IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 11 Issue 12, December 2024
ISSN (Online) 2348 – 7968 | Impact Factor – 6.72
www.ijiset.com

Impact of Cybersecurity Skills Gap on the U.S. Economy and National Security

Babatope Olosunde
Cybersecurity, United Kingdom, 0009-0002-1923-570X

ABSTRACT
The increasing cases of cyberattacks have made it a point of focus for many researchers as it now targets larger organizations. These attacks not only result in financial disruptions but also affect the organization's reputation and third-party firms in relation to the organization. However, with the growing recognition of the effect of cyberattacks on organizations, third-party firms, and people, there is still a significant skill gap in dealing with imminent threats. While the U.S. has experienced a considerable drop in the number of available cybersecurity roles in the past years, the number of organizations lacking or seeking a cybersecurity expert is still rising.
This study uses secondary data and analysis to review the impacts of the cybersecurity skills gap on the U.S. economy and national security. The study, which limited the secondary sources used to the last 5 years, revealed that the U.S. economy and national security are intertwined, making cybersecurity in the digital world a critical aspect. The finding also indicated a need for collaboration between private and public sectors to address the skills gap issue. Lastly, as different sectors have different attacks, there is a need to develop sector-specific initiatives that address the lack of skilled cybersecurity experts.

1.0 INTRODUCTION
Cybersecurity involves protecting networks, devices, and data from unauthorized entry from third parties for criminal use (Blažič, 2021). Angafor, Yevseyeva, and He (2020) also explained that cybersecurity involves protecting the confidentiality, integrity, and availability of information. Thus, cybersecurity skills are the minimum set of skills required by professionals to secure every element of an organization's infrastructure and withstand threats that compromise the security and continuity of operations (Aaltola, Ruoslahti, and Heinonen, 2022). Similarly, Carlton and Levy (2017) defined cybersecurity skills as competencies that skilled individuals must possess to mitigate or avoid the complexity and seriousness that accompany cyber threats. In summary, cybersecurity skills are the individual proficiencies that help minimize the impact or likelihood of security incidents occurring, which can often lead to compromising information assets (Hodson, 2021).
The U.S. economy and national security are intertwined (Benson and Mouradian, 2023), as the economic foundation is essential for protecting the nation's authority, infrastructure, and citizens. Commerce.gov (2022) explained that economic security includes producing and protecting vital technologies, resources, and industries. All this helps to build resilience against external threats such as cybercrime, intellectual property theft, and unfair trade practices. Slawotsky (2024) explained that national security extends beyond military strength but relies heavily on economic systems' stability and innovation to support defense capabilities and critical services.
In the 21st century, cybersecurity is a cornerstone of economic and national security (Commerce.gov, 2022). The increasing digitization of industries, from energy to critical manufacturing, has created interconnected networks vulnerable to cyber threats. These threats include cybercriminals aiming for financial disruption, state-sponsored hackers targeting

intellectual property, and cyber terrorists seeking to destabilize essential systems (Benson and Mouradian, 2023). Hence, cybersecurity breaches can compromise trade, infrastructure, and public safety, declining the nation's competitive edge and security. Therefore, to strengthen economic and national security, the U.S. must address vulnerabilities in its digital ecosystem, enforce trade and security laws, and enhance public safety infrastructure (Garaja, 2022; Luo, 2021). These measures collectively protect economic prosperity while safeguarding against evolving threats in a globally connected world.

According to Forbes (2024), a deficit of 4 million vacancies for cybersecurity jobs exists worldwide. In the US, despite having nearly 25% of the global cybersecurity workforce, over 755,743 cybersecurity job openings remained unfilled in the U.S. (Statista, 2024). This shortage leaves organizations vulnerable to cyberattacks, with the average data breach costing U.S. businesses $9.34 million, the highest globally (Petrosyan, 2024). Benson and Mouradian (2023) explained that the inability to fill critical roles delays the implementation of effective cybersecurity measures, thereby increasing the risk of financial losses, reputational damage, and regulatory penalties.

Operationally, the cybersecurity skills shortage impacts critical areas such as cloud security, artificial intelligence (AI), and zero-trust architecture (Commerce.gov, 2022). However, these are skills in high demand as organizations adopt advanced technologies. Additionally, companies have reported a gap in soft skills, like communication and leadership, further complicating collaboration and comprehensive security planning (Poláková et al., 2023). This is particularly concerning for sectors like healthcare and energy, where cyber threats could disrupt essential services and national infrastructure (Singh, Mandal, and Purohit, 2023).

In 2023, the average cost of a data breach in the U.S. was $9.48 million, the highest globally (IBM, 2024). High-profile incidents, such as the Colonial Pipeline ransomware attack, disrupted fuel supplies and incurred costs exceeding $4.4 million in ransom payments alone, highlighting vulnerabilities in critical infrastructure (Amorosa and Yankson, 2023). The impact of such attacks leads to a decline in consumer trust and imposes regulatory penalties, compounding financial losses for businesses.

That said, the U.S. cybersecurity sector is one of the most advanced globally, driven by rapid digital transformation and escalating cyber threats (Burrell, 2018). With nearly 1.4 million professionals in 2023, the U.S. accounted for about 25% of the global cybersecurity workforce (Statista, 2023). Key focus areas include cloud security, artificial intelligence (AI), zero-trust frameworks, and advanced threat detection (Benson and Mouradian, 2023). Critical sectors like healthcare, energy, and government heavily rely on robust cybersecurity to safeguard sensitive data and infrastructure, making the industry vital to national security and economic resilience (Poláková et al., 2023).

The U.S. cybersecurity sector also remains a cornerstone of the national economy, safeguarding critical industries, fostering innovation, and generating significant economic value (Aaltola, Ruoslahti, and Heinonen, 2022). In 2023, the sector contributed approximately $200 billion to the U.S. GDP, reflecting its vital role in protecting over $20 trillion worth of economic output across finance, healthcare, and energy industries (Statista, 2024). According to Statista, the global cybersecurity market is projected to reach $500 billion by 2030, with the U.S. leading investments in advanced technologies like AI, cloud security, and zero-trust architectures.

