The Role Industry-Academia Partnerships Play in Cybersecurity: Exploring Collaborative Approaches to Address Cybercrime

Emmanuel Berkoh, Benjamin Yankson, Mubarak Hussein and Yvonne Dadson
HackIoT Lab – College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, USA

Byankson@albany.edu

Abstract: Cybercrime presents a pervasive threat globally, affecting governments, organizations, and individuals. Addressing this threat requires collaborative efforts, particularly between industry and academia. This paper delves into the key role played by industry-academia partnerships in elevating cybersecurity training and awareness, intending to narrow gaps and align the trajectories of cybersecurity professionals. Employing a secondary research methodology, this study provides insights into the impact of collaborations between academia and industry on Cybersecurity education and awareness. It identifies areas within the education sector that can be improved to enhance cybersecurity awareness. The findings emphasize the crucial role of industry-academia partnerships in advancing cybersecurity awareness and resilience, offering potential solutions for cultivating skilled cybersecurity professionals. Additionally, the research aims to contribute to policymaking by advocating for laws and regulations that encourage collaborations between state institutions and industry to mitigate cybersecurity crime effectively.

Keywords: Cybersecurity, Cybercrime, Training, Collaboration

1. Introduction

The rapid evolution of technology has brought forth significant benefits to society but also heightened vulnerabilities, particularly concerning Cybercrime (Jang-Jaccard & Nepal, 2014). Cybercrime poses substantial threats to various sectors, impacting economic, financial, and information domains and endangering national security interests (Olmstead & Smith, 2017). Consequently, strategic partnerships between academia, government agencies, and industry are imperative to introduce cybersecurity programs and curricula across education sectors, notably higher education, fostering increased awareness, training, and the production of cybersecurity professionals capable of addressing emerging threats (Barati & Yankson, 2022). As documented by Statista, internet-based crimes, including Cybercrime, are among the fastest-growing cybersecurity threats, underscoring the urgent need for comprehensive collaboration and educational initiatives (Perosyan, 2023).

The financial ramifications of Cybercrime are staggering, with organizations worldwide suffering significant economic losses and data breaches amounting to billions of dollars (Barati & Yankson, 2022). Data breach costs vary across industries, with the healthcare sector bearing the highest average cost per breach, highlighting the criticality of industry-academia partnerships in mitigating such risks (Petrosyan & Ten, 2023). The inherent challenges arising from the rapid adoption of technology necessitate collaborative frameworks between industry, government, and academia to develop long-term solutions that minimize associated risks (Brooks, 2023).

The complexity of modern information systems, compounded by factors like cloud computing and edge computing, underscores the need for enhanced collaboration to address evolving threats effectively (Brooks, 2023). Addressing pressing Cybersecurity issues requires a cohesive approach that leverages the expertise and resources of all stakeholders, emphasizing shared responsibility and coordinated efforts (Brooks, 2023). Collaborative cybersecurity efforts should not be confined to research, government, or industry alone but should encompass a holistic, collaborative approach to safeguarding technology-dependent environments (Brooks, 2023). As Cybercrime's impact continues to escalate, collaboration becomes increasingly critical, with global costs projected to reach trillions of dollars annually by 2025 (Brooks, 2023). Figure 1 and Figure 2 illustrate the yearly costs of data breach trends and some of the World's most significant data breaches, respectively. For instance, McCandless & Evans study reveals the magnitude and scope of cybersecurity challenges (McCandless & Evans, 2022).

