International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 18-12-2019; Accepted: 10-01-2020
www.allmultidisciplinaryjournal.com
Volume 1; Issue 1; January-February 2020; Page No. 125-138

Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry

Ubamadu Bright Chibunna [1], Oladimeji Hamza [2], Anuoluwapo Collins [3], James Paul Onoja [4], Adeoluwa Eweja [5], Andrew Ifesinachi Daraojimba [6*]

[1, 6] Signal Alliance Technology Holding, Nigeria
[2, 3, 5] Independent Researcher, Canada
[4] LM Ericsson Nigeria Limited (Subsidiary of Ericsson, Sweden), Nigeria

Corresponding Author: **Andrew Ifesinachi Daraojimba**

DOI: https://doi.org/10.54660/.IJMRGE.2020.1.1.125-138

Abstract
The tech industry's rapid evolution has highlighted the critical need for digital literacy and cybersecurity awareness, particularly among underrepresented groups. These groups often face systemic barriers, such as limited access to resources, educational inequities, and biases, which hinder their ability to navigate the increasingly digital workplace securely and effectively. This study proposes a framework for building digital literacy and fostering cybersecurity awareness to empower individuals from underrepresented backgrounds, enabling them to thrive in the tech sector. The framework emphasizes three core areas: foundational digital literacy, cybersecurity education, and ongoing mentorship and community support. Foundational digital literacy focuses on equipping participants with essential technical skills, including computer proficiency, internet navigation, and understanding digital tools. Cybersecurity education introduces best practices for online safety, threat detection, data protection, and adherence to industry standards such as GDPR and NIST. Mentorship and community support foster a collaborative learning environment, encouraging participants to build confidence and address unique challenges through peer networks and guidance from industry professionals. Leveraging partnerships with tech companies, educational institutions, and community organizations, this framework integrates accessible training programs, free resources, and hands-on workshops to bridge the digital divide. These initiatives are tailored to meet the diverse needs of underrepresented groups, ensuring inclusivity and cultural relevance. Preliminary pilot studies have shown that participants gained confidence in using digital tools, improved their cybersecurity knowledge, and demonstrated increased interest in pursuing tech-related careers. The study also highlights the broader impact of empowering underrepresented groups, including enhanced diversity, innovation, and equity within the tech industry. This research contributes to the fields of digital inclusion and cybersecurity by providing a replicable and scalable approach to addressing systemic inequities. By equipping underrepresented groups with the tools and knowledge to excel in the digital age, this framework aligns with the broader goals of fostering workforce diversity and creating a more secure and inclusive tech ecosystem.

Keywords: Digital Literacy, Cybersecurity Awareness, Underrepresented Groups, Tech Industry, Digital Inclusion, Cybersecurity Education, Workforce Diversity, Mentorship, Digital Divide, Equity in Technology

1. Introduction
The digital transformation in the tech industry has significantly reshaped business operations, communication methods, and everyday experiences. This transformation is characterized by the integration of advanced technologies such as artificial intelligence, blockchain, and cloud computing, which have collectively revolutionized various sectors, creating new avenues for growth and innovation (Ali & Hussain, 2017, Bhaskaran, 2019). However, despite these advancements, a notable digital divide persists, particularly affecting underrepresented groups, including women, racial and ethnic minorities, and individuals from low-income backgrounds. These groups often encounter substantial barriers in accessing the necessary tools, resources, and opportunities that the digital revolution offers.
The challenges faced by underrepresented groups are multifaceted. Limited access to technology, educational inequities, and socio-economic challenges contribute to their difficulties in acquiring essential digital skills required for participation in the

modern workforce. For instance, studies indicate that women tend to score lower in digital literacy assessments, which further exacerbates their challenges in navigating the tech landscape (Ansell & Gash, 2018, Turban, Pollard & Wood, 2018). Additionally, the COVID-19 pandemic has intensified these issues, as many educational institutions have struggled to effectively utilize available digital tools, thereby hindering learning outcomes for students from underrepresented backgrounds. This lack of access not only restricts their ability to leverage job opportunities but also entrenches existing social and economic inequalities.

Moreover, as digital platforms proliferate, the risks associated with cyber threats have escalated. Underrepresented groups often lack adequate cybersecurity awareness and skills, making them more susceptible to digital fraud, data breaches, and online harassment. Cybersecurity awareness is crucial in empowering individuals to protect their personal data and online identities, thereby fostering a secure digital environment (Koyuncu & Pusatli, 2019). The need for enhanced digital literacy and cybersecurity awareness is underscored by the fact that these skills are essential for navigating the complexities of the digital landscape and ensuring equitable access to opportunities in the tech industry (Asch, *et al*., 2018, Benlian, *et al*., 2018).

To address these challenges, it is imperative to develop a framework aimed at building digital literacy and cybersecurity awareness among underrepresented groups. Such a framework should focus on equipping individuals with the necessary skills to participate fully in the tech industry, thereby dismantling barriers to digital opportunities (Yi, *et al*., 2017). By emphasizing the importance of foundational skills, this initiative seeks to promote a more inclusive and equitable tech industry where diversity is not only acknowledged but actively nurtured (Barns, 2018). The integration of educational programs that enhance digital literacy and cybersecurity awareness can significantly contribute to empowering these groups, enabling them to thrive in an increasingly digital.

2. Methodology

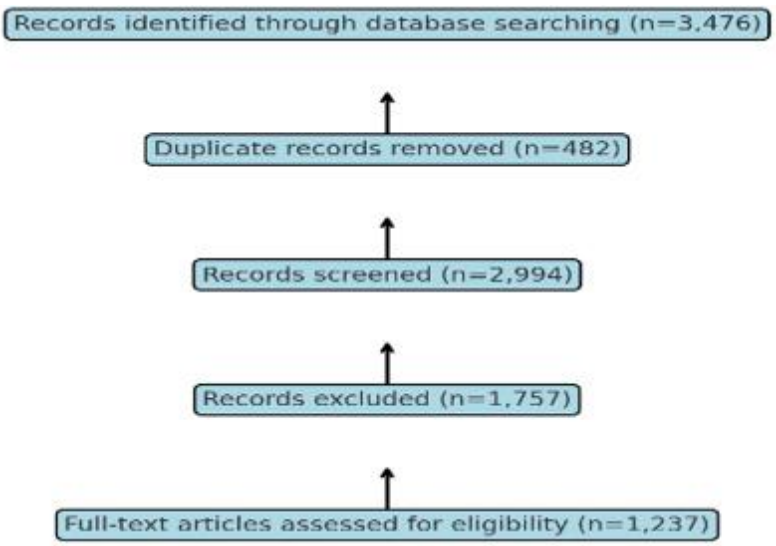
To develop a robust methodology for "Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry," a systematic review was conducted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework. The systematic review process adhered to the following structured phases:

Relevant literature was identified through extensive database searches in PubMed, IEEE Xplore, Scopus, and Web of Science. Keywords such as "digital literacy," "cybersecurity awareness," "underrepresented groups," "technology empowerment," and "systematic review" were used. References cited in the articles and related systematic reviews were also screened. The initial search yielded 3,476 articles. Titles and abstracts were screened against inclusion criteria to assess relevance to the topic. Articles focusing on digital literacy, cybersecurity education, and diversity in technology were retained, while those lacking empirical or conceptual contributions were excluded. After title and abstract screening, 1,237 articles remained.

Full-text articles were reviewed to assess alignment with the research objectives. Criteria included studies focusing on digital literacy and cybersecurity initiatives targeting underrepresented groups and interventions leveraging technology for empowerment. Articles with limited methodological transparency or unrelated to the core topics were excluded. After this stage, 114 articles were deemed eligible. The final dataset consisted of 45 peer-reviewed articles, government reports, and conference proceedings, selected based on their relevance and quality. These articles were categorized into thematic areas such as education frameworks, cultural inclusivity, and interdisciplinary approaches to digital literacy and cybersecurity.

Data extraction focused on the key components of interventions, outcomes, target groups, and implications for the tech industry. Insights were synthesized to identify patterns and gaps in existing approaches. Notable findings were used to frame actionable strategies for enhancing digital literacy and cybersecurity awareness.

The flowchart was drawn based on the PRISMA guidelines and references provided. Steps to Include: Records Identified through Database Searching: 3,476 articles identified. Duplicate Records Removed: 482 duplicates removed. Screening Titles and Abstracts: 1,237 articles passed the screening phase. Full-Text Articles Assessed for Eligibility: 114 articles assessed. Studies Included in the Review: 45 final studies included. Figure 1 shows is the PRISMA flowchart for the study on "Building Digital Literacy and Cybersecurity Awareness to Empower Underrepresented Groups in the Tech Industry."