However, with over 755,000 unfilled cybersecurity positions in 2023, critical sectors like healthcare and energy are exposed to increased cyber threats, causing financial losses, operational disruptions, and heightened vulnerabilities to attacks. The study explores this gap's economic and

security consequences, focusing on its effects on infrastructure and defense against evolving cyber threats. It also investigates strategies such as workforce training, advanced technologies, and public-private collaborations to address the shortage and enhance the U.S.'s economic resilience and national security capabilities.

2.0 LITERATURE REVIEW

Recent literature highlights the critical need for expertise in artificial intelligence (AI), cloud security, and zero-trust architecture, reflecting the evolving threat landscape (Benson and Mouradian, 2023). For instance, the Ponemon Institute reports that AI and machine learning applications in cybersecurity have become essential for proactive threat detection and response (BobSulli, 2024). The global cybersecurity workforce reached 5.5 million professionals in 2023, yet there were 3.4 million unfilled positions, with the U.S. accounting for approximately 755,743 vacancies (Statista, 2024).

There is a pronounced skills mismatch, with employers struggling to find talent proficient in cutting-edge technologies like cloud computing (Cappelli, 2024). A LinkedIn Workforce Report (2024) showed a decline in the demand for cybersecurity-related jobs in countries including Italy, Brazil, Canada, and the United States. The report attributed this decline to the growing cybersecurity workforce in these countries. Statista (2023) also explained that the cybersecurity skill gap is not just technical but also reflects a lack of soft skills such as communication and leadership.

Addressing this gap includes utilizing government-led initiatives such as the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) workforce development programs (Angafor, Yevseyeva, and He, 2020). These initiatives aim to diversify the talent pool by engaging underrepresented groups, including women and minorities (Catal et al., 2022). Similarly, private sector programs support this movement by offering certifications in specialized areas like ethical hacking and risk management to meet the cybersecurity demands of the job market (Juneja, Goswami, and Mondal, 2024). While these efforts are a step in the right direction, with the LinkedIn survey showing a decline in cybersecurity job posts, there is still a large gap to fill (LinkedIn, 2024). Catal et al. (2022) explained that many training programs lack adaptability to the fast-evolving cybersecurity landscape, leaving graduates underprepared for real-world scenarios.

The role of higher education institutions is also evolving, with universities incorporating cybersecurity courses and research opportunities (Sinha and Lee, 2024). However, Mohamed Hashim, Tlemsani, and Matthews (2021) pointed out that curricula often lag behind industry demands, particularly in integrating skills like AI programming. Still, the partnerships between tech firms and universities have produced tailored programs focusing on immediate skill requirements (Mukherjee et al., 2024). Despite progress, there is a need to align the training programs with technological trends and organizational needs. Without such alignment, the cybersecurity skills gap will continue to grow, leaving critical systems and infrastructure vulnerable (Sinha and Lee, 2024; Mukherjee et al., 2024).

Globally, the cybersecurity skills gap significantly affects developed and developing nations (BobSulli, 2024). IBM (2024) observed that organizations with understaffed cybersecurity teams experience data breaches costing an average of $1 million more than those with adequate staffing. Apart from the cost effects, such breaches often disrupt operations, tarnish reputations, and result in financial losses, revealing the critical role skilled cybersecurity experts play (Petrosyan, 2024). Industries in China, the most significant contributor to the global skills gap with 1.7 million

unfilled roles, face delays in implementing robust cybersecurity measures, leading to increased vulnerability (Statista, 2023). India comes close to China, which has an 800,000-role deficit and has reported similar challenges, especially in sectors like IT and banking. This suggests a global trend where industries cannot respond adequately to escalating threats due to insufficient talent (Sinha and Lee, 2024). Furthermore, ICS2 (2023) suggested that understaffed organizations often depend on external consultants, significantly increasing operational costs and delaying response times.

Developing nations face unique challenges, including limited access to advanced training and resources (Sinha and Lee, 2024). Catal et al. (2022) explained that this dependency on foreign expertise limits their ability to establish sustainable, local cybersecurity ecosystems. For instance, African countries struggle to retain talent due to competitive global markets that attract skilled professionals to higher-paying jobs abroad (Mazlan and Jambulingam, 2023).

In the U.S., the skills gap significantly impacts critical infrastructure sectors such as healthcare, energy, and transportation (Mazlan and Jambulingam, 2023). Petrosyan (2024) revealed that nearly 40% of healthcare organizations reported shortages in cybersecurity personnel, leaving sensitive patient data vulnerable to breaches. The energy sector, often targeted by state-sponsored attacks, also struggles with a lack of expertise in securing operational technologies (Poláková et al., 2023). These vulnerabilities lead to economic losses and increase the risk of cascading effects that could disrupt other sectors reliant on these critical services (Amorosa and Yankson, 2023).

Globally, the increasing sophistication of cyber threats, including ransomware and supply chain attacks, further strains limited cybersecurity resources (Petrosyan, 2024). ICS2 (2023) revealed that organizations lacking robust cybersecurity teams often take weeks longer to recover from attacks, leading to financial and operational damages. Efforts to address these issues include international collaborations and government-led initiatives to improve cybersecurity awareness and education (Angafor, Yevseyeva, and He, 2020; Sinha and Lee, 2024). For example, the European Union's Cybersecurity Act has established certification frameworks to standardize and enhance workforce competencies (ENISA, 2021). However, there is an argument that such initiatives often fail to address the root causes of skills shortages, including inadequate early education in STEM fields (Mukherjee et al., 2024).

The cybersecurity skills gap that the U.S. faces has led to economic and national security challenges. Financially, IBM (2024) reported that the average data breach cost in the U.S. is $9.48 million, the highest globally. High-profile incidents, such as the Colonial Pipeline ransomware attack in 2021, show the vulnerabilities that arise from insufficient staffing and a lack of expertise in cybersecurity skills (Blažič, 2021). This attack disrupted fuel supplies across the East Coast, led to financial losses exceeding $4 million, and exposed the fragile state of critical infrastructure systems (Statista, 2024).