Table 1: The Healthcare industry-associated average data breach cost (Alda, 2023)

Categories	May 2020 - Mar 2021	Mar 2021-Mar 2022	Mar 2022-Mar 2023
Healthcare	9.23	10.1	10.93
Financial	5.72	5.97	5.9
Pharmaceuticals	5.04	5.01	4.82
Technology	4.88	4.97	4.66
Energy	4.65	4.72	4.78
Professional Services	4.65	4.7	4.47
Industrial	4.24	4.47	4.73
Global Average	4.24	4.35	4.45
Research	3.6	3.88	3.63
Education	3.79	3.86	3.65
Consumer	3.7	3.86	3.8
Entertainment	3.8	3.83	3.62
Communications	3.62	3.62	3.9

Data analysis attributed to Statista data from March 2022 and March 2023 indicates the highest average data breach cost in Healthcare is approximately 11 million USD. The average per breach in the financial sector was 5.9 million USD. Table 1 provides data breach costs for Pharmaceuticals, Technology, Energy, Professional Services, Industrial, Global, Research, Education, Consumer, Entertainment, and Communications (Petrosyan & Ten, 2023).

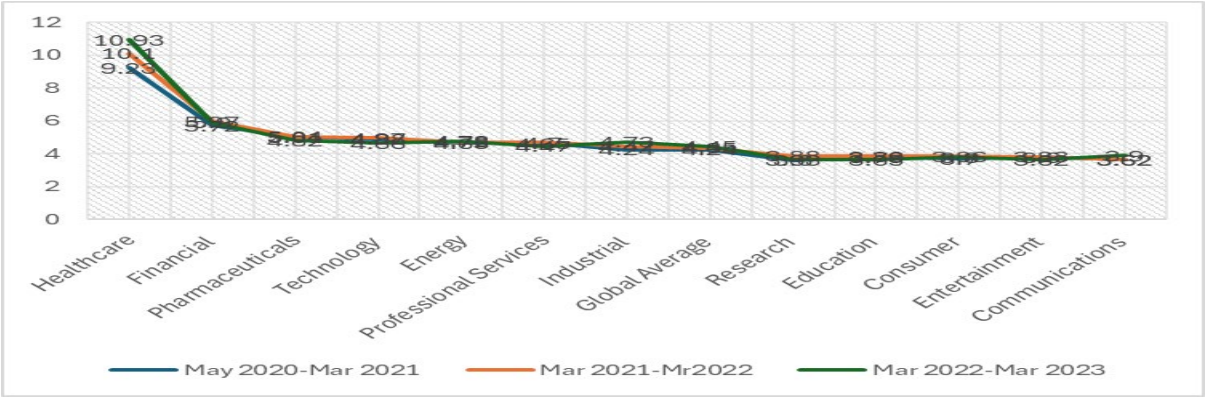

Figure 1: Yearly costs of data breach trends and some of the World's most significant data breaches

The above graph depicts a yearly trend in costs of data breaches within specific industries relative to the global average costs.

1.1 Challenges

The introduction, integration, and rapid adoption of technology spanning innovation in multiple fields have demonstrated significant benefits, including efficiency, productivity, and flexibility with society (Brooks, 2023). Such technological benefits are also accompanied by the risk of harm, especially to the system that supports our critical day-to-day activities, which can be subject to disastrous results such as financial loss, reputation loss, and, in some cases, significant safety concerns as we become more technologically dependent. For example, the adoption of ubiquitous Internet of Things devices, the adoption of AI-enabled devices, the integration of 5G, and the adoption of machine learning are resulting in paradigms requiring these systems to process vast amounts of data or system dependency and requiring instrumentation to protect these dependent systems from breach. Such a problem requires a solution that considers active and current research, industry expertise, and government working together to develop meaningful long-term solutions to minimize the risk associated with integrating and using new technology (Brooks, 2023).

The demand for new technology has become a competitive advantage for companies and a nation-state, which, in some cases, is mostly transitioning rapidly with increased vulnerability and related risks to cause significant

risk. Fundamentally, the continued adoption and use of technology in all aspects of everyday life have increased the attack, which has been enlarged as many companies integrate complex use of systems that allow interconnectivity and people to work anywhere across the globe. Such has resulted in a very complex IT permitter compared to traditional on-premises solutions. For example, today's information systems design and solutions, such as cloud and edge computing, need better industry and academic collaboration to design solutions that address threats through detection, analysis, and response.