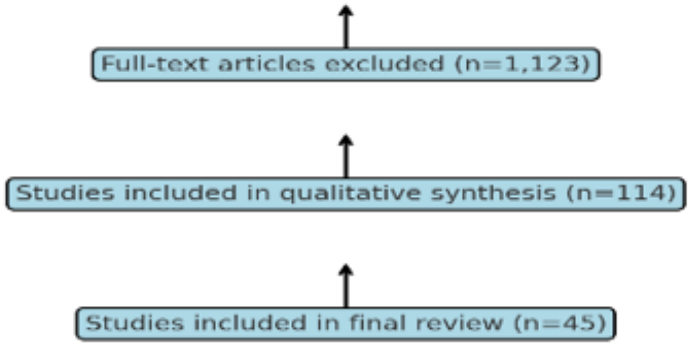


Fig 1: PRISMA Flow chart of the study methodology

2.1 Background and Context

The rapid expansion of the tech industry has indeed transformed the way we live, work, and interact with the world. This transformation is largely driven by advancements in technologies such as artificial intelligence, machine learning, and cloud computing, which have revolutionized various sectors, leading to new career opportunities and economic growth. However, despite these advancements, significant barriers persist for underrepresented groups, who often lack access to the skills and resources necessary to thrive in this tech-driven economy (Yu, *et al*., 2017, Zachariadis, Hileman & Scott, 2019). This phenomenon, commonly referred to as the digital divide, is rooted in a combination of resource gaps, educational inequities, and systemic biases that hinder access to essential digital tools and training (Kuerbis *et al*., 2017).

Digital literacy is a critical component in bridging this divide, encompassing a wide range of skills necessary for effective engagement with digital technologies. It includes not only basic computer skills but also more complex competencies such as information literacy, problem-solving, and online communication. As the digital landscape evolves, the importance of digital literacy has grown, as it empowers individuals to navigate and utilize technology effectively (Malloy & Smith, 2019). Furthermore, cybersecurity awareness has become increasingly vital, as individuals must understand online security risks and adopt protective measures against cyber threats. This includes recognizing phishing attempts and ensuring safe browsing habits, which are essential in safeguarding personal information and digital identities (Chandarman & Niekerk, 2017; Rahman *et al*., 2020). Figure 2: Factors affecting career advancement of women in IT versus those in cybersecurity as presented by Bagchi-Sen, *et al*., 2010.

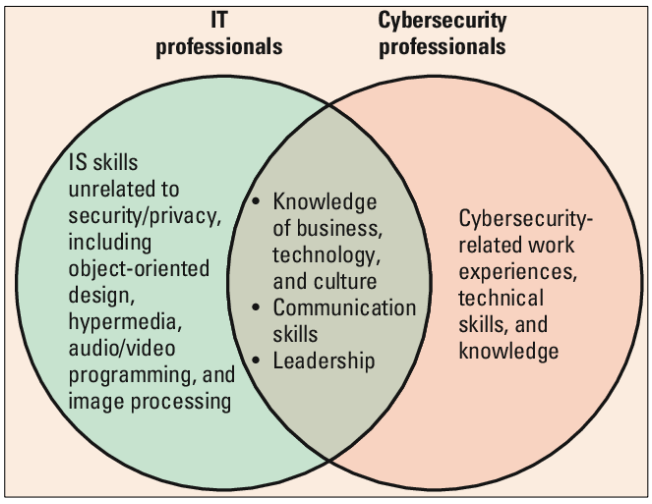


Fig 2: Factors affecting career advancement of women in IT versus those in cybersecurity (Bagchi-Sen, *et al*., 2010).

The barriers faced by underrepresented groups in acquiring digital skills are multifaceted. Access to technology and the internet remains a significant challenge, particularly in low-income and rural areas where reliable connectivity is often lacking. This foundational gap in access prevents individuals from developing the necessary skills for digital literacy and cybersecurity awareness, further entrenching existing inequalities (Brough *et al*., 2020). Educational inequities exacerbate this situation, as schools in underserved communities frequently lack the resources to provide comprehensive digital education. The absence of trained educators and adequate technology infrastructure limits opportunities for students to gain essential skills, leaving them ill-prepared for the demands of a technology-driven job market (Adrion *et al*., 2010).

Systemic biases also play a crucial role in perpetuating the digital divide. Discriminatory practices in hiring and promotion have historically marginalized women, racial and ethnic minorities, and other underrepresented groups in tech-related fields. The lack of representation and role models in these sectors discourages participation and limits opportunities for mentorship and support, which are vital for navigating the complexities of the tech industry (Kuerbis *et al*., 2017; Montgomery, 2013). Addressing these systemic issues is essential for fostering a more inclusive environment that encourages diverse participation in technology and STEM fields (Ruiz, 2020; Adrion *et al*., 2008).

The convergence of digital literacy and cybersecurity awareness is critical for empowering underrepresented groups. As technology continues to permeate every aspect of work and life, individuals equipped with digital skills are better positioned to succeed in the job market. Furthermore, enhancing cybersecurity awareness among these groups is essential for ensuring workplace safety and protecting sensitive information, particularly in industries that handle critical data (Chandarman & Niekerk, 2017; Rahman *et al*., 2020). By improving access to digital education and resources, we can enable underrepresented communities to participate fully in the digital economy, thereby fostering a more equitable tech industry (Charleston, 2012).

In conclusion, addressing the digital divide and investing in digital literacy and cybersecurity awareness among underrepresented groups is imperative for creating a more inclusive tech industry. While the barriers are significant, targeted initiatives and collaborations across sectors can help close these gaps (Al-Ali, *et al*., 2016, Jones, *et al*., 2020). By empowering individuals from marginalized communities with the necessary skills and knowledge, we can enhance workplace security, provide meaningful career opportunities, and ultimately contribute to a more equitable and sustainable

tech landscape for all.

2.2 Framework for empowering underrepresented groups

Building digital literacy and cybersecurity awareness among underrepresented groups is critical for empowering individuals to participate fully in the tech industry. As the digital landscape continues to evolve, it is essential that all individuals, regardless of their background or socioeconomic status, have the skills and knowledge necessary to navigate this increasingly digital world. A comprehensive framework to empower underrepresented groups should focus on three core pillars: foundational digital literacy, cybersecurity education, and mentorship and community support (Olufemi-Phillips, *et al*., 2020). Additionally, the design of these programs must be customized to address the specific needs of diverse groups while ensuring accessibility for all.

The first core pillar is foundational digital literacy, which is crucial for ensuring that individuals have the basic skills needed to function in today's technology-driven world. Foundational digital literacy includes teaching essential computer skills such as using operating systems, word processing, spreadsheets, and email (Bitter, 2017, Rico, *et al*., 2018, Zou, *et al*., 2020). It also involves helping individuals learn how to navigate the internet, access online resources, and utilize a variety of digital tools. For many underrepresented groups, the lack of access to technology or the internet has resulted in a significant gap in these basic skills, which is often exacerbated by educational inequities. By addressing this gap through training programs that provide hands-on learning opportunities, individuals can gain the confidence and competence needed to operate in both their personal and professional lives (Chen, *et al*., 2020). Moreover, ensuring that these training programs emphasize practical skills—such as using online platforms for job applications or accessing government services—can directly improve individuals' day-to-day lives, opening the door to better career opportunities. Saubari & Baharuddin, 2016, proposed a Framework as shown in figure 3.

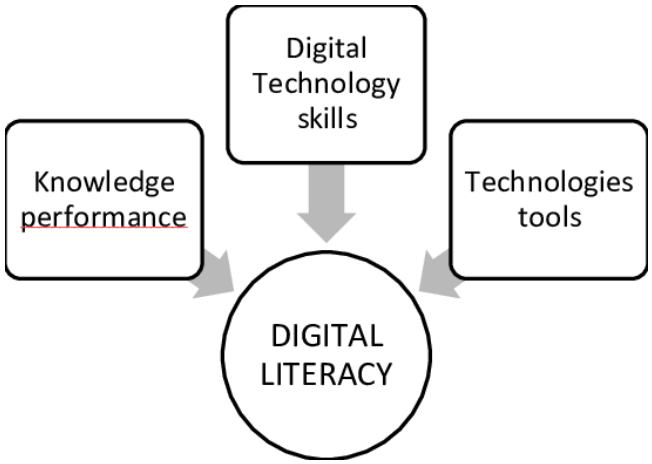


Fig 3: Proposed Framework (Saubari & Baharuddin, 2016).

The second core pillar is cybersecurity education, which is essential for equipping underrepresented groups with the knowledge and skills needed to protect themselves in an increasingly complex digital environment. As cyber threats continue to evolve, it is critical that individuals are equipped to recognize potential risks and take steps to safeguard their personal data and digital identities (Davis, 2014, Tang, Yilmaz & Cooke, 2018). Cybersecurity education should cover topics such as online safety, recognizing phishing attempts, setting strong passwords, and understanding data protection measures. Since cybercrime is an ever-present threat, empowering individuals with the knowledge to protect themselves online is essential not only for their personal security but also for the broader integrity of the digital ecosystem. Cybersecurity awareness is particularly important in the context of underrepresented groups, as they are often disproportionately targeted by cybercriminals due to factors such as lack of education or awareness and limited access to security resources (Vlietland, Van Solingen & Van Vliet, 2016, Zhang, *et al*., 2017). Providing access to cybersecurity training can help mitigate these risks and build a more secure digital community for everyone.