Industries like healthcare and energy are particularly affected, with implications for national resilience (Cappelli, 2024). Healthcare organizations reported a high incidence of ransomware attacks, with staffing shortages taking the lead as one of the factors that delay detection and recovery (Poláková et al., 2023). Similarly, the energy sector faces challenges in protecting operational technologies essential for power distribution and grid management (Singh, Mandal, and Purohit, 2023). These vulnerabilities lead to economic losses and increase the risk of other effects that could disrupt other sectors reliant on these critical services (BobSulli, 2024).

From a national security perspective, the skills gap limits the U.S.'s ability to counter sophisticated cyber threats from adversaries. State.gov (2023) emphasized that state-sponsored actors increasingly target U.S. infrastructure, exploiting weaknesses caused by insufficient cybersecurity

staffing. These attacks aim to disrupt operations, steal sensitive information, and undermine public trust (Petrosyan, 2024). For example, cyberattacks on election systems have raised concerns about the integrity of democratic processes, showing the intersection of cybersecurity and national security (State.gov, 2023).

Efforts to address these challenges have included public-private partnerships and federal programs to build a robust cybersecurity workforce (BobSulli, 2024). Initiatives like the CyberCorps: Scholarship for Service program provide financial incentives for students pursuing cybersecurity careers, emphasizing public sector roles (ICS2, 2023). The Department of Energy has also launched initiatives to enhance workforce capabilities specific to securing energy infrastructure (ENISA, 2021).

Despite these measures, there are still gaps in strategy and execution (Sinha and Lee, 2024). For instance, training programs often fail to address emerging threats like quantum computing and AI-driven attacks, leaving critical systems vulnerable (Mukherjee et al., 2024). Furthermore, the skills gap contributes to economic inefficiencies, with industries spending billions annually on external consultants to fill staffing shortages (Luo, 2021). To address these challenges, there is a need for a multi-faceted approach that combines education reform, workforce development, and international collaboration.

Slawotsky (2024) suggested developing programs that provide professionals with practical skills in high-demand areas, including cloud security, AI, and machine learning. Additionally, initiatives need to incentivize the recruitment of cybersecurity talent into government and critical infrastructure sectors (Mukherjee et al., 2024). Furthermore, a coordinated effort from both the public and private sectors to tackle the cybersecurity skills gap is essential.

3.0 METHODOLOGY

This study's research sources were extracted from academic databases, government reports, industry publications, and reliable news outlets. The research primarily used databases such as Google Scholar, JSTOR, and Scopus to search peer-reviewed articles, white papers, and government reports on cybersecurity workforce gaps, skills shortages, and related topics. The following Boolean search strings were used to filter relevant studies: "Cybersecurity skills gap" OR "Cybersecurity workforce shortage" AND “workforce development" OR "training programs" AND "impact" OR "economic stability" OR "national security.” The focus was on recent publications from the last 5 years to ensure the study reflected current trends and challenges in the cybersecurity sector.

For the data selection, the study prioritized sources that specifically addressed the global cybersecurity skills gap, emphasizing high-demand countries like the U.S., China, and India, as these nations top the chart for the shortages in cybersecurity talent. The data also covered diverse industries, particularly sectors critical to national security and economic stability, such as finance, healthcare, and government. Given the increasing importance of cybersecurity in these sectors, data from these industries was crucial to the study. Articles that offered empirical evidence, statistical data, or case studies on how the skills gap affects these sectors were given preference.

The study also sought sources that provide practical solutions, such as training initiatives, certification programs, and government policies, to close the skills gap. Reports from organizations like the World Economic Forum, the European Union Agency for Cybersecurity (ENISA), and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) helped understand the broader implications of the skills gap on national security and the economy.

Lastly, the study cross-referenced sources for accuracy and consistency. Regarding conflicting

data, the study prioritized studies with larger sample sizes or those published by highly reputable institutions. This ensured that the findings used were based on reliable and validated information.

3.1 Research Design

This study employs a qualitative research design focusing on secondary data analysis. Given the complex and evolving nature of the cybersecurity skills gap, a qualitative approach is most suitable to capture the underlying trends, challenges, and solutions highlighted in the existing literature. The study synthesized various perspectives from different countries, industries, and stakeholders to identify patterns and themes related to the workforce shortage.

3.2 Data Collection Methods

The data collection approach involved gathering secondary data from academic journals, government reports, and industry publications. Given the nature of the research, secondary data was chosen as it allowed access to large-scale datasets and insights from authoritative sources, such as government agencies, cybersecurity firms, and international organizations.

3.3 Inclusion Criteria

To ensure the relevance and quality of the data used for this study, the following inclusion criteria were established: relevance to the cybersecurity skills gap, geographic focus on major economies, journals published within the Last 5 Years, industry diversity

3.4 Exclusion Criteria

The exclusion criteria were also established to eliminate irrelevant or low-quality data: irrelevant to cybersecurity workforce issues, outdated studies, limited geographical or sectoral Focus, lack of empirical data, and non-English sources.

3.5 Data Analysis Techniques

The data analysis for this study was conducted using a thematic analysis approach. This technique identifies recurring patterns, themes, and trends within the selected literature. The thematic analysis was applied to categorize data into relevant themes such as the role of public-private partnerships, sector-specific training, diversity initiatives, and the impacts of the skills gap on national security and economic stability. A cross-sectional analysis was also used to compare findings across different regions, industries, and periods to highlight global trends and country-specific challenges.

3.6 Ethical Considerations

Since this study relied on secondary data, ethical concerns primarily revolved around ensuring that all sources were cited correctly and that data was used responsibly. Furthermore, the study ensured that there was transparency in data sourcing. The research was based on publicly available data, so no direct participant consent was required. However, the study avoided using data from sources that could compromise confidentiality or were not publicly accessible. Additionally, when interpreting findings, efforts were made to present a balanced view without bias, ensuring that the analysis reflected multiple perspectives.

3.7 Limitations and Bias

A key limitation in the methodology for this study is the reliance on secondary data, which could introduce potential biases from the original studies. Furthermore, the selection of data sources was limited to those readily accessible and may not capture all perspectives, particularly from non-English speaking regions or smaller industries. While the study aimed for diversity in data selection, it is acknowledged that gaps remain, particularly in the representation of smaller countries or industries with limited research available.