To address some of the key pressing Cybersecurity issues in adopting new technologies, success can be based on an articulated approach that can be based on proper collaboration between industry, government, and academia-based framework that depends on the proper articulation of Cybersecurity problems, data availability, and sharing, investment in design and protecting new and emerging technologies). Such framework requires the development and facilitation of by industry, government, and academic entities with properly defined roles that develop continued working partnerships with the sole goal of addressing risk to information systems and avenues to leveraging resources and expertise in the respective sector to mitigate risk to widely used and adapted information system for everyday use or critical sectors. Expertise and resource coordination in addressing Cybersecurity challenges based on sharing resources such as tools, methods, and research results will be essential in such collaboration. Brooks (2023) states cybersecurity problems should not be isolated to research, government, or industry but rather collaborative effort. Our era fully depends on technology, which can be subject to Cybercrime and impact the brand, reputation, and revenue significantly. Such impact is well documented through continued attacks and costs related to such attacks. For example, as per estimates, it will grow by 15 percent per year, reaching USD 10.5 trillion annually by 2025 and costing the global economy over six trillion dollars (Brooks, 2023).

Over the last few years, high-profile cybercrime cases that attracted the attention and imagination across the globe include the hacking of the World Anti-Doping Agency and the subsequent release of medical testing records for several athletes and the hacking of Yahoo servers which led to access to confidential information of more than 1 billion account holders. In 2017, the United States Department of Homeland Security, FBI, and CIA all testified and stated that the Russian government was involved in a scheme to hack and influence the outcome of the 2016 US presidential elections (Olmstead & Smith, 2017). These examples demonstrate that the cost of Cybercrime is a social, political, and economic problem that grows daily. As such, a new approach, which entails pursuing strategic industry-academia partnerships, is required to allow the nation to build capacity and resilience to counter the threat of Cybercrime. Ending the ever-evolving threat of Cybercrime through strategic industry-academia partnerships is crucial because it will help bolster national security by preventing potential economic, financial, and personal information loss for millions of people and organizations.

Addressing such cybersecurity-related threats and vulnerabilities and combating or addressing them is necessary to improve the nation's cybersecurity awareness and resilience levels by pursuing robust academia-industry partnerships, bridging the gap, and putting Cybersecurity security researchers and professionals on the same trajectory. This work report will primarily rely on the literature review methodology to obtain information from scholarly articles to help explain the critical role that industry-academia partnerships play in increasing cybersecurity training and awareness. The scope of this study entails exploring the role of industry-academia strategic partnerships in cybersecurity training and awareness. The research investigates the critical role of the education sector in creating awareness around the vital issue of Cybersecurity in a world where Cybercrime is quickly transcending borders and adversely impacting digital systems and devices.

The objective of this research is to (1) examine the role of industry-academia partnerships in cybersecurity training and awareness; (2) To identify the people or organizations adversely impacted by Cybercrime and propose potential academia-industry solutions to help end it; (3) To explain what industry-academia partnerships ought to do to reduce or eliminate the threat of Cybercrime; (4)To determine the critical areas in the education sector, significantly higher education, that require Improvement to build and bolster cybersecurity awareness and resilience. The key research questions include: (1) To what degree do industry-academia partnerships and initiatives influence cybersecurity training and awareness levels? (2) What are the critical areas in the education sector require Improvement to sustain efforts to create a nation embedded in cybersecurity awareness? (3) To what degree do industry-academia partnerships affect or influence the ability to achieve the desired levels of cybersecurity awareness? (4) How will academia-industry partnerships help develop cybersecurity professionals to bolster the nation's cybersecurity capacity and resilience?

This work contributes to the current literature on industry and academic collaboration in Cybersecurity. Second, this work will serve as an academic resource for other researchers interested in expanding on industry-

academia partnerships and initiatives that influence cybersecurity training and awareness levels by addressing critical areas in academia that require Improvement to sustain efforts to create a nation embedded in cybersecurity awareness. The rest of the paper is organized as follows: Section 2.0 Background and related work. Section 3.0 presents a detailed methodology and implementation. Section 4.0 provides findings and analysis, section 5.0 concludes, and section 6.0 contains the references.