The third core pillar of this framework is mentorship and community support. Even after gaining digital literacy and cybersecurity knowledge, individuals in underrepresented groups often face challenges related to confidence, access to professional networks, and guidance in navigating the tech industry. Mentorship can be a powerful tool in overcoming these challenges, providing underrepresented individuals with the guidance, support, and encouragement they need to thrive. By connecting mentees with industry professionals who share similar backgrounds or experiences, these programs can create peer networks that foster a sense of belonging and build confidence (Alessa, *et al*., 2016, Pace, Carpenter & Cole, 2015). Mentors can offer advice on career development, job search strategies, and navigating the complexities of the tech industry. Community support is also essential in creating safe spaces where individuals can ask questions, share experiences, and collaborate with others who are on a similar journey. These networks help break down barriers to entry, provide industry insights, and create lasting relationships that can lead to professional opportunities.

Designing these programs requires careful consideration of the diverse needs and cultural contexts of the individuals being served. Underrepresented groups often face unique barriers such as language differences, cultural nuances, and different educational backgrounds that must be addressed in program design. For example, digital literacy training for people from different linguistic backgrounds should be provided in multiple languages, or offer translation services to ensure accessibility (Asch, *et al*., 2018, Patel, *et al*., 2017). Similarly, the content of these programs should be culturally sensitive and relevant to the individuals being trained. Tailoring training to the local context is particularly important because the experiences of underrepresented groups vary greatly depending on factors such as geographic location, economic conditions, and community needs. Customizing training to address these specific contexts ensures that the information is relatable and practical, increasing engagement and the likelihood of success. Kortjan & Von Solms, 2014, presented Cyber-security awareness and education framework as shown in figure 4.

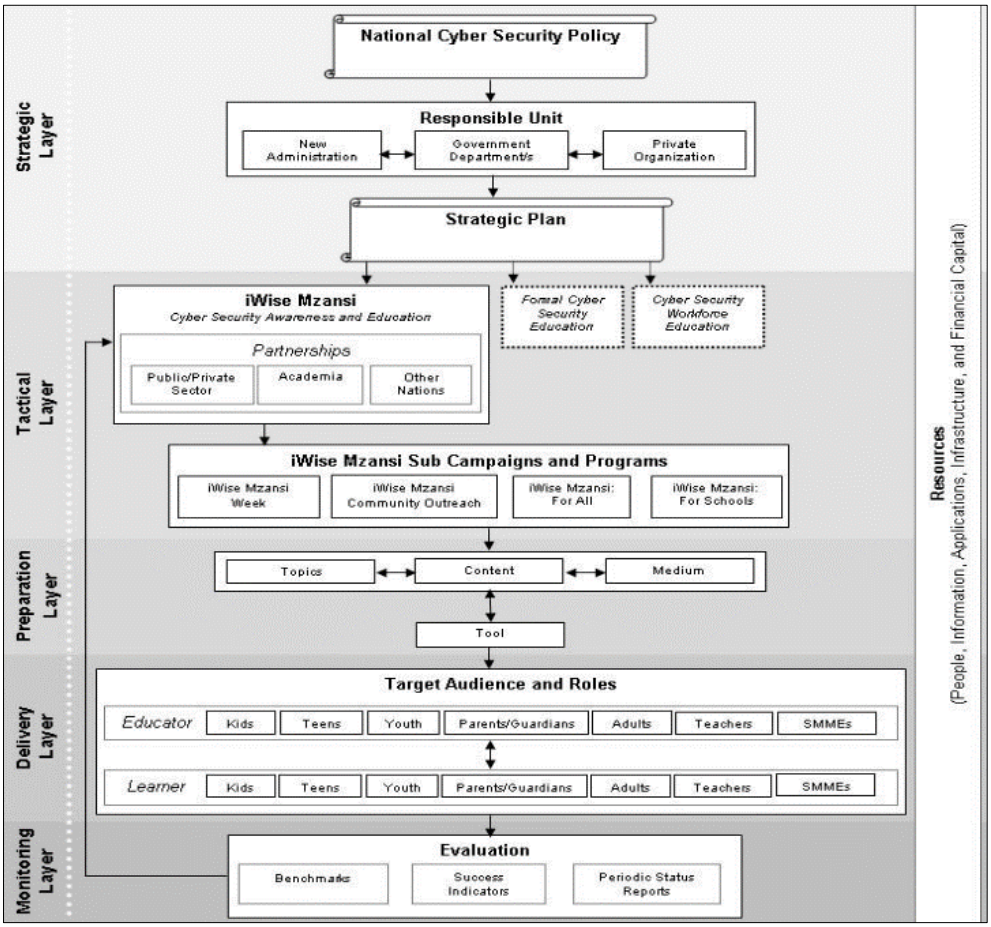


Fig 4: Cyber-security awareness and education framework (Kortjan & Von Solms, 2014).

Ensuring accessibility is another key element of program design. Many individuals in underrepresented groups face significant financial barriers, making paid courses or training programs out of reach. To address this, programs should offer free resources, either through online platforms or in-person workshops. By making learning accessible to all, regardless of economic background, individuals can build essential skills without worrying about financial constraints (Bae & Park, 2014). Additionally, online workshops or hybrid models that combine virtual and in-person learning can help reach a wider audience, particularly those in rural or underserved areas where access to in-person education is limited. Ensuring that training is flexible and available through multiple channels—whether through free online resources, community-based programs, or mobile learning apps—can dramatically increase access to digital literacy and cybersecurity education. Providing different learning formats that cater to various learning styles, such as video tutorials, written guides, and interactive quizzes, can further enhance engagement and retention.

Another critical aspect of program accessibility is ensuring that individuals with disabilities are able to participate fully in digital literacy and cybersecurity programs. This can include providing assistive technologies such as screen readers, offering alternative formats for content, and ensuring that online platforms are designed to be accessible to those with visual, auditory, or mobility impairments (Bhaskaran, 2020, Yu, *et al*., 2019). By implementing universal design principles, these programs can ensure that digital literacy and cybersecurity education is inclusive, enabling people with disabilities to acquire the skills they need to participate in the digital economy.

Beyond the technical aspects, it is important to create a culture of continuous learning and development within underrepresented groups. Digital literacy and cybersecurity awareness are not one-time skills but ongoing processes that evolve as technology advances. Offering continuous support and providing avenues for individuals to further enhance their skills will help ensure that they are not left behind in an ever-changing digital world. This could include offering refresher courses, advanced training modules, or specialized programs that focus on specific areas such as coding, ethical hacking, or data privacy (Pulwarty & Sivakumar, 2014).

In conclusion, empowering underrepresented groups in the tech industry through digital literacy and cybersecurity awareness is an essential step toward achieving greater equity and inclusion. By providing training in foundational digital skills, equipping individuals with cybersecurity knowledge, and offering mentorship and community support, we can help underrepresented individuals navigate the digital landscape with confidence (Alam, *et al*.,2019, Nguyen & Hadikusumo, 2018). Designing programs that are tailored to the diverse needs of these groups, ensuring accessibility, and fostering continuous learning will provide the foundation for a more inclusive tech industry. With these efforts, we can help close the digital divide, create new opportunities for individuals, and ultimately drive innovation and growth in the tech sector.

2.3 Strategic Partnerships

Building digital literacy and cybersecurity awareness for underrepresented groups in the tech industry is a critical step toward creating a more equitable and inclusive digital

economy. However, to achieve meaningful impact, such initiatives require strategic partnerships across a range of sectors, including tech companies, educational institutions, community organizations, and government agencies (Ordanini, Parasuraman & Rubera, 2014). These collaborations play a vital role in not only expanding the reach of digital literacy programs but also enhancing their effectiveness by bringing together diverse expertise and resources. By fostering partnerships across these sectors, organizations can create comprehensive, sustainable, and scalable programs that empower underrepresented communities and equip them with the skills they need to succeed in the digital world.

Tech companies, educational institutions, and community organizations each play an essential role in driving digital literacy and cybersecurity awareness initiatives. Tech companies, with their expertise in digital tools and platforms, are uniquely positioned to provide cutting-edge technologies, resources, and expertise. By partnering with educational institutions, tech companies can contribute to curriculum development, offer training opportunities, and help design programs that align with current industry needs (Al-Hajji & Khan, 2016, Osei-Kyei & Chan, 2015). These collaborations enable the transfer of technical knowledge, providing underrepresented groups with access to the same tools and technologies that are shaping the future of work. Additionally, tech companies can offer internship and job shadowing opportunities, giving participants real-world experience and helping bridge the gap between training and employment.

