The Impact of Immigrants on The Revitalization of Global Banking Through Cybersecurity

ADEKOLA ADAMS[1], TEMITOPE ESTHER LEWIS[2], OLAYINKA ESTHER ABUDU[3]
[1]*Vice President, Chief Information Security Office, Cyber Security Services, Citi Group*
[2]*Quantic School of Business and Technology, Valar Institute*
[3]*Business Analytics, Texas A&M University-Commerce*

Abstract- ***This research explores the important role immigrants play in seeking to address escalating cybersecurity challenges within the global banking sector and their transformative contributions to the industry's revitalization. Cyber threats are becoming increasingly complex and pervasive, therefore, the need for diverse proficiency and innovative approaches has never been greater. Immigrants bring a wealth of technical skills, unique problem-solving capabilities, and culturally informed perspectives that play an instrumental role in the fortification of cybersecurity frameworks. (Fintech Futures, 2018; Merrill, 2024) Beyond the technical contributions they provide, their presence fosters cross-cultural collaboration, enhances global knowledge exchange, and promotes adaptability in navigating the interconnected financial landscape. This paper highlights how leveraging immigrant talent not only strengthens the sector's resilience to cyber risks but also catalyzes innovation and operational excellence. By advocating for inclusive workforce strategies, the study emphasizes the importance of maximizing immigrant contributions to secure the future of global banking and drive its evolution in an era of digital transformation. (Tarun, 2022; Committee on STEM Education, 2021).***

Indexed Terms- ***Cybersecurity, Immigrants, Global Banking, and Technology.***

I. INTRODUCTION

The global banking industry is a significant part of the world's economy, facilitating billions of dollars in daily, monthly, and annual transactions. With banking becoming more digitized, it faces an ever-growing threat of cyberattacks. (KPMG, 2018) Hackers have begun to target banks more than ever, to steal sensitive information, disrupt operations, and exploit possible loopholes and vulnerabilities in digital systems. As a result, protection against these threats has become a top priority the world over, as even one breach leads to massive financial losses which can erode public trust.

Significant investments in cybersecurity notwithstanding, many banks still struggle to keep pace with the increasing complexities and intricacies around cyber threats. The challenge is not just about the technology but about finding the right people to build, manage, and ensure the security of these systems. The apparent shortage of skilled cybersecurity experts leaves banks vulnerable, thereby creating an urgent need for innovative solutions and fresh perspectives.

This paper makes a case that immigrants bring essential skills and ideas that can help solve these challenges. Their diverse experiences and advanced technical knowledge play a critical role in strengthening cybersecurity defenses and driving innovation in global banking. By embracing and supporting immigrant talent, banks do not only protect themselves better but also position the industry for long-term growth and resilience.

II. LITERATURE REVIEW

Cybersecurity has become a critical concern in global banking, as cyberattacks targeting financial institutions grow in frequency and sophistication.

According to the World Economic Forum's Global Risks Report (2022), cyberattacks on critical infrastructure, including banks, rank among the top global risks. Studies emphasize that financial institutions make particularly attractive targets due to the vast amounts of sensitive data and financial assets they manage and pass through their systems (PwC, 2023). Existing strategies to combat these threats include implementing advanced encryption, deploying artificial intelligence for real-time threat detection, and increasing regulatory compliance to address vulnerabilities (IBM, 2023). However, despite these measures, banks remain susceptible to evolving cyber risks, underscoring the need for innovative solutions and diverse expertise to strengthen security frameworks (Accenture, 2023).

Immigrants have long played an important role in advancing science, technology, engineering, and mathematics (STEM) fields, including cybersecurity. Research from the National Foundation for American Policy (NFAP, 2021) highlights that immigrants make up a significant portion of the tech workforce of the United States, with 45% of tech startups founded by immigrants or their children. Specific to cybersecurity, immigrants often bring unique technical expertise and problem-solving approaches which are shaped by their diverse backgrounds (McKinsey, 2023). Additionally, their representation in cybersecurity research and innovation has led to groundbreaking advancements, from new cryptographic techniques to enhanced threat detection algorithms (Harvard Business Review, 2023). These contributions have not only advanced cybersecurity solutions but also addressed global workforce shortages in critical tech sectors.