2. Background and Related Work

Globally, Cybercrime poses an urgent and growing threat to governments, businesses, and individuals. The global cost of Cybercrime in 2021 was estimated to be over $6 trillion, up from around $3 trillion in 2015 (Morgan, 2018, 2020). In 2023, the amount exceeded $8.15 trillion; more than $13.82 trillion is estimated in cybercrime costs by 2028 (Petrosyan, 2023). Increasingly, cybercriminals use sophisticated methods to breach systems and steal valuable data and funds. As the digital landscape expands with new technologies like cloud computing, IoT, and cryptocurrencies, so do vulnerabilities and opportunities for Cybercrime (Phipps, 2024). However, no single entity can address the existing complex and evolving challenges of Cybersecurity alone. Therefore, collaboration between key stakeholders, including industry, government, and academia, is critical for developing holistic and proactive solutions (The White House, 2023). In particular, industry-academia partnerships hold great promise for bridging gaps between research and practice to enhance Cybersecurity (Ahmed et al., 2022).

A recent review of the literature on industry-academia collaborations for Cybersecurity reveals several benefits and focus areas for these partnerships. Partnerships can help advance cybersecurity research and translate findings into impactful real-world solutions by bridging gaps between academic research and industry needs (Smyth et al., 2019). While universities often lack the practical context, companies frequently lack resources for foundational research. Activities like collaborative projects, staff exchanges, data sharing, and joint training programs can overcome these challenges (Ahmed et al., 2022). Strategic policies can catalyze impactful collaborations between industry and academia, but a measured approach may be required (World Economic Forum, 2020).

Vogel (2016) writes that industry-academia partnerships have a significant role in improving knowledge and awareness around the emerging issue of Cybersecurity. Strategic collaborations between government, academia, industry, and the private sector can breach the cybersecurity skills gap by ensuring that relevant cybersecurity skills are taught to students across all levels. The private sector and academia can collaborate to establish a US Cybersecurity challenge aimed at augmenting the pool of IT and cybersecurity professionals in the United States. This initiative seeks to bolster the nation's capacity to address and mitigate emerging cyber threats through proactive measures. Additionally, the author advocates for implementing cybersecurity challenges, competitions, and networking events to broaden access to career pathways within the cybersecurity sector. Such endeavors are pivotal in bridging the gap identified in the author's work. Pengulu, Lee & Muller (2012) posit that strategic partnerships between federal, state, and local governments, industry organizations, territorial-level private companies, and academic institutions can address cybersecurity issues.

Cooperation between the private sector and academia is a highly effective tool for achieving cybersecurity goals. The federal government has pursued collaborative efforts with academia and the private sector, bolstering the nation's cyber defense capacities. Encouraging the growth of these collaborations will help combat and eliminate the threat of Cybercrime for the years to come. Members of academia and the private sector should also be involved in the efforts to protect the nation's critical digital infrastructure by sharing information that can help prevent hostile acts of Cybercrime with them. In the past, InfraGard, an FBI program, has collaborated with the private sector and academia to increase the level of awareness on matters of Cybercrime and counterterrorism. Expanding such partnerships to involve the academic sector can improve the nation and make it more proactive in facing the threat of Cybercrime. Although the authors identify critical issues in such partnerships, they missed an opportunity to identify them.