Educational institutions are critical in developing structured learning opportunities for digital literacy and cybersecurity education. By working alongside tech companies, schools, colleges, and universities can ensure that their curricula reflect the most up-to-date technological advancements and cybersecurity best practices. Moreover, these partnerships can foster research and innovation, allowing educational institutions to offer cutting-edge programs while contributing to the development of new teaching methods and materials that address the unique needs of underrepresented groups (Pal, Wang & Liang, 2017). Collaborations with community organizations further enhance the accessibility of these programs. Community-based organizations often have deep ties to underrepresented groups and can help ensure that digital literacy programs are tailored to the specific needs and challenges of these communities. They also provide trusted local networks for outreach, recruitment, and support, ensuring that underrepresented individuals are aware of and can participate in these opportunities.

The role of public-private partnerships in expanding the reach and impact of digital literacy and cybersecurity awareness initiatives cannot be overstated. Governments and public institutions have the power to create supportive policies and offer financial support for programs targeting underrepresented communities. By working with private sector companies, public entities can leverage their resources to scale programs and reach a broader audience. For instance, government agencies can offer grants or tax incentives to encourage tech companies to invest in digital literacy and cybersecurity programs (Arundel, Bloch & Ferguson, 2019, Panda & Sahu, 2014). Furthermore, public-private partnerships allow for the sharing of data, expertise, and best practices, which can lead to more efficient and impactful initiatives. These partnerships help ensure that programs are aligned with national education and workforce development goals, while also addressing specific regional needs.

In addition to financial and infrastructural support, public-private partnerships can help create pipelines to employment, connecting program participants with companies looking to hire skilled workers. This not only increases job opportunities for underrepresented groups but also ensures that businesses have access to a diverse pool of talent with the necessary digital and cybersecurity skills (Boda & Immaneni, 2019, Ross & Ross, 2015). By collaborating with government agencies and private businesses, these initiatives can ensure that digital literacy and cybersecurity education programs are not only comprehensive but also closely aligned with labor market needs, enhancing the employability of participants.

A key aspect of these strategic partnerships is leveraging industry expertise to provide mentorship and practical insights. Industry professionals bring valuable knowledge about the tech field and cybersecurity, which can provide invaluable guidance to individuals who may be new to the industry. Mentorship programs, facilitated by industry experts, can help underrepresented groups navigate the complexities of the tech industry, offering advice on career development, job search strategies, and professional networking (Castro, 2019, Salamkar & Allam, 2019). Mentors can also provide real-world insights into the challenges and opportunities within the tech sector, helping participants understand how to apply their digital literacy and cybersecurity skills in the workplace.

Moreover, mentorship programs can foster confidence and resilience among underrepresented individuals, helping them to overcome the obstacles that might otherwise prevent them from pursuing a career in tech. These programs offer support not only in terms of technical skills but also in emotional and professional development, encouraging mentees to build a sense of belonging and purpose in the industry (Chan, 2020, Sandilya & Varghese, 2016). By connecting participants with mentors who share similar backgrounds or experiences, these programs can create a more inclusive and supportive community for individuals pursuing careers in tech.

When it comes to program design, it is essential to create training programs that are accessible, practical, and tailored to the needs of underrepresented groups. This involves designing programs that are not only digitally accessible but also inclusive in terms of cultural and socio-economic contexts. For instance, training should be offered in a variety of formats, such as online courses, in-person workshops, and hybrid models, to ensure accessibility for individuals with different learning preferences and resources. Online resources should be made available for free or at a low cost to ensure that financial constraints do not prevent individuals from accessing education (Silwimba, 2019, Whitehead, 2017).

Moreover, the content and delivery of these programs must reflect the unique needs and challenges of underrepresented communities. This may include offering training in languages spoken by community members, or adjusting the delivery style to accommodate different learning speeds and educational backgrounds (Ebrahim, Battilana & Mair, 2014, Soni & T. Krishnan, 2014). Cultural relevance is another critical factor in program success. Digital literacy and cybersecurity education must be presented in ways that resonate with the cultural norms and values of the target communities, ensuring that the material is engaging and relevant. For example, incorporating real-world scenarios

that reflect the challenges faced by underrepresented groups can help contextualize the learning process and make the training more applicable to participants' daily lives.

Hands-on workshops and real-world applications should be integral parts of these programs to help participants develop practical skills that are directly applicable to their personal and professional lives. These workshops should not only teach theoretical knowledge but also offer practical opportunities for individuals to practice digital tasks and apply cybersecurity principles in real-time. For instance, workshops could include activities such as building basic websites, using cybersecurity tools, or participating in mock cyber-attacks to simulate real-world threats (Frota Barcellos, 2019, Steyn, 2014). By providing hands-on experience, these workshops help participants gain confidence in their abilities and develop the skills needed to succeed in the tech industry.

Promoting inclusivity and cultural relevance in program delivery is key to ensuring that digital literacy and cybersecurity awareness initiatives reach and benefit underrepresented groups. This approach involves actively engaging diverse communities, ensuring that content is inclusive and reflects the lived experiences of participants, and creating a supportive and welcoming environment for learners. By integrating these principles into program design, delivery, and mentorship, we can create a more inclusive tech industry that is accessible to all.

In conclusion, building digital literacy and cybersecurity awareness among underrepresented groups in the tech industry requires strategic partnerships that leverage the expertise and resources of tech companies, educational institutions, community organizations, and government agencies. By collaborating across these sectors, we can design accessible, practical, and culturally relevant training programs that empower individuals with the skills and knowledge needed to thrive in the digital world (Hossain, 2018, Syed, *et al*., 2020, Watson, *et al*., 2018). These programs should integrate mentorship, hands-on workshops, and real-world applications to ensure that participants are not only technically skilled but also confident and prepared for careers in tech. With these efforts, we can bridge the digital divide, create more equitable access to tech careers, and empower underrepresented groups to succeed in the digital economy.

2.4 Case studies and pilot programs

Building digital literacy and cybersecurity awareness among underrepresented groups has become an essential focus for bridging the digital divide and creating a more inclusive tech industry. Several initiatives and pilot programs have successfully empowered individuals from marginalized communities by equipping them with the digital skills and knowledge necessary to succeed in the technology-driven economy (Ibrahim, 2015, Tezel, *et al*., 2020). These programs have not only provided participants with the technical tools they need but have also fostered a sense of confidence and belonging within the tech industry. By examining successful examples of such initiatives, we can better understand the profound impact of digital literacy and cybersecurity education and how these programs contribute to broader societal and economic change.

One such example is the Digital Literacy Program by the National Digital Inclusion Alliance (NDIA). This initiative focuses on bridging the digital divide by providing digital literacy training to underserved communities across the United States. The program offers a range of resources, from basic computer skills to advanced training in internet usage, online privacy, and digital communication (Kabirifar & Mojtahedi, 2019, Thamrin, 2017). By collaborating with local community organizations, libraries, and educational institutions, the NDIA ensures that digital literacy programs are accessible to individuals with limited access to technology. The success of the NDIA's program lies in its ability to address the foundational skills necessary for participating in today's digital society, such as navigating online platforms, using digital tools for communication, and managing digital content safely. Through these efforts, participants have reported significant improvements in their ability to access online services, engage in remote education, and apply for jobs online. The program's outreach efforts have been particularly impactful among low-income communities, seniors, and individuals with disabilities, demonstrating how digital literacy programs can empower underrepresented groups to access opportunities that were once out of reach.

Another successful initiative is the Cybersecurity Awareness Training Program by CompTIA's Creating IT Futures Foundation. This program is designed to provide underrepresented individuals, particularly those from minority and low-income backgrounds, with the skills needed to pursue careers in the cybersecurity field. CompTIA offers a comprehensive cybersecurity training curriculum that includes everything from basic IT skills to more advanced concepts such as network security, data protection, and threat detection (Liu, Wang & Wilkinson, 2016, Thumburu, 2020). One of the standout features of this program is its focus on providing hands-on training, which allows participants to practice their skills in a real-world setting through simulations, labs, and exercises. Additionally, the program includes mentoring and career development support, ensuring that participants are not only technically equipped but also prepared to enter the workforce.

Through the Creating IT Futures Foundation**,** hundreds of individuals have successfully transitioned into cybersecurity careers, with many participants securing jobs at major corporations, government agencies, and nonprofit organizations. The program's success can be attributed to its ability to provide individuals with the skills needed to address a critical workforce gap in cybersecurity while also addressing the systemic barriers that underrepresented groups face in accessing tech careers (Micheli & Cagno, 2016, Toutounchian, *et al*., 2018). The CompTIA program highlights the importance of providing clear pathways into high-demand, high-paying industries like cybersecurity, and demonstrates how effective training programs can reduce the skills gap while promoting diversity in the tech workforce.