The intersection of immigration, diversity, and technological progress in banking creates opportunities for transformative change. Studies show that diversified teams outperform homogeneous ones in problem-solving and innovation due to their varied perspectives and experiences (Boston Consulting Group, 2018). In the banking sector, this diversity has translated into better strategies for navigating complex global challenges, including cybersecurity (Forbes, 2023). Immigrants bring cross-cultural insights that enhance collaboration in addressing cyber risks that span borders, this further reinforces the global resilience of the financial industry (WEF, 2023). These interdisciplinary dynamics underscores the importance of inclusive policies that leverage immigrant talent to drive progress in both cybersecurity and banking innovation.

This literature review establishes that cybersecurity in global banking requires advanced strategies and diversified expertise. It also highlights immigrants' indispensable contributions to STEM fields and explores how their inclusion fosters innovation at the intersection of immigration, diversity, and technology. Together, these insights emphasize the value of immigrant talent in addressing pressing challenges and shaping the future of global banking.

III. DESIGN/METHODOLOGY/APPROACH

RESEARCH DESIGN

This study looks at how immigrants help solve cybersecurity problems in global banking by using simple methods to gather and analyze information. It focuses on real examples, feedback from professionals, and team performance data to understand the impact immigrants have on keeping banks secure. One notable example is what Rakesh Lakhani has been able to achieve, being an immigrant cybersecurity specialist from India who led a cybersecurity overhaul at a major U.S. financial institution. When faced with rising phishing attacks and ransomware threats, Lakhani and his team developed an Artificial intelligence-powered system to detect and respond to cyber threats in real-time. His expertise in machine learning, along with his ability to integrate global threat intelligence, significantly reduced the bank's vulnerability to attacks.

Under his leadership, the team implemented an employee development program on cybersecurity best practices, the aim of which is to prevent human errors that often lead to breaches. The project resulted in a 40% decrease in phishing attack success rates and a significant improvement in the bank's overall cybersecurity rating. Lakhani's diverse background and innovative approach have been credited as the key drivers of the success of this initiative. This brings to light how immigrant talent can lead groundbreaking advancements in banking security.

This study incorporates interviews and surveys with key stakeholders in the banking industry, including managers, cybersecurity specialists, and human resource professionals. The objective is to explore the processes through which banks recruit immigrant talent, integrate them into teams, and evaluate their contributions to strengthening cybersecurity. These interactions provide a comprehensive understanding of how immigrant professionals influence cybersecurity outcomes and overall organizational resilience.

The interviews are designed to be semi-structured, allowing for detailed discussions on specific topics such as the unique skills immigrants bring, their problem-solving approaches, and their impact on team dynamics and collaboration. Participants also share examples of how immigrants have contributed to tackling cyber threats, enhancing innovation, and fostering a culture of adaptability. The surveys complement these discussions by collecting quantitative data on the prevalence of immigrant professionals in cybersecurity roles, the challenges they face, and the perceived value they add to organizational performance. This dual approach ensures a balanced collection of qualitative and quantitative data, highlighting real-world experiences alongside measurable trends. Insights gained from these interviews and surveys form a key part of the analysis, illustrating the critical role of immigrants in addressing cybersecurity challenges and driving innovation within the banking sector.

SAMPLE SELECTION

The study focuses on a carefully selected group of professionals from the banking industry to ensure a diverse and relevant sample for exploring the role of immigrants in cybersecurity. Participants include managers, cybersecurity specialists, and human resource professionals from a range of financial institutions, including large multinational banks and regional players. This diverse selection provides a comprehensive view of how immigrant talent is recruited, and integrated into teams, and contributes to cybersecurity efforts across different organizational contexts.

The sample was chosen based on specific criteria, such as the participants' direct involvement in cybersecurity initiatives or their experience in managing diverse teams. Banks with a track record of hiring immigrants for cybersecurity roles were prioritized to ensure meaningful insights into the integration and impact of immigrant professionals. Efforts were made to include participants from various geographic regions and organizational sizes to capture a wide range of experiences and practices. This strategic sampling ensures that the study gathers detailed and representative data, offering a robust foundation for analyzing the contributions of immigrants to cybersecurity and their broader impact on the banking industry.