Plunkett (2014) also affirms that robust partnering between the National Security Agency, government agencies, and academia can help build and develop the cyber workforce. Such partnerships provide opportunities for young people to acquire the skills and knowledge required to perform and execute a whole spectrum of cybersecurity and information assurance functions. Plunkett also notes that higher education in Cybersecurity and information assurance must be promoted to enable the nation to produce enough professionals with skills and expertise to address cybercrime vulnerabilities. It is also imperative that the United States and the rest of the World focus and direct their resources toward creating a broader and more technically diverse human workforce to meet the ever-evolving threat of cybersecurity challenges. The author

also ascertains that the role of academia in achieving cybersecurity awareness is critical. In partnerships with the NSA and the private sector, academia can help build strong cybersecurity curriculums that can benefit the nation from a cybersecurity perspective. The academic sector can also help develop an acceptable and desired level of cybersecurity resilience by embedding cybersecurity programs and curriculums in higher education.

Wang & Guo (2020) postulate that industry-academia partnerships- collaborations between the Department of Homeland Security, the Department of Education, the Department of Defense, the Office of the Director of National Intelligence, and the National Science Foundation- can help increase the nation's awareness of cybersecurity threats. Introducing cybersecurity education programs and higher education curricula can help train and produce cybersecurity professionals, cybersecurity researchers, and a country full of citizens aware of Cybersecurity. One way the education sector can improve the nation's Cybersecurity professional capacity is by holding annual cybersecurity championships that bring together all the institutions of higher learning. Such encourages college and university students to actively participate in cybersecurity construction and produce enough cybersecurity specialists to meet the growing needs of the information defense system. More importantly, countries worldwide should strive to provide excellent and sustainable continuing education and training opportunities for cybersecurity educators to improve their skills and knowledge. It is critical, considering that the field of Cybersecurity is evolving rapidly. Thus, according to cybersecurity trainers and educators, a continuous learning opportunity helps update their knowledge reserves, making them competent and qualified cybersecurity experts.

Critical areas to focus partnerships include secure software development, cloud security, network defense, cryptography, and AI/ML security. Such focus helps align research with current industry problems and provides innovative capabilities to improve cyber defenses (Tariq et al., 2023). Industry-academia partnerships also facilitate the development of Cybersecurity through shaping curricula and providing internships and training. The partnership is crucial to addressing the skills gap as companies struggle to find professionals with relevant expertise (Blažič, 2021). According to a 2022 Workforce Cybersecurity study, there were over 700,000 unfilled positions in the United States as companies struggled to recruit professionals with relevant hands-on skills while students lacked an understanding of real-world workforce needs (Eckert, 2023). Furthermore, governments have crucial roles in incentivizing partnerships through funding programs, grants, tax credits, and consortiums. However, some argue that balanced oversight is needed to avoid potential pitfalls, ensure academic independence, and develop sustainable skills programs (Pinguelo & Muller, 2012; Plunkett 2014; Vogel, 2016; Wang & Guo, 2020).

3. Methodology

This research examines the impact of industry-academia partnerships on cybersecurity training and awareness, focusing on collaborative approaches to enhance global cybersecurity measures. The study uses secondary research methodology to explore the roles of industry-academia collaborations in raising awareness and fortifying the World against cyber threats. The primary data collection method involves reviewing and analyzing existing literature from digital library databases, including IEEE Xplore, Google Scholar, and JSTOR. The study employs keywords such as Cybersecurity industry, cybersecurity collaborative approaches, academic partnership, Cybersecurity attacks, Cybercrime, and Cybersecurity research during a comprehensive literature search to identify significant challenges.

The selection criteria for research works are narrowed to those specifically related to collaborative approaches to Cybersecurity and Cybercrime, focusing on papers published between 2018 and 2021. However, the study also incorporates relevant seminal papers predating 2018. Literature sources are selected based on publication year and information quality. The reason for employing a secondary research methodology is multifaceted. Firstly, this approach facilitates evaluating, reviewing, and selecting pertinent literature sources, given their availability and accessibility online. Secondly, the secondary research methodology proves cost-effective, eliminating the need for fieldwork. Access to various academic search engines via an internet-enabled laptop provides the researcher with a wealth of credible and relevant sources.