4.0 FINDINGS

Research from the U.S., India, China, and Europe all point to the urgent need for targeted interventions and long-term strategies to develop and retain cybersecurity talent. In the U.S., a study by ISACA (2023) identified the role of public-private partnerships in bridging the cybersecurity skills gap. One proposed solution was the CyberCorps Scholarship for Service program, which offers financial incentives for students to pursue cybersecurity careers in government roles. This initiative aims to direct talent into critical sectors, including defense, healthcare, and infrastructure. Additionally, Cappelli (2024) and Catal et al. (2022) suggested that companies should invest in upskilling and reskilling current employees through on-the-job training and certification programs. These efforts could reduce reliance on external consultants and promote internal workforce development, particularly for entry-level positions.

In Europe, a European Union Agency for Cybersecurity (ENISA, 2023) study emphasized the need for a unified cybersecurity training framework across member states. The report advocated harmonized curricula and certification systems to ensure cybersecurity professionals possess the necessary skills to operate within the EU's diverse regulatory environments. It also called for increased investment in cybersecurity education programs, emphasizing practical skills in real-world scenarios. Countries like Germany and France have already begun incorporating cybersecurity simulations and ethical hacking programs into their educational systems (Alawida et al., 2022). These efforts aim to provide students with hands-on experience and a deeper understanding of cyber threats and defense mechanisms.

The Chinese government has taken significant steps to address the issue in China, where the cybersecurity workforce gap is one of the largest globally (Tan et al., 2024). The government has launched initiatives such as the National Cybersecurity Talent and Innovation Base, a training center to develop cybersecurity professionals in emerging technologies, including AI and big data (Vukosavljevic, Kralj and Vidnjevic, 2024). Prümmer, van Steen, and van den Berg (2023) suggested focusing on international collaborations for cybersecurity training. Given China's extensive manufacturing and technological sectors, these initiatives are designed to equip professionals with skills that address national security concerns and the needs of the fast-growing tech industry.

In India, which has also faced significant cybersecurity workforce shortages, particularly in the IT and financial sectors, a study by the National Association of Software and Service Companies (NASSCOM) revealed the need for cross-industry collaboration (Ray, Kathuria, and Kumar, 2020). This collaboration could involve technology companies, academic institutions, and government bodies working together to develop industry-specific cybersecurity talent pools (Nizami, Tripathi, and Mohan, 2022). Chenoy, Ghosh, and Shukla (2019) recommended implementing cybersecurity apprenticeships to provide on-the-job training for students, especially in critical sectors like finance and healthcare. Furthermore, the study also suggested creating cybersecurity labs in universities to allow students to simulate and respond to real-time cyberattacks.

In Japan, where cybersecurity talent is critical due to the country's industrial sector, a Japanese Ministry of Internal Affairs and Communications report suggested enhancing collaborations between industry and academia to develop a steady supply of skilled professionals (Esangbedo et al., 2023). This involves internships and cybersecurity-focused academic research programs to integrate emerging technologies like blockchain and AI into real-world cybersecurity defense mechanisms. Japan focuses on building expertise in both the private sector and government institutions, emphasizing developing a culture of continuous learning and improvement within

organizations (Aljohani et al., 2022).

For the energy sector, a 2023 study by the International Energy Agency (IEA) called for the implementation of specialized training programs for securing operational technologies (OT) (Caiafa et al., 2023). The report revealed the need for training that explicitly addresses the cybersecurity needs of critical infrastructure, which differs from traditional IT systems. Dennhardt et al. (2023) also stated the importance of cybersecurity risk management frameworks to help energy companies identify vulnerabilities and invest in the necessary skills and technology to mitigate these risks. The study stressed that companies should collaborate with government agencies to implement national cybersecurity policies to build a skilled workforce capable of defending against cyber threats targeting energy systems.

In the healthcare industry, having cybersecurity talent in health IT is crucial. The report recommended a multi-pronged approach, including specialized cybersecurity certifications for health professionals, cybersecurity awareness programs for non-technical staff, and healthcare-focused cyber simulation exercises. Singh, Mandal, and Purohit (2023) proposed the establishment of cybersecurity talent pipelines to create a steady flow of qualified professionals in the sector.

5.0 DISCUSSIONS

5.1 Public-Private Partnerships for Workforce Development

Public-private partnerships (PPPs) have emerged as a critical solution to the cybersecurity skills gap, especially in countries like the U.S., China, and India, where the shortage of skilled professionals in cybersecurity remains a significant challenge (Luo, 2021). These partnerships leverage the strengths of both public institutions (government) and private organizations (corporations) to address workforce development issues and create a sustainable talent pipeline for the cybersecurity sector (Burrell, 2018). One of the most prominent examples of a PPP in cybersecurity workforce development is the CyberCorps Scholarship for Service (SFS) program in the United States (ICS2, 2023). This initiative, funded by the federal government, provides scholarships to students pursuing cybersecurity degrees while requiring them to work in federal, state, local, or tribal government positions upon graduation. The program addresses the need for qualified cybersecurity professionals in critical government roles. This model has proven successful in providing financial support to students and ensuring that the U.S. government has a skilled workforce to protect its infrastructure from cyber threats (Statista, 2024).

Similarly, China's National Cybersecurity Talent and Innovation Base highlights the Chinese government's efforts to foster collaboration with private entities to address the growing cybersecurity workforce shortage (Tan et al., 2024). The government has invested in training centers, partnered with tech giants like Huawei and Tencent, and established research hubs focused on cybersecurity (Alawida et al., 2022). This government and private industry collaboration helps align education with market demands, ensuring the workforce has the relevant skills and certifications to deal with emerging threats (Vukosavljevic, Kralj, and Vidnjevic, 2024).

In addition to these national programs, private corporations also recognize the need for collaboration with the public sector to develop and retain cybersecurity talent. Major companies in the tech sector, including Microsoft, Cisco, and IBM, have launched cybersecurity training and certification programs in partnership with universities and government agencies (BobSulli, 2024). These corporate-backed educational initiatives ensure that students gain theoretical knowledge and receive practical, industry-specific training that improves their employability.