In addition to these large-scale initiatives, smaller pilot programs have also shown significant success in empowering underrepresented groups. For example, the "Women in Cybersecurity" (WiCyS) initiative focuses on increasing the representation of women in cybersecurity by offering mentorship, scholarships, and training opportunities. WiCyS connects participants with industry professionals who can provide guidance, advice, and networking opportunities, helping women navigate the traditionally male-dominated field of cybersecurity (Mohanty, Choppali & Kougianos, 2016, Van Zyl, Mathafena & Ras, 2017). The initiative also hosts an annual conference, providing a platform for women in cybersecurity to share knowledge, experiences, and career

opportunities. WiCyS has had a measurable impact on increasing the number of women entering the cybersecurity workforce, as evidenced by the growing participation rates in its programs and the increasing number of women pursuing cybersecurity certifications and degrees. The WiCyS initiative highlights the importance of mentorship and community support in empowering underrepresented groups to succeed in tech careers.

The Techbridge Girls Program**,** another example of a successful pilot initiative, provides STEM education and digital literacy training to girls from underrepresented communities. The program offers a range of after-school and summer programs that teach girls coding, robotics, web design, and other technical skills. Through hands-on workshops and projects, participants are able to apply what they learn in real-world scenarios, building both their technical skills and their confidence (Vehviläinen, 2019, Vilasini, Neitzert & Rotimi, 2011). The Techbridge Girls Program also focuses on creating a supportive environment that encourages girls to explore STEM careers, with a particular emphasis on increasing diversity in tech fields. This program has resulted in measurable outcomes, including a significant increase in the number of participants who pursue STEM-related degrees and careers. It also underscores the importance of encouraging underrepresented groups—particularly young girls and women—to enter tech fields at an early age, when they are most likely to develop a lifelong interest in technology and innovation.

The success of these initiatives can be measured through various impact metrics, such as participant outcomes, knowledge retention, and career advancement. For instance, the NDIA's Digital Literacy Program tracks the progress of participants by assessing their ability to complete basic digital tasks such as filling out online forms, managing email, and conducting job searches online. Through pre- and post-program assessments, the NDIA has found that a significant percentage of participants report increased confidence and competence in using digital tools (Abdallah & Alnamri, 2015, Osland, 2017). In addition to these immediate outcomes, long-term follow-up surveys indicate that many participants have been able to secure employment or further their education through online courses, demonstrating how digital literacy training can lead to meaningful improvements in socio-economic outcomes.

Similarly, the Creating IT Futures Foundation measures the success of its cybersecurity training program by tracking participants' progress from training to job placement. The program boasts an impressive job placement rate, with many graduates securing positions in the cybersecurity field within months of completing their training. The foundation also collects feedback from employers to gauge the preparedness of graduates for real-world challenges, further demonstrating the program's effectiveness in equipping individuals with the skills necessary to succeed in the workforce (Abu-Nimer & Smith, 2016, Pasic, 2020). By providing career pathways in high-demand fields, the program helps address the growing need for cybersecurity professionals while also promoting diversity in the tech industry.

In the case of the WiCyS initiative, metrics such as the number of women receiving cybersecurity certifications, the number of job offers extended to participants, and the increase in women pursuing leadership roles in cybersecurity organizations all serve as indicators of the program's success. WiCyS also tracks the long-term impact on participants' careers, with many reporting that the program helped them build a professional network, gain visibility in the cybersecurity field, and secure promotions or leadership positions (Ora, 2016).

For programs like Techbridge Girls, impact metrics include the percentage of participants who go on to pursue STEM degrees and careers. Techbridge Girls also tracks participants' engagement with STEM subjects and their increased confidence in their ability to succeed in tech-related fields. The program's long-term success is evident in the growing number of women and girls who are choosing to study STEM subjects, particularly in underrepresented fields like computer science and engineering (Ora, 2016).

In conclusion, successful initiatives for building digital literacy and cybersecurity awareness among underrepresented groups have made a profound impact on participants, fostering both personal and professional growth. Programs like those offered by the National Digital Inclusion Alliance**,** CompTIA's Creating IT Futures Foundation**,** Women in Cybersecurity**,** and Techbridge Girls provide valuable lessons in how to design effective training and mentorship programs that empower individuals to succeed in the tech industry (Anttila, 2015, Steers & Nardon, 2014). By measuring impact through participant outcomes, knowledge retention, and career advancement, these programs demonstrate the importance of addressing digital literacy and cybersecurity gaps as a means of promoting equity and inclusion in the tech sector. These case studies offer a roadmap for scaling such initiatives and ensuring that underrepresented groups have the opportunity to thrive in the digital economy.

2.5 Impact on the tech industry

Building digital literacy and cybersecurity awareness among underrepresented groups has profound implications for the tech industry. The effort to empower these groups through digital education not only addresses existing gaps in the workforce but also fosters an environment of innovation, security, and resilience. As the tech sector increasingly becomes a cornerstone of the global economy, it is essential to ensure that people from diverse backgrounds can participate in and contribute to the development of digital technologies (Barclay, 2014, Sucher & Cheung, 2015). By enhancing workforce diversity and inclusion, increasing innovation through diverse perspectives, and promoting a more secure and resilient digital ecosystem, the tech industry stands to benefit greatly from the integration of underrepresented groups into its workforce.

The most immediate impact of building digital literacy and cybersecurity awareness is on workforce diversity and inclusion. The tech industry has historically been dominated by a narrow demographic, with women, racial minorities, and individuals from low-income backgrounds facing significant barriers to entry. These barriers can include a lack of access to digital tools, limited educational opportunities, and discrimination or bias in hiring and promotion processes (Bouncken, Brem & Kraus, 2016). By addressing these barriers and providing targeted training and resources, the tech industry can cultivate a more inclusive workforce that reflects the diversity of the broader population. This is critical not only for social equity but also for the growth and competitiveness of the industry. Diverse teams bring a wider range of ideas, experiences, and skills to the table, which can lead to more creative and effective solutions to the challenges

faced by the tech industry. Increased diversity in the workforce also helps to ensure that the technologies being developed are more representative of the needs and experiences of all users, reducing the risk of creating products that unintentionally exclude or harm certain groups.

In addition to enhancing workforce diversity, building digital literacy and cybersecurity awareness increases innovation through the infusion of diverse perspectives. When individuals from different backgrounds are empowered to engage with digital technologies, they bring unique insights and approaches that can spark innovation. This is especially important in the tech industry, where innovation is the key driver of progress. A workforce that reflects a broad range of demographics is more likely to think outside the box and develop novel solutions to complex problems. For example, underrepresented groups may approach challenges in ways that those with more traditional tech backgrounds might overlook (Cletus, *et al*., 2018). Furthermore, diverse perspectives in technology development help ensure that the products and services created are accessible, equitable, and capable of addressing a wider array of consumer needs. As the global market for tech products expands, creating inclusive, innovative solutions will be essential for maintaining competitiveness in an increasingly globalized economy.

One of the most important benefits of empowering underrepresented groups through digital literacy and cybersecurity education is the promotion of a more secure and resilient digital ecosystem. As the world becomes more interconnected and digital threats continue to evolve, cybersecurity has never been more critical. However, the shortage of skilled cybersecurity professionals, particularly from diverse backgrounds, poses a significant challenge to building a secure digital infrastructure (French, 2015, Shakerian, Dehnavi & Shateri, 2016). By equipping individuals from underrepresented groups with cybersecurity awareness and skills, the tech industry can help meet the growing demand for cybersecurity talent. Furthermore, increasing the diversity of cybersecurity professionals ensures that the industry is better equipped to identify and address a wide range of threats. A diverse cybersecurity workforce can approach problems from different angles, improving the ability to detect and mitigate cyber risks (Kreikamp, 2018, Lisak, *et al*., 2016). Additionally, diverse teams are better positioned to anticipate the needs of a global and varied user base, creating more effective and user-centric security solutions.

Despite the clear benefits, there are challenges to effectively implementing programs aimed at building digital literacy and cybersecurity awareness among underrepresented groups. One of the primary barriers is funding. Many individuals from underserved communities lack the financial resources to access digital education and training programs. Even when these programs exist, they can be prohibitively expensive or difficult to access due to transportation, childcare, or other logistical challenges (Gotsis & Grimani, 2016, Nassef & Albasha, 2019). To overcome these financial barriers, it is essential to secure funding from a variety of sources, including government grants, corporate social responsibility programs, and philanthropic organizations. Additionally, partnerships between the public and private sectors can help to pool resources and create programs that are both affordable and widely accessible. By providing scholarships, free or subsidized training, and access to digital tools, these programs can ensure that cost is not a barrier to participation (Kappagomtula, 2017, Ljubica, Dulčić & Aust, 2016).

Outreach also remains a challenge, particularly in reaching individuals who may not be aware of available digital literacy and cybersecurity programs. Many underrepresented groups, especially those in rural or remote areas, may not have access to information about these opportunities, or they may lack the necessary support systems to navigate the complex world of digital education. Addressing this requires targeted outreach efforts that engage community leaders, local organizations, and trusted influencers to spread the word about available training and resources (Griffith & Dunham, 2014, Moran, Abramson & Moran, 2014). This outreach must be tailored to the specific needs and concerns of each community to ensure that individuals are aware of the benefits of digital literacy and cybersecurity awareness, as well as the opportunities for training and education. Digital literacy programs that are community-based and delivered in partnership with local organizations are more likely to succeed because they leverage existing trust networks and cater to the specific needs of the community (Jackson, 2018, Lücke, Kostova & Roth, 2014).