4. Findings and Discussion

The findings presented from the literature review indicate that academia-industry partnerships play a vital role in raising cybersecurity awareness by empowering learners with skills and knowledge to mitigate the rising cybersecurity vulnerabilities. For example, Vogel (2016) notes that the US government, through the American National Security Agency (NSA), can work with academia to develop cybersecurity programs tailored to equipping young learners with skills and capabilities to enable them to combat the rising levels of Cybercrime.

These programs allow the country to build resilience and capacity in the digital arena. In the past, similar cybersecurity programs rolled out by the National Security Agency (NSA) in partnership with academia have borne the desired outcomes. These programs have also helped promote cybersecurity knowledge and awareness in higher education by producing qualified Cyberdefense professionals. Similarly, Wang & Guo (2020) agree that the increased production of cybersecurity professionals made possible by establishing a sustainable education system that provides education and training opportunities to cybersecurity educators can help reduce the vulnerabilities experienced across the US networks. This is by giving the learners and cybersecurity educators a sustainable and continuing framework that enables them to constantly hone, shape, and improve their cyberspace knowledge and skills.

Notwithstanding the current gaps in industry and academic partnership, there is a growing concern within Cybersecurity as a field, which is a worldwide shortage of qualified personnel who take roles in academia, industry, and government, therefore adding to the challenging risk issue already faced by the field. A recent study by the government and public sector of approximately 3.4 million shortfalls workers demonstrated an increase in shortage of about 26% from 2021 (ISC2, 2022). Although academia continues to train future cyber workers who can problem-solve and understand the design and use of technology and related trends and security risks they face, there continues to be a gap in the number of professionals entering the field (Vogel, 2016). The need for growth in such collaboration in industry, academia, and government is poignant here. The growth in Cybercrime demands workers who can work on cutting-edge technology to protect their respective countries against threats and address vulnerabilities in Information systems against future Cyber-attacks. Growth can be achieved through collaboration between these avenues to provide opportunities for minority women and retooling and skilling opportunities for other professionals, such as veterans.

The current growth of technology and digital resources in all aspects of society pushes the next frontier of vulnerability and threat landscape and avenues for threat actors with malicious intent. Unfortunately, the growth in technology and digital resources that have not yet been adopted into mainstream use or yet to be by the cybersecurity industry, academia, or government poses great and dire challenges and require cooperation and collaboration to begin to unearth vulnerabilities and threat in other to protect organizations, institution, or government. To address the challenge at hand, each of the identified areas has a role to play. Academic institution roles include training and adopting pedagogy to increase the required skills yet maintain the rigor necessary for Cyber professionals to solve complex problems in the field. At the same time, academic institutions must maintain the balance of improving enrollment and recruitment from some nontraditional student cohorts, such as programs and opportunities for minorities. The role also involves contributing to research and development of breakthrough technology to address some of the unresolved complex problems. Although some institutions have continued development in these areas, others have lagged in the research and development sphere. As stipulated by (Brooks, 2023), a school such as MIT, Cal Tech, University of Chicago, Harvard, Carnegie Mellon, and other research-intensive institutions continue to find avenues to conduct basic research and create a pipeline of scientists, engineers, and cybersecurity practitioners who care capable of commercializing the technology.

Resolving this issue is not only isolated to institutions but also the government has a role to play, including but not limited to policy foundation for adoption and use of new technology, promoting public and private partnership, developing best practices, and designing models to prototype and providing working avenues for both academia and industry to contribute to event programs. The government's role also serves as the foundation. It provides some level of resources and funding necessary to jumpstart addressing the pressing issues of vulnerability and threat in current and emerging technologies while at the same time developing comprehensive research and development programs and supporting git.

In the cybersecurity industry, roles include conducting research and development from some of the basic research academia has produced, offering a playback for innovation through some lessons and experiences, and sharing them with the industry for solutions. Industry investment and collaboration are also necessary for developing products and bringing products into being while developing talents. Such industry contributions include technology development, research and development in many areas, and collaboration with academia and government to discuss operational challenges.