However, there are still challenges in ensuring that these partnerships lead to a long-term, sustainable solution. One issue is the reliance on government funding, which can fluctuate with

changes in political administrations and budget priorities (State.gov, 2023). BobSulli (2024) also explained that not all private companies have the resources or incentives to engage in these partnerships. Small and medium-sized enterprises (SMEs) often lack the funding to invest in cybersecurity workforce development. Moreover, the rapid pace of technological advancement means that training programs must continuously evolve, which can be challenging to keep up with when public and private stakeholders have competing priorities (Hodson, 2021).

5.2 Sector-Specific Training and Certifications

Sector-specific training and certifications are essential in addressing the growing cybersecurity skills gap as different industries face unique challenges and threats (Dennhardt et al., 2023). As cybersecurity threats become more sophisticated, industries such as healthcare, finance, energy, and government increasingly require specialized skills to protect their networks and data. For example, the rise of health information technology (HIT) in the healthcare industry has made hospitals and medical institutions prime targets for cyberattacks (Singh, Mandal, and Purohit, 2023). The healthcare sector's regulatory requirements, such as those of the U.S. Health Insurance Portability and Accountability Act (HIPAA), necessitate cybersecurity professionals with specific knowledge of data protection and privacy laws (Poláková et al., 2023). Similarly, organizations like ISC2 have developed specialized certifications, such as the Certified Information Systems Security Professional (CISSP) with a healthcare focus, to ensure that cybersecurity professionals possess the knowledge to protect patient information (Petrosyan, 2024).

Also, the financial sector faces an entirely different set of cybersecurity risks due to the increasing integration of fintech and digital banking services (Alshaikh, 2020). Cybercriminals often target Banks and financial institutions seeking access to payment systems, credit card details, and financial records (Admass, Munaye and Diro, 2024). As such, the demand for professionals with specific skills in areas like cryptography, blockchain security, and payment security has surged. The Certified Financial Services Security Professional (CFSSP) certification, provided by the Financial Services Information Sharing and Analysis Center (FS-ISAC), targets the unique cybersecurity needs of the finance industry (Corallo et al., 2022).

The energy sector, particularly critical infrastructure like power grids and oil pipelines, is another area where sector-specific cybersecurity skills are urgently needed (Statista, 2024). With the increase in Internet of Things (IoT) devices, energy companies now face new vulnerabilities, including SCADA systems and industrial control systems (ICS) (Petrosyan, 2024). The SANS Institute offers sector-specific training on ICS cybersecurity through its Certified SCADA Security Architect (CSSA) program, designed to address the unique challenges of protecting these critical systems (SANS INSTITUTE, 2023). However, there is still a significant shortage of professionals with the expertise to deal with threats to operational technology (OT), which is often overlooked compared to IT security (Tan et al., 2024). The lack of comprehensive OT security training means that energy companies remain vulnerable to cyberattacks that could disrupt power grids, supply chains, and other critical infrastructure (Beerman et al., 2023).

The government sector faces cybersecurity challenges, often related to national security and critical infrastructure protection. Agencies such as the U.S. Department of Homeland Security (DHS) and NATO have implemented specialized training programs for professionals working in defense and intelligence roles (State.gov, 2023). The Certified Information Security Manager (CISM) and Certified Information Systems Auditor (CISA) certifications, for example, have been designed to meet the specific requirements of government cybersecurity roles, ensuring professionals can respond to national security threats (Mukherjee et al., 2024).

5.3 Diversity and Inclusion in the Cybersecurity Workforce

The need for a diverse talent pool has become more critical with the rapid expansion of digital infrastructure and the increasing frequency of cyber threats. The cybersecurity workforce has traditionally been male-dominated and predominantly homogenous, with women and underrepresented minorities facing significant barriers to entry and advancement in the field (Stanfield, 2024). Promoting diversity and inclusion within cybersecurity teams can foster a more innovative and resilient workforce better equipped to tackle the modern era's complex and evolving cyber threats (Osman et al., 2023).

The lack of diversity in cybersecurity has become a pressing issue as it directly affects the quality of problem-solving and the ability to anticipate and address different cyber risks (Hamburg, 2023). A more inclusive cybersecurity workforce encompassing different ethnic, gender, and cultural backgrounds brings a variety of perspectives that can help organizations better understand and address the diverse range of cyber threats (Stanfield, 2024). The cybersecurity landscape, with its technical, social, and geopolitical dimensions, benefits from individuals with diverse skill sets and life experiences, which enhance the field's adaptability and effectiveness.

There has been an increasing recognition of the need for greater racial and ethnic diversity within the cybersecurity workforce (Osman et al., 2023). Underrepresented minorities, particularly Black, Hispanic, and Native American individuals, make up a disproportionate share of the cybersecurity talent shortage (Hamburg, 2023). Systemic inequalities in access to education, mentorship, and career opportunities often compound these groups' barriers. Addressing these challenges requires targeted outreach, mentorship programs, and scholarships to support individuals from diverse racial and ethnic backgrounds (Stanfield, 2024; Osman et al., 2023)

Mukherjee et al. (2024) explained that promoting diversity and inclusion in cybersecurity is not solely about recruitment; it also involves fostering an environment where individuals from diverse backgrounds can succeed and advance in their careers. This requires organizations to implement inclusive hiring practices, mentorship programs, and diversity-conscious leadership training (Osman et al., 2023). Companies like IBM, Cisco, and Microsoft have pioneered initiatives to support diverse talent in cybersecurity by creating inclusive work cultures, offering mentorship opportunities, and implementing flexible work policies that accommodate the needs of underrepresented employees (Hamburg, 2023).

However, the efforts to increase diversity and inclusion in cybersecurity face several challenges. One of the most significant is the persistence of unconscious biases that influence hiring decisions, performance evaluations, and opportunities for advancement (Corallo et al., 2022). Additionally, there are instances where the lack of inclusive workplace cultures and supportive networks forces many talented individuals to leave the cybersecurity field early in their careers (Beerman et al., 2023). Despite these challenges, the benefits of a more diverse and inclusive cybersecurity workforce are clear: it enhances creativity, problem-solving, and adaptability, all crucial in addressing the constantly evolving nature of cyber threats.

