwartz, 2017). As for educators, all stakeholders in educational systems and organizations need to be proactive in including digital literacy and citizenship in the curriculum and then using project-based experiential learning (Li, 2022). Schools need to do this through robust investment in professional learning so that educators can feel confident and competent in teaching these skills (Gerdeman, 2022). Creating connections with industry is essential for keeping the curriculum up-to-date and providing additional curriculum to build on job market needs (Kaplan & Haenlein, 2016). For employers, businesses need to emphasize that their workforce training is a capital investment rather than an ongoing expense (Georgopoulou et al., 2025). Setting up a continuous education/learning environment for workforce training that is aligned with continuous improvement hours of work and dedicated resources to reskilling individuals (Georgopoulou et al., 2025). Employers need to work with education to co-develop training and apprenticeships to build a sustainable talent development pipeline (Saleh, 2019). Lastly, for policymakers, it is critical that government digital skills strategy development is championed by the government (Languille, 2017). This would mean developing access to digital skills through funding digital infrastructure and bridging the gap, promoting public-private partnerships through monetary support and/or incentives or grants, or building a regulatory framework that would enable innovative credentialing and flexibility to earn badges and credentials outside of their degree (Revuelta-Domínguez et al., 2022).

Conclusion

In today's data-driven societies, the ability to understand and work with data is essential for people as well as organisations. However, addressing the challenges associated with integration and ensuring effective implementation remains essential. The implications of this research emphasize the urgency for organizations to invest in comprehensive and ongoing cybersecurity awareness and data literacy training programs. By prioritizing employee training and developing a proactive security mindset, businesses can proactively protect their assets, maintain customer trust, and ensure a secure future amidst the ever-evolving cybersecurity landscape.

References

1. Annunziata, M. (2020, February 5). The skills of the future: Problem-solving. *Forbes*. <https://www.forbes.com/sites/marcoannunziata/2020/02/05/the-skills-of-the-future-problem-solving/>
2. Asa, A. R., Campbell, H., & Nautwima, J. P. (2022). A critical review of organizing knowledge management for innovation. *International Journal of Management Science and Business Administration*, 8(2), 7-15. doi:<https://doi.org/10.18775/ijmsba.1849-5664-5419.2014.82.1001>
3. Autor, D. H. (2015). Why are there still so many jobs? The history and future of workplace automation. *Journal of Economic Perspectives*, 29(3), 3–30. <https://doi.org/10.1257/jep.29.3.3>
4. Bejaković, P., & Mrnjavac, Ž. (2020). The importance of digital literacy on the labour market. *Employee Relations: The International Journal*, 42(4), 921-932. <https://doi.org/10.1108/ER-07-2019-0274>

5. Bresnahan, T. F., Brynjolfsson, E., & Hitt, L. M. (2002). Information technology, workplace organization, and the demand for skilled labor: Firm-level evidence. *The Quarterly Journal of Economics*, 117(1), 339-376. <https://doi.org/10.1162/003355302753399526>
6. Brosnan, M. J. (2002). Technophobia: The psychological impact of information technology. *Computers in Human Behavior*, 73, 1-13. <https://doi.org/10.4324/9780203436707>
7. Casner-Lotto, J., & Barrington, L. (2006). Are they really ready to work? Employers' perspectives on the basic knowledge and applied skills of new entrants to the 21st century US workforce. The Conference Board. <https://www.frontiersin.org/journals/education/articles/10.3389/feduc.2025.1562391/full>
8. Pangrazio, L. (2016). Reconceptualising critical digital literacy. *Discourse: Studies in the Cultural Politics of Education*, 37(2), 163-174. <https://doi.org/10.1080/01596306.2014.942836>
9. Pluto Insights. (2024). Developing effective search strategies for literature reviews. Pluto.im. Retrieved from <https://insights.pluto.im/developing-effective-search-strategies-for-literature-reviews/>
10. Eshet, Y. (2012). Thinking in the digital era: A revised model for digital literacy. *Issues in Informing Science and Information Technology*, 9, 267-276. <https://doi.org/10.28945/1621>
11. García-Peñalvo, F. J. (2021). Avoiding the dark side of digital transformation in teaching. An institutional reference framework for eLearning in higher education. *Sustainability*, 13(4), 2023. <https://doi.org/10.3390/su13042023>
12. Kshetri, N. (2021). Economics of Artificial Intelligence in Cybersecurity. *IT Professional*, 23(5), 73-77. <https://doi.org/10.1109/MITP.2021.3100177>
13. Lee, C. S., & Chua, Y. T. (2024). The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States. *Crime & Delinquency*, 70(9), 2250-2277. <https://doi.org/10.1177/00111287231180093>
14. Lee, J. J., & Meng, J. (2021). Digital competencies in communication management: a conceptual framework of Readiness for Industry 4.0 for communication professionals in the workplace. *Journal of Communication Management*, 25(4), 417-436. <https://doi.org/10.1108/JCOM-10-2020-0116>
15. Li, G., Hou, Y., & Wu, A. (2017). Fourth Industrial Revolution: technological drivers, impacts and coping methods. *Chinese Geographical Science*, 27(4), 626-637. <https://doi.org/10.1007/s11769-017-0890-x>
16. Li, L. (2022). Reskilling and Upskilling the Future-ready Workforce for Industry 4.0 and Beyond. *Inf Syst Front*. 2022 Jul 13:1-16. <https://doi.org/10.1007/s10796-022-10308-y>
17. Tinmaz, H., Lee, Y. T., Fanea-Ivanovici, M., & Baber, H. (2022). A systematic review on digital literacy. *Smart Learning Environments*, 9(1), 21. <https://doi.org/10.1186/s40561-022-00204-y>
18. van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2020). Determinants of 21st-Century Skills and 21st-Century Digital Skills for Workers: A Systematic Literature Review. *SAGE Open*, 10(1). <https://doi.org/10.1177/2158244019900176>
19. Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, 54(1), 1-39. <https://doi.org/10.1145/3427920>
20. Asa Romeo Asa , Johanna Pangeiko Nautwima , Helvi Nyete Johannes Digital Literacy for Workforce Readiness: Bridging the Skills Gap in the 21st Century DOI:10.18775/ijied.1849-7551-7020.2015.311.2001 URL:<https://doi.org/10.18775/ijied.1849-7551-7020.2015.311.2001>
21. Dawit Negussie Tolossa, Importance of cyber security awareness training for employees in business, <http://vidyajournal.org>
22. Lee, J. J., & Meng, J. (2021). Digital competencies in communication management: a conceptual framework of Readiness for Industry 4.0 for communication professionals in the workplace. *Journal of Communication Management*, 25(4), 417-436. <https://doi.org/10.1108/JCOM-10-2020-0116>
23. Ritter, G., & D'Auria, A. (2023). The human-tech interface: Why emotional intelligence is the new digital superpower. *Harvard Business Review*, 101(4), 88-97.