Similarly, Blažič (2022) agrees that the education sector can help increase cybersecurity awareness by imparting learners at all levels the desired specialized skills and knowledge to help combat the rising threat of Cybercrime. The author argues that the United States should increase its cybersecurity training and education efforts by adopting new approaches. Strategic partnerships between academia and the private sector are crucial for

promoting and enhancing cybersecurity competence and resilience levels. The ultimate objective of such collaborations is to cultivate a skilled workforce comprising cybersecurity professionals and ICT experts. Blažič's research findings underscore that a significant factor hindering the nation's ability to achieve desired levels of cybersecurity awareness and resilience is the prevalence of theory-based education curricula rather than hands-on training approaches. Consequently, reorganizing and redefining educational and training pathways are essential steps toward bolstering the nation's capacity to cultivate cybersecurity professionals who can effectively address the evolving demands of cyberspace.

Plunkett's findings also affirm that the most effective way of achieving cyberspace's desired confidence and resilience is through robust partnering between academia, the private sector, government agencies, and industry. These partnerships help unveil the much-needed resources and experts that can help shape and mentor young learners, thus enhancing the nation's capacity to build a pool of sustainable cybersecurity professionals capable of meeting the needs and demands of the cyberspace sector. Plunkett (2014) also reveals that such partnerships are critical for creating the next generation of cybersecurity practices and standards, which will play a vital role in educating the future cyberspace workforce. Similarly, the Pinguelo Lee & Muller findings assert that cooperation between academia, the government, and the private industry can significantly help achieve cybersecurity training and awareness objectives and goals. Leaving the burden of achieving the desired levels of cybersecurity awareness and resilience to the education sector alone or the government can be costly. As such, the partnerships will aid in the efforts to help the nation bolster its cybersecurity defenses and capabilities.

5. Conclusion

This study significantly advances cybersecurity awareness and resilience by proposing innovative strategies fostering collaboration among industry, academia, and government entities. The study underscores the pivotal role of academia, in conjunction with government agencies and the private sector, in elevating national cybersecurity awareness. By actively participating in initiatives aimed at producing highly skilled IT professionals with requisite cybersecurity expertise, academia becomes a key driver in achieving this goal. The ongoing technological evolution underscores the escalating reliance on technology across various sectors. Organizations are increasingly adopting advanced technological solutions to harness the benefits of emerging technologies. Coordinating efforts for cybersecurity solutions becomes imperative to safeguard these technologies, thereby enhancing organizational efficiency, profitability, and competitive advantage.

Furthermore, this research highlights the feasibility of overcoming cybersecurity competency gaps, awareness deficits, and skill shortages by reshaping the current educational paradigm. Shifting towards a more practical, hands-on training approach rather than a theory-centric education model proves instrumental in bridging these gaps. Establishing robust strategic partnerships among academia, the private sector, and government agencies emerges as a vital catalyst, providing essential human capital and financial resources. These collaborations are integral to developing and implementing a revised educational curriculum tailored to producing a greater number of cybersecurity experts and professionals, effectively addressing the nation's pressing needs in the realm of Cybersecurity.

References

Ahmed, F., Fattani, M. T., Ali, S. R., & Enam, R. N. (2022). Strengthening the Bridge Between Academic and the Industry Through the Academia-Industry Collaboration Plan Design Model. *Frontiers in Psychology*, *13*. https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.875940

Alda,M.(2021).TheStatisticsPortal.Statista.https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#definition

Blažič, B. J. (2022). Changing the Landscape of Cybersecurity Education in the EU: Will the
New Approach Produce the Required Cybersecurity Skills? Education and information technologies, 27(3), 3011-3036.