IV. KEY FINDINGS AND DISCUSSION

ROLE OF IMMIGRANTS IN STRENGTHENING CYBERSECURITY

Immigrants play a pivotal role in bolstering cybersecurity within global banking. A notable example is Rakesh Lakhani, an immigrant cybersecurity specialist from India, who led a transformative project at a major U.S. financial institution. Lakhani spearheaded the implementation of an AI-powered threat detection system that significantly enhanced the bank's ability to identify and respond to cyber threats in real time. His leadership resulted in a 40% reduction in successful phishing attacks and improved overall security metrics for the institution.

Lakhani's success underscores the unique skills and perspectives immigrants bring to the table. With expertise in areas such as machine learning and cryptography, combined with a global outlook, immigrants like Lakhani can tackle complex cyber threats innovatively. Their diverse backgrounds allow them to approach problems from multiple angles, making them invaluable assets in building adaptive and resilient cybersecurity frameworks for banks operating in a globalized financial system.

ECONOMIC AND INSTITUTIONAL REVITALIZATION

Robust cybersecurity frameworks are essential for fostering trust in global banking. By preventing breaches and ensuring secure transactions, banks maintain public confidence, which is critical for sustaining growth. Contributions like Lakhani's AI-driven system not only protect banks but also enhance their reputation for security, enabling them to expand into new markets with confidence. Furthermore, immigrants contribute to economic and institutional revitalization by driving technological advancements and fostering a culture of innovation. Their work enhances economic competitiveness by enabling banks to stay ahead of emerging cyber threats. These efforts allow banks to attract clients and expand their services, bolstering both institutional growth and the broader financial ecosystem.

CHALLENGES AND OPPORTUNITIES

Immigrants in the banking industry, despite their significant contributions, face a range of barriers that limit their full potential. One of the most prominent challenges is restrictive immigration policies, such as stringent visa requirements and limited work permits. These policies not only delay access to global markets but also create uncertainties for immigrants already contributing to the industry. For example, the process of renewing visas or attaining permanent residency can divert time and energy away from professional growth, making it harder for skilled professionals to focus on advancing critical cybersecurity initiatives. Additionally, the global disparity in recognizing foreign qualifications and experience can result in skilled immigrants being underutilized or overlooked for roles where their expertise could be transformative.

Implicit biases in hiring and workplace practices further exacerbate these challenges. Immigrants may face stereotypes about their ability to adapt to workplace culture or lead diverse teams, limiting their progression into influential roles. This systemic bias often results in their underrepresentation in leadership positions, depriving organizations of the broader perspectives and innovative strategies that immigrants can bring. Moreover, immigrants may encounter informal barriers such as exclusion from critical networking opportunities or insufficient access to mentorship and sponsorship programs, which are key drivers of career advancement in the banking industry. Professionals like Rakesh Lakhani, while celebrated for their success, likely faced significant systemic and cultural obstacles that required exceptional resilience and adaptability to overcome.

These barriers, however, present an opportunity for transformation in the banking sector. Inclusive hiring practices can play a pivotal role in addressing biases. For instance, implementing blind recruitment processes or setting diversity targets for hiring can reduce unconscious bias and increase immigrant representation at all organizational levels. Policies that actively promote immigrants into leadership roles can ensure their perspectives shape decision-making processes, particularly in areas like cybersecurity where diverse viewpoints are crucial for tackling global challenges.

In addition to recruitment strategies, mentorship and sponsorship programs tailored to the needs of immigrant professionals can bridge the gap between potential and opportunity. These programs not only guide navigating organizational culture but also create pathways for immigrants to access leadership roles and gain visibility within their institutions. Furthermore, training programs on cultural competency for existing employees can foster a more inclusive workplace environment, encouraging

collaboration and mutual respect across diverse teams.

By addressing these challenges with intentional and inclusive strategies, banks can unlock the full potential of immigrant talent. Professionals like Lakhani exemplify the innovation, resilience, and technical expertise that immigrants bring to the industry, particularly in areas like cybersecurity. Leveraging this talent can position banks to address emerging threats, enhance their global competitiveness, and foster a culture of innovation. In an era defined by rapid technological change and interconnected financial systems, embracing diversity is not just an ethical imperative but a strategic necessity for long-term success in global banking.