5.4 Continuous Learning and Upskilling for Existing Professionals

Continuous learning and upskilling are essential in addressing the cybersecurity skills gap, especially as the threat landscape evolves and new technologies emerge. The rapid pace of digital transformation and the increasingly advanced nature of cyberattacks require cybersecurity professionals to continually update their knowledge and skills to defend against emerging threats effectively (Aaltola, Ruoslahti, and Heinonen, 2022). In many industries, existing cybersecurity professionals are expected to stay ahead of these changes through regular training, certification programs, and engagement with the broader cybersecurity community (Catal et al., 2022). This is essential to ensure cybersecurity teams have the expertise to mitigate current and future risks

effectively.

One area where continuous learning is critical is artificial intelligence (AI) and machine learning (ML), which are becoming increasingly integral to cybersecurity strategies (LinkedIn, 2024). AI and ML technologies can enhance threat detection, automate responses, and predict cyberattacks, making them invaluable for cybersecurity professionals (Admass, Munaye, and Diro, 2024). However, to use these technologies effectively, existing professionals must acquire specialized skills in data science, algorithm development, and advanced security protocols (Corallo et al., 2022).

In addition to technical skills, continuous learning should also focus on developing soft skills such as communication, leadership, and problem-solving (ISACA, 2023). Cybersecurity is about technical defense, incident management, communicating with stakeholders, and leading teams in high-pressure situations (Mazlan and Jambulingam, 2023). By incorporating soft skills training into professional development programs, organizations can equip their cybersecurity teams to handle technical and strategic aspects of cybersecurity challenges.

Professional certifications play a significant role in ensuring cybersecurity professionals remain up-to-date with industry standards and best practices. Certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and Certified Cloud Security Professional (CCSP) are among the most widely recognized credentials in the field (IBM, 2024). These certifications validate an individual's expertise and provide a structured framework for ongoing learning. As cybersecurity continues to evolve, professional bodies and organizations update certification requirements to reflect new technologies, threats, and regulatory frameworks (Benson and Mouradian, 2023).

One of the challenges in upskilling existing cybersecurity professionals is the financial cost and time commitment required for continuous education and training (Blažič, 2021). While large organizations may have the resources to invest in ongoing training programs, smaller businesses may struggle to provide such opportunities for their employees (Luo, 2021). Governments, industry bodies, and educational institutions have increasingly offered low-cost or free training and certification programs to mitigate this issue (ISACA, 2023).

6.0 CONCLUSIONS & RECOMMENDATIONS

6.1 Summary of the Findings

The analysis of the cybersecurity skills gap revealed that the growing demand for cybersecurity professionals is driven by increasing cyber threats and the advancement of digital technologies. The U.S., Europe, and Asia face significant shortages, with countries like China and India experiencing the most critical gaps. Despite efforts to address these shortages through education and training, the gap remains a persistent challenge due to difficulties in attracting and retaining qualified talent.

The increasing importance of specialized skills, such as expertise in cloud security, artificial intelligence (AI), machine learning (ML), and Zero Trust architectures, are highly sought after, especially in industries like finance, healthcare, and government, where cybersecurity is critical to protecting sensitive data and infrastructure. The shortage of professionals with these specialized skills has led organizations to invest heavily in upskilling and certification programs. However, the skills mismatch is still a barrier, with many professionals lacking expertise in the latest cybersecurity technologies and strategies.

Another key finding is the role of public-private partnerships in addressing the cybersecurity workforce gap. Governments and businesses have recognized the need for collaboration to develop

training programs, share resources, and create pathways for individuals to enter the cybersecurity field. These partnerships have led to initiatives to foster a diverse and inclusive cybersecurity workforce, essential for creating a robust and resilient cybersecurity infrastructure. However, the effectiveness of these partnerships varies by country and industry, with some regions experiencing more success than others.

Sector-specific training and certifications emerged as a vital solution to address the skills gap. Tailored training programs focused on industry-specific needs, such as finance, healthcare, and manufacturing, have proven effective in preparing professionals to meet the unique cybersecurity challenges of these sectors. Certifications such as CISSP, CEH, and CCSP are essential for ensuring cybersecurity professionals have the expertise to tackle modern cyber threats.

Finally, international collaboration and cross-border initiatives are essential for addressing the global nature of cybersecurity threats. Global efforts to standardize training and certification requirements and the sharing of threat intelligence have helped improve the overall security posture of nations and organizations. However, inconsistencies in cybersecurity laws and regulations across countries remain challenging, hindering cross-border collaboration.

6.2 Limitations of the Study

The study has limitations, including primarily relying on secondary data sources, which may not fully capture real-time developments or occurrences in specific industries or regions. Additionally, the focus on particular countries (e.g., the U.S., China, and India) may limit the generalizability of the findings to other areas with different cybersecurity challenges. Also, the rapid pace of technological advancements in cybersecurity means that the study may not account for the most recent trends and emerging threats. Finally, the study's focus on workforce-related issues may overlook other critical factors, such as organizational culture and policy impacts, in addressing the skills gap.

6.3 Recommendations for Future Work

Future research should explore the long-term effectiveness of current workforce development initiatives, such as public-private partnerships and sector-specific training programs, to determine their impact on reducing skills shortages. Research could examine the success of existing training programs and identify best practices that could be scaled globally.

Also, there is a need for more data on the evolving cybersecurity skills landscape, particularly in emerging technologies such as AI, blockchain, and quantum computing. Future work should investigate how these technologies reshape cybersecurity roles and what new competencies professionals must develop to stay relevant. Additionally, exploring the impact of diversity and inclusion efforts on workforce development would be valuable. Research could examine how diverse teams contribute to enhanced cybersecurity outcomes and whether inclusive training models lead to better workforce retention and innovation.