Brooks, C. (2023, October 5). Academia, industry, and government can create innovative partnerships and Help Secure Our Digital Future. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/07/13/academia-industry-and-government-can-create-innovative-partnerships-and-help-secure-our-digital-future/?sh=362c83ca6730

Blažič, B. J. (2021). The cybersecurity labor shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, *67*, 101769. https://doi.org/10.1016/j.techsoc.2021.101769

Eckert, C. (2023). *U.S. Desperately Needs Cyber Talent, Congress Says*. https://www.nationaldefensemagazine.org/articles/2023/6/26/us-desperately-needs-cyber-talent-congress-says

ISC2, I. (2021, February 12). A critical need for cybersecurity professionals persists in the year 2022. https://media.isc2.org/. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in Cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Morgan, S. (2018, December 8). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Morgan, S. (2020, November 9). Cybercrime Damages $6 Trillion by 2021. *Cybercrime Magazine*. https://cybersecurityventures.com/annual-cybercrime-report-2017/

Olmstead, K., & Smith, A. (2017, 01 26). Americans and Cybersecurity. Retrieved from Pew

Research Center: https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/

Pinguelo, F. M., Lee, W., & Muller, B. W. (2012). Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow. Va. JL & Tech., 17, 75.

Plunkett, D. A. (2014). Achieving Confidence in Cyberspace in an Ever-Changing

Ecosystem. Journal of Information Warfare, 13(2), 1-7.

Petrosyan, A. (2023, December 19). Topic: U.S. consumers and Cyber Crime. Statista. https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/#topicOverview Ani Petrosyan,

Petrosyan, A., & Ten, O. (2023, October 10). The global average cost of a data breach by industry 2023. Statista. https://www.statista.com/statistics/387861/cost-data-breach-by-industry/

Petrosyan, A. (2023). *Global Cybercrime is estimated to cost 2028*. Statista. https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Phipps, B. (2024, January 2). *The Evolution of Cybersecurity: Staying Ahead of Emerging Threats - Bakersfield, Lancaster, Porterville*. Second Star Technologies. https://www.secondstartechnologies.com/2024/01/the-evolution-of-cybersecurity-staying-ahead-of-emerging-threats/

Pinguelo, F. M., & Muller, B. W. (2012). *Virtual Crimes, Real Damages Part II: What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow* (SSRN Scholarly Paper 2028457). https://papers.ssrn.com/abstract=2028457

Plunkett, D. A. (2014). Achieving Confidence in Cyberspace in an Ever-Changing

Ecosystem. Journal of Information Warfare, 13(2), 1-7.

Smyth, S. J., Curran, K., & McKelvey, N. (2019). The Role of Education and Awareness in Tackling Insider Threats: In I. Vasileiou & S. Furnell (Eds.), *Advances in Information Security, Privacy, and Ethics* (pp. 33–52). IGI Global. https://doi.org/10.4018/978-1-5225-7847-5.ch003

Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

The White House. (2023). *National-Cybersecurity-Strategy-2023.pdf*. https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Vogel, R. (2016). Closing the Cybersecurity Skills Gap. Salus journal, 4(2), 32-46.

Wang, W., & Guo, L. (2020, December). Cyber Security Training in Europe and America and its Enlightenment to China. In 2020, the 6th International Conference on Social Science and Higher Education (ICSSHE 2020) (pp. 377-382). Atlantis Press.

Wang, W., & Guo, L. (2020). Cyber Security Training in Europe and America and its Enlightenment to China: *Proceedings of the 2020 6th International Conference on Social Science and Higher Education (ICSSHE 2020)*. 2020 6th International Conference on Social Science and Higher Education (ICSSHE 2020), Xiamen, P.R. China. https://doi.org/10.2991/assehr.k.201214.073

World Economic Forum. (2020). *Partnership Against Cybercrime*. World Economic Forum. https://www.weforum.org/projects/partnership-against-cybercime/

World Economic Forum. (2022, December 2). *How to Develop the Global Cybersecurity Workforce Today*. World Economic Forum. https://www.weforum.org/agenda/2022/12/how-to-develop-the-global-cybersecurity-workforce-and-build-a-security-first-mindset/