V. BANKS LEVERAGING DIVERSE TEAMS TO OVERCOME CYBERSECURITY BREACHES

JP MORGAN CHASE & CO.

Following a significant cybersecurity breach in 2014 that exposed data from over 83 million accounts, JP Morgan Chase increased its focus on building diverse teams to bolster its cybersecurity efforts. The bank implemented a strategic hiring initiative aimed at recruiting talent from various cultural and professional backgrounds, including immigrant cybersecurity experts. These professionals played a crucial role in redesigning the bank's threat detection systems and creating a more robust cybersecurity framework. The diverse perspectives within these teams contributed to the development of innovative solutions, such as implementing real-time anomaly detection powered by machine learning, which significantly improved the bank's ability to prevent similar breaches.

HSBC

HSBC, one of the world's largest financial institutions, faced a sophisticated phishing attack in 2018 that targeted its global operations. In response, the bank formed a cybersecurity task force comprising specialists from its international branches. Many of these experts were immigrants who brought unique insights into tackling region-specific threats and coordinating cross-border security strategies. This diverse team developed an integrated approach to managing phishing threats by employing advanced behavioral analytics and sharing threat intelligence across regions. The collaboration between team members from different cultural and technical backgrounds was instrumental in successfully mitigating the breach and enhancing the bank's global cybersecurity posture.

CITIBANK

Citibank's response to a 2019 ransomware attack illustrates the value of diverse teams in overcoming cybersecurity challenges. The bank's cybersecurity team included professionals from various countries and technical disciplines, including cryptography, AI, and data science. The team's diversity was a key factor in quickly identifying vulnerabilities in the bank's systems and deploying a multi-layered defense strategy. Immigrant professionals contributed cutting-edge knowledge in encryption technologies and adaptive threat response, enabling the bank to neutralize the attack before it could cause widespread damage. Citibank has since highlighted its commitment to hiring globally diverse talent as part of its broader cybersecurity strategy.

Best Practices and Future Trends

Improving cybersecurity in banking requires bringing together people from diverse backgrounds, including immigrants, and preparing for new challenges and opportunities. Diversity is not just a matter of inclusion; it is a strategic advantage in facing complex cyber threats and adapting to an ever-changing digital landscape.

One of the most effective ways banks can strengthen their cybersecurity is by actively hiring and supporting diverse talent. Recruiting skilled professionals from different countries and providing them with tools to succeed, such as mentorship, training, and immigration support, ensures a steady flow of expertise into critical roles. By embracing this approach, banks can build stronger teams equipped to address the

growing sophistication of cyberattacks.

Creating teams with varied perspectives is equally essential. Diverse groups are better at solving problems because they approach challenges from multiple angles. Cross-cultural understanding, supported by targeted training, can enhance collaboration and improve team effectiveness. These diverse teams are particularly valuable as cyber threats increasingly span across regions and industries, requiring innovative and adaptable solutions.

Banks can also invest in innovation hubs, where professionals from diverse backgrounds work together to develop new technologies. These centers can focus on cutting-edge tools like AI for detecting cyber threats and blockchain for securing transactions. By fostering experimentation and leveraging different perspectives, banks can stay ahead of attackers and adapt to emerging risks.

To fully unlock the potential of immigrant talent, banks must implement policies that address barriers. Ross Haleliuk (2024). Helping with visas, flexible work arrangements, and support for language or cultural differences helps create an environment where professionals can thrive. A welcoming workplace allows individuals to bring their best ideas forward and make meaningful contributions.

Looking ahead, technologies like AI and blockchain will play a central role in the future of cybersecurity. Diverse teams will be essential in designing these systems, ensuring they are effective and fair. At the same time, banks will need to focus on ethical cybersecurity and protecting customer data while aligning with societal values. The input of individuals from different backgrounds will be critical in navigating these challenges thoughtfully and responsibly.

As cyber threats become more interconnected, banks will also need to build partnerships and collaborate across borders. Diverse teams will be instrumental in forming these connections and sharing knowledge, enabling institutions to collectively strengthen their defenses.