Future work could also study the role of government regulations and international collaboration in closing the skills gap. Research should focus on how harmonizing cybersecurity standards and certifications across borders affect the global workforce. Using a longitudinal study on the career paths of cybersecurity professionals would help understand how continuous learning and upskilling shape career progression and industry retention, offering insights into effective career development strategies.

References

1) Aaltola, K., Ruoslahti, H. and Heinonen, J. (2022). Desired cybersecurity skills and skills acquisition methods in the organizations. *European Conference on Cyber Warfare and Security*, 21(1), pp.1–9. doi:https://doi.org/10.34190/eccws.21.1.293.
2) Admass, W.S., Munaye, Y.Y. and Diro, A.A. (2024). Cyber security: State of the art, Challenges and Future Directions. *Cyber Security and Applications*, [online] 2(2), p.100031. doi:https://doi.org/10.1016/j.csa.2023.100031.
3) Alawida, M., Omolara, A.E., Abiodun, O.I. and Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10), pp.8176–8206. doi:https://doi.org/10.1016/j.jksuci.2022.08.003.
4) Aljohani, N.R., Aslam, A., Khadidos, A.O. and Hassan, S.-U. (2022). Bridging the skill gap between the acquired university curriculum and the requirements of the job market: A data-driven analysis of scientific literature. *Journal of Innovation & Knowledge*, 7(3), p.100190. doi:https://doi.org/10.1016/j.jik.2022.100190.
5) Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, 98(98), p.102003. doi:https://doi.org/10.1016/j.cose.2020.102003.
6) Amorosa, K. and Yankson, B. (2023a). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *Holistica*, 14(1), pp.110–132. doi:https://doi.org/10.2478/hjbpa-2023-0007.
7) Amorosa, K. and Yankson, B. (2023b). Human Error - A Critical Contributing Factor to the Rise in Data Breaches: A Case Study of Higher Education. *Holistica*, 14(1), pp.110–132. doi:https://doi.org/10.2478/hjbpa-2023-0007.
8) Angafor, G.N., Yevseyeva, I. and He, Y. (2020). Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis. *Serious Games*, pp.117–131. doi:https://doi.org/10.1007/978-3-030-61814-8_10.
9) Beerman, J., Berent, D., Falter, Z. and Bhunia, S. (2023). *A Review of Colonial Pipeline Ransomware Attack*. [online] IEEE Xplore. doi:https://doi.org/10.1109/CCGridW59191.2023.00017.
10) Benson, E. and Mouradian, C. (2023). How Do the United States and Its Partners Approach Economic Security? *www.csis.org*. [online] Available at: https://www.csis.org/analysis/how-do-united-states-and-its-partners-approach-economic-security.
11) Blažič, B.J. (2021). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills? *Education and Information Technologies*, 27. doi:https://doi.org/10.1007/s10639-021-10704-y.
12) BobSulli (2024). *Cybersecurity Threat and Risk Management Report | Ponemon-Sullivan Privacy Report*. [online] Ponemonsullivanreport.com. Available at: https://ponemonsullivanreport.com/2024/07/2024-cybersecurity-threat-and-risk-management-report/ [Accessed 30 Nov. 2024].
13) Burrell, D.N. (2018). An Exploration of the Cybersecurity Workforce Shortage. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1), pp.29–41. doi:https://doi.org/10.4018/ijhiot.2018010103.
14) Caiafa, C., Hattori, T., Nam, H. and H.C. de Coninck (2023). International technology innovation to accelerate energy transitions: The case of the international energy agency

technology collaboration programmes. *Environmental Innovation and Societal Transitions*, 48, pp.100766–100766. doi:https://doi.org/10.1016/j.eist.2023.100766.
15) Cappelli, P.H. (2024). Skill Gaps, Skill Shortages, and Skill Mismatches. *ILR Review*, 68(2), pp.251–290. doi:https://doi.org/10.1177/0019793914564961.
16) Carlton, M. and Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of advanced persistent threats (APTs) mitigation. *Online Journal of Applied Knowledge Management*, 5(2), pp.16–28. doi:https://doi.org/10.36965/ojakm.2017.5(2)16-28.
17) Catal, C., Ozcan, A., Donmez, E. and Kasif, A. (2022). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. *Education and Information Technologies*. doi:https://doi.org/10.1007/s10639-022-11261-8.
18) Chenoy, D., Ghosh, S.M. and Shukla, S.K. (2019). Skill development for accelerating the manufacturing sector: the role of 'new-age' skills for 'Make in India'. *International Journal of Training Research*, [online] 17(sup1), pp.112–130. doi:https://doi.org/10.1080/14480220.2019.1639294.
19) Commerce.gov (2022). *Strengthen U.S. Economic and National Security*. [online] U.S. Department of Commerce. Available at: https://2017-2021.commerce.gov/about/strategic-plan/strengthen-us-economic-and-national-security.html.
20) Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, 137, p.103614. doi:https://doi.org/10.1016/j.compind.2022.103614.
21) Dennhardt, B., Zaidi, A., Chubb, J. and Wong, J. (2023). *State-of-the art approaches in OT Cybersecurity*.
22) ENISA (2021). *Reframing Cybersecurity Awareness Raising: Exploring the human factor in cybersecurity communication | ENISA*. [online] Europa.eu. Available at: https://www.enisa.europa.eu/news/reframing-cybersecurity-awareness-raising-exploring-the-human-factor-in-cybersecurity-communication [Accessed 1 Dec. 2024].
23) Esangbedo, C.O., Zhang, J., Esangbedo, M.O., Kone, S.D. and Xu, L. (2023). The role of industry-academia collaboration in enhancing educational opportunities and outcomes under the digital driven Industry 4.0. *Journal of Infrastructure, Policy and Development*, [online] 8(1). doi:https://doi.org/10.24294/jipd.v8i1.2569.
24) Garaja, A. (2022). Information Engineering and Electronic Business. [online] 5(5), pp.1–14. doi:https://doi.org/10.5815/ijieeb.2022.05.01.
25) Hamburg, I. (2023). SUPPORTING INTERDISCIPLINARITY, DIVERSITY AND INCLUSION IN CYBERSECURITY. *INTED proceedings*. doi:https://doi.org/10.21125/inted.2023.0050.
26) Hodson, C. (2021). Cybersecurity Skills. *Springer eBooks*, pp.1–5. doi:https://doi.org/10.1007/978-3-642-27739-9_1577-1.
27) IBM (2024a). *Cost of a Data Breach 2024*. [online] IBM. Available at: https://www.ibm.com/reports/data-breach.
28) IBM (2024b). *IBM Report: Escalating Data Breach Disruption Pushes Costs to New Highs*. [online] IBM Newsroom. Available at: https://newsroom.ibm.com/2024-07-30-IBM-Report-Escalating-Data-Breach-Disruption-Pushes-Costs-to-New-Highs.
29) ICS2 (2023). *How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce 2023*. [online] Available at: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_S