Systemic inequities also pose a significant challenge to the widespread adoption of digital literacy and cybersecurity programs. Many underrepresented groups face additional barriers such as lack of access to reliable internet, inadequate digital infrastructure, and discrimination in the workplace. To address these challenges, policy interventions are required to create an environment that supports digital inclusion (Hajro, Gibson & Pudelko, 2017, Moran & Abramson, 2017). Policymakers should focus on ensuring equitable access to digital tools and resources, particularly for communities that have historically been marginalized in terms of access to technology. This may include initiatives to improve broadband infrastructure in underserved areas, as well as policies that incentivize companies to invest in digital education for underrepresented groups. Additionally, addressing systemic biases within the tech industry itself—through measures such as affirmative hiring practices, diversity quotas, and anti-discrimination training—can help ensure that underrepresented individuals are not only trained in digital literacy and cybersecurity but are also given fair opportunities to advance in the tech workforce (Hutt & Gopalakrishnan, 2020, Luo & Shenkar, 2017).

Another important policy recommendation is the creation of more industry-wide standards for digital literacy and cybersecurity training. By establishing clear benchmarks for digital skills and cybersecurity competencies, governments and industry leaders can ensure that training programs are aligned with the needs of the tech industry. These standards will help improve the quality and consistency of training programs, making it easier for employers to identify qualified candidates and for participants to pursue meaningful careers in the tech field (Hibbert & Hibbert, 2014, Mirza, 2018, Spring, 2017).

In conclusion, building digital literacy and cybersecurity awareness among underrepresented groups has the potential to significantly impact the tech industry. Through enhanced workforce diversity and inclusion, the infusion of diverse perspectives, and the promotion of a more secure and resilient digital ecosystem, empowering underrepresented communities is not only a matter of equity but also a strategic advantage for the tech sector (Hitt, 2016, Malik, 2018). However, addressing the challenges of funding, outreach, and

systemic inequities will require concerted efforts from both the public and private sectors. By overcoming these barriers and implementing policy changes that foster inclusivity and digital equity, we can create a more diverse, innovative, and secure tech industry that benefits everyone (Holvino, 2014). Empowering underrepresented groups with the skills and knowledge to thrive in the digital world will lead to a stronger, more dynamic, and more inclusive future for the tech industry and society at large.

3. Conclusion and Recommendations

In conclusion, the framework for building digital literacy and cybersecurity awareness among underrepresented groups has significant benefits and far-reaching impacts for both individuals and the tech industry. By focusing on providing essential digital skills and fostering a deep understanding of cybersecurity, this approach not only empowers individuals from diverse backgrounds but also contributes to creating a more inclusive and resilient workforce. The efforts to bridge the digital divide enable underrepresented groups to access opportunities, engage with the digital economy, and contribute to the development of secure and innovative technologies. Additionally, increasing diversity in the tech industry enhances innovation by bringing in a wider range of perspectives, helping to develop more effective solutions that meet the needs of a global user base.

Empowering underrepresented groups in the tech industry also has long-term societal benefits, particularly in terms of economic mobility and workforce security. Digital literacy opens doors to a wide range of careers, and cybersecurity awareness ensures individuals are better equipped to navigate and protect themselves in the increasingly complex digital environment. These initiatives not only help individuals secure stable jobs but also create a more secure digital ecosystem, where diverse professionals can collaborate to address emerging cyber threats and enhance the overall security of the digital world.

To expand digital literacy and cybersecurity awareness initiatives, several practical recommendations should be considered. First, a stronger partnership between public institutions, private companies, and community organizations is crucial. By pooling resources, expertise, and networks, these collaborations can help ensure that digital education reaches the communities most in need. Public-private partnerships can also help provide funding for scholarships, infrastructure improvements, and access to cutting-edge technology for underserved populations. Additionally, designing training programs that are flexible, culturally relevant, and accessible is critical. Offering a mix of in-person and online options, along with ensuring that resources are available in multiple languages, can significantly increase participation rates. Programs should be designed to meet the specific needs of each community, taking into account local challenges such as language barriers, limited internet access, and varying levels of digital readiness.

Moreover, creating mentorship and peer support networks within these programs can provide valuable guidance and encouragement. Connecting individuals with role models and mentors who share similar backgrounds can foster confidence and help bridge the gap between learning and real-world application. These networks also provide ongoing support, which is essential for retaining participants and helping them succeed in the workforce. Finally, policies at the local, regional, and national levels should be crafted to support the integration of digital education into broader social and economic strategies. This could include offering tax incentives for companies that invest in digital education or creating policies that ensure equitable access to the internet and digital devices in underserved areas.

For future directions in research and program development, it is important to continue evaluating the effectiveness of existing programs and identifying best practices. Research should focus on understanding the specific barriers faced by underrepresented groups in different regions and contexts and how these barriers can be overcome. Data-driven insights into participant outcomes, knowledge retention, and career advancement will help refine and enhance the design of these programs. Additionally, as technology continues to evolve, ongoing updates to digital literacy and cybersecurity curricula will be necessary to ensure that individuals are equipped with the latest skills and knowledge.

Exploring new forms of collaboration between academia, industry, and government can also provide fresh insights into how to scale successful initiatives. Future research should investigate the role of artificial intelligence, blockchain, and other emerging technologies in shaping digital literacy and cybersecurity training. By understanding how these technologies can be integrated into training programs, we can better prepare individuals to navigate the complexities of the digital landscape and address future challenges in cybersecurity.

In summary, building digital literacy and cybersecurity awareness is essential for empowering underrepresented groups in the tech industry. It provides individuals with the skills and knowledge needed to participate fully in the digital economy, enhances diversity in the workforce, and promotes a more secure digital environment. By expanding these initiatives and addressing the unique needs of different communities, we can create a more inclusive and resilient tech industry. Furthermore, continued research and development of innovative programs will ensure that the benefits of digital education and cybersecurity awareness are accessible to all, paving the way for a more equitable and secure future in the tech sector.

4. References

1. Abdallah WM, Alnamri M. Non-financial performance measures and the BSC of multinational companies with multi-cultural environment: An empirical investigation. Cross Cultural Management. 2015;22(4):594-607.
2. Abu-Nimer M, Smith RK. Interreligious and intercultural education for dialogue, peace and social cohesion. International Review of Education. 2016;62:393-405.
3. Adrion W, Biskup S, Boisvert D, Clarke L, Fountain J, Grocer P, *et al*. Broadening participation in computing: K12-community-college-university-graduate pathways. S4F-15-S4F-20. 2008. doi:10.1109/fie.2008.4720489.
4. Adrion W, Fall R, Matos M, Peterfreund A. Integrating evaluation into program development. 2010. doi:10.1145/1734263.1734273.
5. Al-Ali R, Kathiresan N, El Anbari M, Schendel ER, Zaid TA. Workflow optimization of performance and quality of service for bioinformatics application in high performance computing. Journal of Computational Science. 2016;15:3-10.
6. Alam M, Zou PX, Stewart RA, Bertone E, Sahin O,