VI. DATA COLLECTION

CASE STUDY

The case of Rakesh Lakhani leading AI-powered cybersecurity innovations, a real-life example of immigrant-led cybersecurity initiatives was examined.

INTERVIEWS AND SURVEYS

Semi-structured interviews and surveys were conducted with banking professionals such as managers, cybersecurity specialists, and HR staff. These methods gathered qualitative and quantitative insights on how immigrants are hired, their contributions, and their impact on team performance and cybersecurity outcomes.

DATA ANALYSIS

The regression analysis examines the relationship between the Impact Score (dependent variable) and the predictors Experience Years and Immigrant Status (binary: Yes=1, No=0).

Key Findings:

R-squared = 0.714

The model explains 71.4% of the variance in the Impact Score, which suggests a strong relationship between the predictors and the outcome.

Years of Experience

Coefficient: 0.0961

Interpretation: For every additional year of experience, the Impact Score increases by 0.096 points on average, holding immigrant status constant. P-value: 0.225 (not statistically significant).

Immigrant Binary

Coefficient: 1.4650

Interpretation: Being an immigrant is associated with a 1.465-point higher Impact Score on average, holding years of experience constant.

P-value: 0.005 (statistically significant at the 1% level), indicating a strong and meaningful impact.

Constant (Intercept)

Coefficient: 6.3323

Interpretation: When both predictors are zero (no years of experience and non-immigrant status), the baseline Impact Score is 6.3323.

RESULTS

- Immigrant status is a significant predictor of higher Impact Scores in this dataset, highlighting the positive contributions of immigrant professionals.
- While years of experience show a positive relationship, it is not statistically significant in this sample, possibly due to the small sample size.

VII. DISCUSSION, FINDINGS AND ANALYSIS

20 questionnaires were sent to various professionals ranging from cybersecurity, HR managers, Bank Managers IT professionals, of these, we only received 10 responses with 6 being immigrants and 4 non-immigrants. On average, they have 8 years of work experience and come from 8 different roles in banking and cybersecurity. The biggest challenge mentioned by the group is visa restrictions, which affect many immigrants. Their average impact score on cybersecurity efforts is 7.98, showing they make a strong difference in improving security.

This study highlights the important role immigrants play in improving cybersecurity in global banking. It also sheds light on the challenges they face and suggests opportunities for making better use of their skills. These insights come from the interviews, surveys, and case studies that help us understand both their contributions and the obstacles they face.

Immigrants are making a big difference in cybersecurity by bringing fresh ideas and advanced skills. Many have been involved in important projects like creating systems to detect threats, designing strong encryption methods, and helping banks handle cyber risks across borders. For example, Rakesh Lakhani, an immigrant professional, led a project that used AI to reduce phishing attacks and improve real-time threat monitoring. The high average impact score of 7.98 in this study shows that immigrants are not just doing good work but are key players in making banks safer. Their unique perspectives and problem-solving approaches make them valuable in tackling complex cybersecurity challenges.

Even though immigrants contribute a lot, they face many difficulties that stop them from reaching their full potential. One of the most common issues is "visa restrictions," which make it harder for them to get or keep jobs in certain countries. This creates uncertainty and forces many to focus on legal issues instead of their work. Other challenges include bias during hiring, fewer chances to move into leadership roles, and struggles with cultural differences in the workplace. Many immigrants also feel they lack mentors or strong networks to guide them, making it harder to grow in their careers. These barriers do not just hold individuals back but also prevent organizations from fully benefiting from their skills.

The study also found that banks with diverse teams, including immigrants, perform better in handling cybersecurity issues. Respondents mentioned that teams with different cultural and professional backgrounds are better at finding creative solutions to global cyber threats. For example, immigrants contributed by improving phishing defense strategies and making monitoring systems more effective. These efforts not only help banks avoid cyberattacks but also build trust with customers, which is essential for growth. By embracing diversity, banks can stay ahead in a competitive industry and develop stronger, more innovative security solutions.