tudy_2023.pdf [Accessed 25 Mar. 2024].
30) ISACA (2023). *Solving the Cybersecurity Skills Gap Requires a Mindset Change*. [online] ISACA. Available at: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/solving-the-cybersecurity-skills-gap-requires-a-mindset-change [Accessed 1 Dec. 2024].
31) Juneja, A., Goswami, S.S. and Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of technology innovations and energy, 3(2), pp.1–22. doi:https://doi.org/10.56556/jtie.v3i2.907.
32) LinkedIn (2024). *Workforce insights from LinkedIn's Economic Graph*. [online] economicgraph.linkedin.com. Available at: https://economicgraph.linkedin.com/workforce-data?selectedFilter=view-all%2Fby-year.
33) Luo, Y. (2021). Illusions of techno-nationalism. *Journal of International Business Studies*, 53. doi:https://doi.org/10.1057/s41267-021-00468-5.
34) Mazlan, M.R.M. and Jambulingam, M. (2023). Challenges of Talent Retention: A Review of Literature. Journal of Business and Management Review, [online] 4(2), pp.078–091. doi:https://doi.org/10.47153/jbmr42.6302023.
35) Mohamed Hashim, M.A., Tlemsani, I. and Matthews, R. (2021). Higher Education Strategy in Digital Transformation. *Education and Information Technologies*, 27. doi:https://doi.org/10.1007/s10639-021-10739-1.
36) Mukherjee, M., Ngoc Thuy Le, Chow, Y.-W. and Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information*, 15(2), pp.117–117. doi:https://doi.org/10.3390/info15020117.
37) Nizami, N., Tripathi, T. and Mohan, M. (2022). Transforming Skill Gap Crisis into Opportunity for Upskilling in India's IT-BPM Sector. *The Indian Journal of Labour Economics*. doi:https://doi.org/10.1007/s41027-022-00383-9.
38) Osman, M., Namukasa, M., Ficke, C., Piasecki, I., OConnor, T.J. and Carroll, M. (2023). Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis. *Journal of Cybersecurity Education, Research and Practice*, [online] 2023(2). doi:https://doi.org/10.32727/8.2023.23.
39) Petrosyan, A. (2024). *Cost of a data breach in the U.S. 2022*. [online] Statista. Available at: https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/.
40) Poláková, M., Suleimanová, J.H., Madzík, P., Copuš, L., Molnárová, I. and Polednová, J. (2023). Soft skills and their importance in the labour market under the conditions of industry 5.0. *Heliyon*, 9(8), p.e18670. doi:https://doi.org/10.1016/j.heliyon.2023.e18670.
41) Prümmer, J., van Steen, T. and van den Berg, B. (2023). A systematic review of current cybersecurity training methods. *Computers & Security*, [online] 136(103585). doi:https://doi.org/10.1016/j.cose.2023.103585.
42) Ray, P.K., Kathuria, V. and Kumar, V. (2020). Slippery space and sticky places: evidence from the Indian IT industry. *Regional Studies, Regional Science*, 7(1), pp.52–74. doi:https://doi.org/10.1080/21681376.2020.1718545.
43) SANS INSTITUTE (2023). *ICS Security Training | SCADA Systems Security Training | SANS ICS410*. [online] www.sans.org. Available at: https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/ [Accessed 15 Aug. 2021].
44) Singh, A., Mandal, S. and Purohit, K.C. (2023). Significance of Cyber Security in Healthcare Systems. *Advances in information security, privacy, and ethics book series*, pp.51–71. doi:https://doi.org/10.4018/978-1-6684-6646-9.ch004.

45) Sinha, S. and Lee, Y.M. (2024). Challenges with developing and deploying AI models and applications in industrial systems. *Discover Artificial Intelligence*, 4(1). doi:https://doi.org/10.1007/s44163-024-00151-2.
46) Slawotsky, J. (2024). Conceptualizing National Security in an Era of Great Power Rivalry: Implications for International Economic Law. *East Asia*. doi:https://doi.org/10.1007/s12140-024-09434-y.
47) Stanfield, M. (2024). Bridging the Gap. *Advances in Medical Technologies and Clinical Practice*, pp.75–91. doi:https://doi.org/10.4018/979-8-3693-3226-9.ch005.
48) State.gov (2023). *United States International Cyberspace & Digital Policy Strategy*. [online] United States Department of State. Available at: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/.
49) Statista (2023). *Cybersecurity workforce estimate by country 2021*. [online] Statista. Available at: https://www.statista.com/statistics/1172449/worldwide-cybersecurity-workforce/.
50) Statista (2024). *Number of cybersecurity job openings by state U.S. 2023*. [online] Statista. Available at: https://www.statista.com/statistics/1272555/us-cybersecurity-job-openings-state/.
51) Tan, L., Liu, Z., Yuan, T., Wang, F. and Li, D. (2024). The Feasibility Exploration of Cyberspace Security Talent Training Program Under the Background of Digital Transformation. *Atlantis Highlights in Computer Sciences*, pp.254–260. doi:https://doi.org/10.2991/978-94-6463-502-7_27.
52) Vukosavljevic, B., Kralj, M. and Vidnjevic, M. (2024). Analysis of China-CEEC digital economy. *MEST Journal*, [online] 12(2), pp.75–82. doi:https://doi.org/10.12709/mest.12.12.02.10.