Buntine C, *et al*. Government championed strategies to overcome the barriers to public building energy efficiency retrofit projects. Sustainable Cities and Society. 2019;44:56-69.
7. Alessa L, Kliskey A, Gamble J, Fidel M, Beaujean G, Gosz J. The role of Indigenous science and local knowledge in integrated observing systems: moving toward adaptive capacity indices and early warning systems. Sustainability Science. 2016;11:91-102.
8. Al-Hajji H, Khan S. Keeping oil & gas EPC major projects under control: strategic & innovative project management practices. In: Abu Dhabi International Petroleum Exhibition and Conference. 2016. p. D021S033R003.
9. Anttila J. Multicultural team leadership in an MNC: a middle manager's perspective [Master's thesis]. 2015.
10. Arundel A, Bloch C, Ferguson B. Advancing innovation in the public sector: Aligning innovation measurement with policy goals. Research Policy. 2019;48(3):789-98.
11. Asch M, Moore T, Badia R, Beck M, Beckman P, Bidot T, *et al*. Big data and extreme-scale computing: Pathways to convergence-toward a shaping strategy for a future software and data ecosystem for scientific inquiry. The International Journal of High Performance Computing Applications. 2018;32(4):435-79.
12. Bae MJ, Park YS. Biological early warning system based on the responses of aquatic organisms to disturbances: a review. Science of the Total Environment. 2014;466:635-49.
13. Bagchi-Sen S, Rao HR, Upadhyaya SJ, Chai S. Women in cybersecurity: A study of career advancement. IT Professional. 2010;12(1):24-31.
14. Barclay J. Conscious culture: How to build a high performing workplace through values, ethics, and leadership. Morgan James Publishing. 2014.
15. Bhaskaran SV. Integrating Data Quality Services (DQS) in Big Data Ecosystems: Challenges, Best Practices, and Opportunities for Decision-Making. Journal of Applied Big Data Analytics, Decision-Making, and Predictive Modelling Systems. 2020;4(11):1-12.
16. Bitter J. Improving multidisciplinary teamwork in preoperative scheduling [Doctoral dissertation]. 2017.
17. Boda VVR, Immaneni J. Streamlining FinTech Operations: The Power of SysOps and Smart Automation. Innovative Computer Sciences Journal. 2019;5(1).
18. Bouncken R, Brem A, Kraus S. Multi-cultural teams as sources for creativity and innovation: The role of cultural diversity on team performance. International Journal of Innovation Management. 2016;20(01):1650012.
19. Brough M, Literat I, Ikin A. "Good social media?": underrepresented youth perspectives on the ethical and equitable design of social media platforms. 2020. doi:10.32376/3f8575cb.16df1b21.
20. Castro R. Blended learning in higher education: Trends and capabilities. Education and Information Technologies. 2019;24(4):2523-46.
21. Chan N. Building Information Modelling: An analysis of the methods used to streamline design-to-construction in New Zealand [Doctoral dissertation]. Open Access Te Herenga Waka-Victoria University of Wellington; 2020.
22. Chandarman R, Niekerk B. Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication. 2017;(20). doi:10.23962/10539/23572.
23. Charleston L. A qualitative investigation of African Americans' decision to pursue computing science degrees: implications for cultivating career choice and aspiration. Journal of Diversity in Higher Education. 2012;5(4):222-43. doi:10.1037/a0028918.
24. Chen Q, Hall DM, Adey BT, Haas CT. Identifying enablers for coordination across construction supply chain processes: a systematic literature review. Engineering, Construction and Architectural Management. 2020;28(4):1083-1113.
25. Cletus HE, Mahmood NA, Umar A, Ibrahim AD. Prospects and challenges of workplace diversity in modern-day organizations: A critical review. HOLISTICA–Journal of Business and Public Administration. 2018;9(2):35-52.
26. Davis JE. Temporal meta-model framework for Enterprise Information Systems (EIS) development [Doctoral dissertation]. Curtin University; 2014.
27. Ebrahim A, Battilana J, Mair J. The governance of social enterprises: Mission drift and accountability challenges in hybrid organizations. Research in Organizational Behavior. 2014;34:81-100.
28. French R. Cross-cultural management in work organisations. Kogan Page Publishers. 2015.
29. Barcellos J. Critical elements of a successful project. 2019.
30. Gotsis G, Grimani K. Diversity as an aspect of effective leadership: Integrating and moving forward. Leadership & Organization Development Journal. 2016;37(2):241-64.
31. Griffith BA, Dunham EB. Working in teams: Moving from high potential to high performance. Sage Publications. 2014.
32. Habibi M, Kermanshachi S, Rouhanizadeh B. Identifying and measuring engineering, procurement, and construction (EPC) key performance indicators and management strategies. Infrastructures. 2019;4(2):14.
33. Hajro A, Gibson CB, Pudelko M. Knowledge exchange processes in multicultural teams: Linking organizational diversity climates to teams' effectiveness. Academy of Management Journal. 2017;60(1):345-72.
34. Hibbert E, Hibbert R. Leading multicultural teams. William Carey Publishing. 2014.
35. Hitt MA. International strategy and institutional environments. Cross Cultural & Strategic Management. 2016;23(2).
36. Holvino E. Developing multicultural organizations. The NTL Handbook of Organization Development and Change. 2014:517-34.
37. Hossain MD. Performance evaluation of procurement system in ICT Industry: a case study. 2018.
38. Hutt C, Gopalakrishnan S. Leadership humility and managing a multicultural workforce. South Asian Journal of Business Studies. 2020;9(2):251-60.
39. Ibrahim II. Project planning in construction procurement: the case of Nigerian indigenous contractors [Doctoral dissertation]. 2015.
40. Jackson J. Preparing students for the global workplace: The impact of a semester abroad. In: Language and Intercultural Communication in the Workplace. Routledge; 2018. p. 88-103.
41. Jones CL, Golanz B, Draper GT, Janusz P. Practical Software and Systems Measurement Continuous

Iterative Development Measurement Framework. Version. 2020;1:15.
42. Kabirifar K, Mojtahedi M. The impact of engineering, procurement, and construction (EPC) phases on project performance: A case of a large-scale residential construction project. Buildings. 2019;9(1):15.
43. Kappagomtula CL. Overcoming challenges in leadership roles–managing large projects with multi- or cross-culture teams. European Business Review. 2017;29(5):572-83.
44. Kortjan N, Von Solms R. A conceptual framework for cyber-security awareness and education in SA. South African Computer Journal. 2014;52(1):29-41.
45. Koyuncu M, Pusatli Ö. Security awareness level of smartphone users: An exploratory case study. Mobile Information Systems. 2019;2019:1-11. doi:10.1155/2019/2786913.
46. Kreikamp R. The benefits of applying cultural intelligence concepts to customer satisfaction and team performance [Doctoral dissertation]. Middlesex University; 2018.
47. Kuerbis A, Mulliken A, Muench F, Moore A, Gardner D. Older adults and mobile technology: Factors that enhance and inhibit utilization in the context of behavioral health. Mental Health and Addiction Research. 2017;2(2). doi:10.15761/mhar.1000136.
48. Lisak A, Erez M, Sui Y, Lee C. The positive role of global leaders in enhancing multicultural team innovation. Journal of International Business Studies. 2016;47:655-73.
49. Liu T, Wang Y, Wilkinson S. Identifying critical factors affecting the effectiveness and efficiency of tendering processes in Public–Private Partnerships (PPPs): A comparative analysis of Australia and China. International Journal of Project Management. 2016;34(4):701-16.
50. Ljubica J, Dulčić Ž, Aust I. Linking individual and organizational cultural competences: One step closer to multicultural organization. Management: Journal of Contemporary Management Issues. 2016;21(Special issue):51-82.
51. Lücke G, Kostova T, Roth K. Multiculturalism from a cognitive perspective: Patterns and implications. Journal of International Business Studies. 2014;45:169-90.
52. Luo Y, Shenkar O. The multinational corporation as a multilingual community: Language and organization in a global context. Language in International Business: Developing a Field. 2017;59-92.
53. Malik RS. Educational challenges in the 21st century and sustainable development. Journal of Sustainable Development Education and Research. 2018;2(1):9-20.
54. Malloy A, Smith Y. Retaining and advancing underrepresented women in technology: Insights from ITSMF emerge survey and focus group. 2019. doi:10.28945/4353.
55. Micheli GJ, Cagno E. The role of procurement in performance deviation recovery in large EPC projects. International Journal of Engineering Business Management. 2016;8:1847979016675302.
56. Mirza MA. Project Management and Leadership Challenges, Volume III: Respecting Diversity, Building Team Meaningfulness, and Growing to Leadership Roles. Business Expert Press. 2018.
57. Mohanty SP, Choppali U, Kougianos E. Everything you wanted to know about smart cities: The Internet of Things is the backbone. IEEE Consumer Electronics Magazine. 2016;5(3):60-70.
58. Montgomery B. Book review: Fostering success of ethnic and racial minorities in STEM: The role of minority-serving institutions. International Journal of Multicultural Education. 2013;15(2). doi:10.18251/ijme.v15i2.743.
59. Moran RT, Abramson NR. Managing cultural differences: Global leadership for the 21st century. Routledge. 2017.
60. Moran RT, Abramson NR, Moran SV. Managing cultural differences. Routledge. 2014.
61. Nassef A, Albasha H. Best Leadership Style to Lead Multi-Cultural Teams of Service Companies in the Oil & Gas Industry in the Arabian Gulf. In: SPE Middle East Oil and Gas Show and Conference; 2019. p. D021S011R002.
62. Nguyen HT, Hadikusumo BH. Human resource-related factors and engineering, procurement, and construction (EPC) project success. Journal of Financial Management of Property and Construction. 2018;23(1):24-39.
63. Olufemi-Phillips AQ, Ofodile OC, Toromade AS, Eyo-Udo NL, Adewale TT. Optimizing FMCG supply chain management with IoT and cloud computing integration. International Journal of Management & Entrepreneurship Research. 2020;6(11).
64. Ora E. Effective leadership and management of a multicultural team: Case: Radisson Blu Resort & Spa, Malta Golden Sands [Master's thesis]. 2016.
65. Ordanini A, Parasuraman A, Rubera G. When the recipe is more important than the ingredients: A qualitative comparative analysis (QCA) of service innovation configurations. Journal of Service Research. 2014;17(2):134-49.
66. Osei-Kyei R, Chan AP. Review of studies on the Critical Success Factors for Public–Private Partnership (PPP) projects from 1990 to 2013. International Journal of Project Management. 2015;33(6):1335-46.
67. Osland JS. An overview of the global leadership literature. In: Global Leadership. 2017. p. 57-116.
68. Pace ML, Carpenter SR, Cole JJ. With and without warning: Managing ecosystems in a changing world. Frontiers in Ecology and the Environment. 2015;13(9):460-7.
69. Pal R, Wang P, Liang X. The critical factors in managing relationships in international engineering, procurement, and construction (IEPC) projects of Chinese organizations. International Journal of Project Management. 2017;35(7):1225-37.
70. Panda D, Sahu GP. E-procurement implementation: Comparative study of governments of Andhra Pradesh and Chhattisgarh. SSRN. 2014.
71. Pasic A. Cultural diversity impact on the decision-making of leaders within organizations [Master's thesis]. 2020.
72. Patel A, Alhussian H, Pedersen JM, Bounabat B, Júnior JC, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. Computers & Security. 2017;64:92-109.
73. Pulwarty RS, Sivakumar MV. Information systems in a changing climate: Early warnings and drought risk management. Weather and Climate Extremes. 2014;3:14-21.