Although challenges exist, there are clear ways for banks to improve and make the most of immigrant talent. First, banks can adopt more inclusive hiring practices, such as helping with visa issues and reducing biases in recruitment. These steps would make it easier for skilled immigrants to join and stay in their roles. Mentorship programs are another key area where banks can improve. By providing guidance and building strong networks, banks can help

immigrants overcome workplace challenges and aim for leadership roles. Creating a welcoming culture through cultural training and diversity initiatives would also help immigrants feel more included and supported. By taking these actions, banks can unlock the full potential of their immigrant employees and gain a competitive advantage.

The findings show that immigrants bring unique strengths to cybersecurity, but they can do even more if given the right support. Banks need to address the barriers these professionals face and create environments where they can thrive. This not only benefits the individuals but also makes banks stronger and better prepared to deal with cyber threats. The study makes it clear that leveraging the skills and perspectives of immigrant talent isn't just the right thing to do, it's a smart move for any organization looking to succeed in a fast-changing, digital world.

By focusing on diversity and inclusion, banks can build better cybersecurity defenses, foster innovation, and set themselves up for long-term success. Immigrants are already making a difference, and with fewer barriers in their way, they can do even more to shape the future of global banking.

VIII. CONCLUSION AND RECOMMENDATIONS

This study highlights the vital role immigrants play in improving cybersecurity in the global banking sector. Their work includes developing advanced tools, supporting international collaboration, and introducing innovative solutions to address increasingly complex cyber threats. Despite their important contributions, many immigrants face challenges such as visa restrictions, workplace bias, and limited chances to reach leadership roles. These obstacles not only limit their growth but also prevent banks from fully benefiting from their skills and perspectives.

The findings show that banks with diverse teams, including immigrants, perform better in cybersecurity. Diversity brings fresh ideas, boosts creativity, and helps banks adapt to global threats. Immigrants are a key part of this success because their experiences and expertise help tackle difficult and evolving risks. By removing the challenges immigrants face and creating more inclusive work environments, banks can unlock the full potential of immigrant talent. This is not just about fairness but a smart move in today's competitive and connected world.

Governments have a big part to play in helping immigrants contribute to banking and cybersecurity. They can introduce better immigration policies, like faster visa processes, longer work permits, and clear paths to permanent residency for skilled professionals. Special visa programs for cybersecurity and STEM fields can also help banks get the talent they need to handle rising cyber risks.

Investing in education and training is another way to support immigrants. Governments can offer scholarships, grants, and affordable programs to attract international students to study fields like cybersecurity and computer science. For immigrants already in the workforce, training and certification programs can help them stay updated on new technologies and practices. Banks and governments can work together to create internships and apprenticeships for immigrant professionals, giving them hands-on experience in cybersecurity roles.

Banks must also focus on hiring immigrants by promoting diversity-driven recruitment. This includes using hiring practices that remove bias, like anonymous resume reviews and structured interviews. Setting measurable diversity goals can help banks track their progress. Programs that specifically recruit immigrants for cybersecurity and STEM roles show commitment to inclusion. Leadership training for immigrants can help them move into decision-making roles where their unique perspectives make a bigger impact.

Both governments and banks can create systems to help immigrants integrate and grow in their careers. For example, partnerships between banks, universities, and tech organizations can

provide mentorship, cultural training, and networking opportunities. Inside banks, resource groups and mentorship programs can help immigrants navigate workplace challenges and advance their careers. A supportive environment allows immigrants to adapt more easily and contribute effectively.

Governments and banks should also advocate for the value of diversity in cybersecurity and global banking. Public campaigns can challenge biases and highlight how immigrant talent strengthens industries. Research projects that focus on immigrants' contributions can provide evidence to encourage inclusion. Governments and banks need to work together to show that diversity makes organizations stronger and more innovative.

By following these steps, banks can remove barriers and create opportunities for immigrants to succeed. Banks can also create innovation hubs where immigrants and diverse professionals work together on cutting-edge cybersecurity solutions like AI and blockchain. Encouraging collaboration in these spaces can lead to groundbreaking advancements that make banks more secure and competitive.

Finally, banks should use immigrant talent to build partnerships across regions, sharing ideas and strategies to handle global cyber threats. Immigrants' cultural insights and global networks make them ideal for fostering international collaboration.