74. Rahman N, Sairi I, Zizi N, Khalid F. The importance of cybersecurity education in school. International Journal of Information and Education Technology. 2020;10(5):378-82. doi:10.18178/ijiet.2020.10.5.1393.
75. Ren J, Guo Y, Zhang D, Liu Q, Zhang Y. Distributed and efficient object detection in edge computing: Challenges and solutions. IEEE Network. 2018;32(6):137-43.
76. Rico R, Hinsz VB, Davison RB, Salas E. Structural influences upon coordination and performance in multiteam systems. Human Resource Management Review. 2018;28(4):332-46.
77. Roden S, Nucciarelli A, Li F, Graham G. Big data and the transformation of operations models: A framework and a new research agenda. Production Planning & Control. 2017;28(11-12):929-44.
78. Rogers K. Creating a culture of data-driven decision-making [Master's thesis]. Liberty University; 2020.
79. Ross DF. Procurement and supplier management. In: Distribution Planning and Control: Managing in the Era of Supply Chain Management. 2015. p. 531-604.
80. Roth S, Valentinov V, Kaivo-Oja J, Dana LP. Multifunctional organisation models: A systems-theoretical framework for new venture discovery and creation. Journal of Organizational Change Management. 2018;31(7):1383-400.
81. Ruiz E. Underrepresented groups and constitution-making: the Mexico City case. Political Studies Review. 2020;19(2):164-70. doi:10.1177/1478929920944825.
82. Salamkar MA, Allam K. Data Lakes Vs. Data Warehouses: Comparative Analysis on When to Use Each, With Case Studies Illustrating Successful Implementations. Distributed Learning and Broad Applications in Scientific Research. 2019;5.
83. Sandilya SK, Varghese K. A study of delays in procurement of engineered equipment for engineering, procurement and construction (EPC) projects in India: A mixed method research approach. 2016.
84. Santoni G. Standardized cross-functional communication as a robust design tool: Mitigating variation, saving costs, and reducing the New Product Development Process' lead time by optimizing the information flow [Doctoral dissertation]. Politecnico di Torino; 2019.
85. Saubari N, Baharuddin MF. Digital literacy awareness among students. Research Hub. 2016;2(1):57-63.
86. Sebastian IM, Ross JW, Beath C, Mocker M, Moloney KG, Fonstad NO. How big old companies navigate digital transformation. In: Strategic Information Management. Routledge; 2020. p. 133-50.
87. Shakerian H, Dehnavi HD, Shateri F. A framework for the implementation of knowledge management in supply chain management. Procedia-Social and Behavioral Sciences. 2016;230:176-83.
88. Shaw T, McGregor D, Brunner M, Keep M, Janssen A, Barnet S. What is eHealth (6)? Development of a conceptual model for eHealth: Qualitative study with key informants. Journal of Medical Internet Research. 2017;19(10):e324.
89. Silwimba S. An investigation into the effects of procurement methods on project delivery in the Zambian road sector [Doctoral dissertation]. The University of Zambia; 2019.
90. Singh A, Chatterjee K. Cloud security issues and challenges: A survey. Journal of Network and Computer Applications. 2017;79:88-115.
91. Singh SP, Nayyar A, Kumar R, Sharma A. Fog computing: From architecture to edge computing and big data processing. The Journal of Supercomputing. 2019;75:2070-105.
92. Skelton M, Pais M. Team Topologies: Organizing Business and Technology Teams for Fast Flow. IT Revolution; 2019.
93. Soni P, Krishnan RT. Frugal innovation: Aligning theory, practice, and public policy. Journal of Indian Business Research. 2014;6(1):29-47.
94. Steers RM, Nardon L. Managing in the Global Economy. Routledge; 2014.
95. Steyn M. Organisational benefits and implementation challenges of mandatory integrated reporting: Perspectives of senior executives at South African listed companies. Sustainability Accounting, Management and Policy Journal. 2014;5(4):476-503.
96. Stone M, Aravopoulou E, Gerardi G, Todeva E, Weinzierl L, Laughlin P, *et al*. How platforms are transforming customer information management. The Bottom Line. 2017;30(3):216-35.
97. Sucher W, Cheung C. The relationship between hotel employees' cross-cultural competency and team performance in multi-national hotel companies. International Journal of Hospitality Management. 2015;49:93-104.
98. Sun Y, Zhang J, Xiong Y, Zhu G. Data security and privacy in cloud computing. International Journal of Distributed Sensor Networks. 2014;10(7):190903.
99. Syed J, Mahmood SKA, Zulfiqar A, Sharif M, Sethi UI, Ikram U, *et al*. The construction sector value chain in Pakistan and the Sahiwal coal power project. In: China's Belt and Road Initiative in a Global Context: Volume II: The China Pakistan Economic Corridor and its Implications for Business. 2020. p. 271-87.
100. Tang P, Yilmaz A, Cooke N. Automatic imagery data analysis for proactive computer-based workflow management during nuclear power plant outages (No. 15-8121). Arizona State Univ.; 2018.
101. Tariq N, Asim M, Al-Obeidat F, Zubair Farooqi M, Baker T, Hammoudeh M, *et al*. The security of big data in fog-enabled IoT applications including blockchain: A survey. Sensors. 2019;19(8):1788.
102. Tezel A, Papadonikolaki E, Yitmen I, Hilletofth P. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management. 2020;7:547-63.
103. Thamrin DAF. Six Sigma Implementation and Integration within Project Management Framework in Engineering, Procurement, and Construction Projects: A Case Study in a Southeast Asian Engineering, Procurement, and Construction Company. 2017.
104. Thumburu SKR. Integrating SAP with EDI: Strategies and Insights. MZ Computing Journal. 2020;1(1).
105. Toutounchian S, Abbaspour M, Dana T, Abedi Z. Design of a safety cost estimation parametric model in oil and gas engineering, procurement and construction contracts. Safety Science. 2018;106:35-46.
106. Tuli FA, Varghese A, Ande JRP. Data-Driven Decision Making: A Framework for Integrating Workforce Analytics and Predictive HR Metrics in Digitalized Environments. Global Disclosure of Economics and

Business. 2018;7(2):109-22.
107. Van Zyl ES, Mathafena RB, Ras J. The development of a talent management framework for the private sector. SA Journal of Human Resource Management. 2017;15(1):1-19.
108. Vehviläinen T. Improving process efficiency and supply chain management by taking advantage of digitalization-based procurement tools. 2019.
109. Vilasini N, Neitzert TR, Rotimi JO. Correlation between construction procurement methods and lean principles. International Journal of Construction Management. 2011;11(4):65-78.
110. Vlietland J, Van Solingen R, Van Vliet H. Aligning codependent Scrum teams to enable fast business value delivery: A governance framework and set of intervention actions. Journal of Systems and Software. 2016;113:418-29.
111. Watson R, Wilson HN, Smart P, Macdonald EK. Harnessing difference: A capability-based framework for stakeholder engagement in environmental innovation. Journal of Product Innovation Management. 2018;35(2):254-79.
112. Whitehead J. Prioritizing sustainability indicators: Using materiality analysis to guide sustainability assessment and strategy. Business Strategy and the Environment. 2017;26(3):399-412.
113. Yu W, Dillon T, Mostafa F, Rahayu W, Liu Y. A global manufacturing big data ecosystem for fault detection in predictive maintenance. IEEE Transactions on Industrial Informatics. 2019;16(1):183-92.
114. Zhang C, Tang P, Cooke N, Buchanan V, Yilmaz A, Germain SWS, *et al*. Human-centered automation for resilient nuclear power plant outage control. Automation in Construction. 2017;82:179-92.
115. Zou M, Vogel-Heuser B, Sollfrank M, Fischer J. A cross-disciplinary model-based systems engineering workflow of automated production systems leveraging socio-technical aspects. In: 2020 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). IEEE; 2020. p. 133-40.