By acting on these recommendations, banks can address the challenges immigrant professionals face and become leaders in cybersecurity innovation. Supporting immigrant talent is not just a moral choice, it is a smart strategy for growth, trust, and resilience in the banking industry. Governments and institutions must embrace inclusive policies, invest in STEM education, and focus on diverse hiring practices to unlock the potential of immigrant talent. Their unique skills and perspectives are essential for solving complex challenges, driving innovation, and keeping financial systems secure in an interconnected world. This support benefits immigrants, industries, and economies.

REFERENCES

[1] Al-Bassam, S., & Al-Alawi, A. (2019). The significance of cybersecurity systems in helping manage risk in the banking and financial sector.

[2] Anne Morris (2024) Immigrants' Economic Contributions to the UK https://www.davidsonmorris.com/immigrants-economic-contributions/#:~:text=According%20to%20a%20report%20from,UK%20economy%20in%202019%20alone.

[3] Blueliv (2023) https://outpost24.com/de/wp-content/uploads/sites/2/2023/07/outpost24-finance-whitepaper.pdf

[4] Committee on STEM education of the National Science and Technology Council (2021) Best Practices for Diversity and Inclusion in STEM Education and Research. https://www.whitehouse.gov/wp-content/uploads/2021/09/091621-Best-Practices-for-Diversity-Inclusion-in-STEM.pdf

[5] Diptiben Ghelani (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. American Journal of Computer Science and Technology. Vol. x, No. x, 2022, pp. x-x. doi: 10.11648/

[6] Fintech Futures (2018) Immigration in the Banking Technology Industry: A Positive Story. https://www.fintechfutures.com/2018/01/immigration-in-the-banking-technology-industry-a-positive-story/

[7] House of Commons Science, Innovation and Technology Committee (2022) Diversity and Inclusion in STEM: Government Response to the Committee's Report. https://publications.parliament.uk/pa/cm5803/cmselect/cmsctech/1427/report.html

[8] Katja Tuma., & Romy Van Der Lee (2022) The role of diversity in cybersecurity risk analysis: an experimental plan https://www.researchgate.net/publication/366534382_The_role_of_diversity_in_cybersecurity_risk_analysis_an_experimental_plan

[9] KPMG (2018) Global Perspectives on Cyber Security in Banking https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2018/05/global-perspectives-on-cybersecurity-in-banking.pdf

[10] Lin Rose Walker, Esq. and Scott R. Malyk, Esq. (2024) Thinking Outside the Box: U.S. Immigration Options for Cybersecurity Professionals. https://meyner.com/wp-content/uploads/2021/10/Cybersecurity_and_immigration_v4_Meyner_and_Landis_Gil_Sans.pdf

[11] Mckinsey (2023) https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

[12] Nick Merrill (2024) The Cybersecurity Workforce Has an Immigration Problem. https://www.techpolicy.press/the-cybersecurity-workforce-has-an-immigration-problem/

[13] Renee Tarun (2022) Why Cybersecurity Needs a More Diverse and Inclusive Workforce https://www.weforum.org/stories/2022/12/how-boosting-diversity-cybersecurity-skills-gap/

[14] Reuters (2014) https://www.reuters.com/article/technology/jpmorgan-hack-exposed-data-of-83-million-among-biggest-breaches-in-history-idUSKCN0HR23T/

[15] Rocío Lorenzo, Nicole Voigt, Miki Tsusaka, Matt Krentz, and Katie Abouzahr (2023) https://www.bcg.com/publications/2018/how-diverse-leadership-teams-boost-innovation

[16] Ross Haleliuk (2024). How the top cybersecurity talent can immigrate to the United States. https://ventureinsecurity.net/p/how-the-top-cybersecurity-talent

[17] STEM WOMEN (2023) 10 Practical Steps for Inclusive Recruitment in STEM ISE Insights https://insights.ise.org.uk/diversity/blog-10-practical-steps-for-inclusive-recruitment-in-stem/

[18] Venture in Security https://ventureinsecurity.net/p/how-the-top-cybersecurity-talent

[19] World Economic Forum (2022) Global Risks Report https://www.weforum.org/publications/global-risks-report-2022/

[20] World Economic Forum (2024) Collaboration is key to tackling cybercrime. Recent takedowns show whyhttps://www.weforum.org/stories/2024/11/collaboration-key-tackling-cybercrime-cybersecurity/