International Journal of Global Tech Management (IJGTM)
Volume 2, Issue 1, January-June, 2025
Available online at: https://pgrpublication.com/index.php/ijgtm

Effectiveness of Cybersecurity Awareness Training in Tech-Driven Firms

Anand R. Mehta[1], Srikarthick Vijayakumar[2], Phani Pradyumna Somayajula[3], Jatin Vaghela[4], Sravan Kumar Pala[5]

[1,2,3,4,5]Independent Researcher, USA

Article history: Received: 25 January 2025, Accepted: 16 February 2025, Published online: 02 March 2025.

ABSTRACT

Security Education Training and Awareness plays a dynamic role for organizations in endorsing resources' thoughtfulness and accessibility. This paper determines the importance of security awareness training in dealing with cyber threats. This research uses the Technology Acceptance Model (TAM), indicating that at-risk employees' behavior and information security awareness training execution are successful interventions. Yet, those investigations did not examine Artificial Intelligence (AI) enabled training, so this study fills that literature gap. This analysis used a qualitative research design. The article examines employees' behavior and the effectiveness of AIbased security awareness training programs. The study here helps analyze information security awareness training in the workplace, encouraging behavioral transformations that would restrain data breaches by incorporating the users' exposure and the stringency of coercion and the retort to peril in prophesying behavior discretions.

Keywords: Cybersecurity, Risk culture, AI, Security Awareness Training

INTRODUCTION

One of the most pressing challenges emerging alongside technological innovation is the protection of digital environments from malicious intrusions [1]. There is a pressing requirement to establish robust security frameworks, starting from foundational levels such as municipalities and extending to broader government entities. This growing concern has made digital defense a pivotal topic within the field of information systems, especially in light of the rise of cyber collectives like Anonymous, whose intent is to disrupt governmental digital infrastructures [2]. Within organizations, it becomes the duty of system analysts to guide staff on cyber resilience, fostering a culture of awareness about the dangers lurking in digital realms and equipping them to make prudent, security-conscious choices [3].

The core focus of this paper is to explore educational and procedural initiatives that can be adopted to reinforce data protection and raise alertness to digital system weaknesses. The principal goal of the study is to empower organizational personnel with the knowledge of existing cyber threats and to instill practices that protect internal information architecture, by addressing both technological loopholes and behavioral vulnerabilities that could be exploited. An additional objective is to pinpoint fragile links within the organizational security framework that could serve as potential gateways for breaches. However, the research must contend with a significant hurdle—the constant evolution of digital threats and the parallel advancement of defensive technologies, which may outpace implemented solutions.

BACKGROUND AND CONTEXT

The rapid expansion of the tech industry has indeed transformed the way we live, work, and The modern world is undergoing a profound shift in how individuals connect and operate within digital ecosystems. This evolution is primarily fueled by breakthroughs in fields like artificial intelligence, data-driven algorithms, and remote computing infrastructure. These innovations have significantly reshaped multiple industries, introducing new avenues for professional development and fostering economic progress. Yet, despite these technological leaps, marginalized communities frequently encounter obstacles that prevent them from accessing the essential capabilities and tools needed to participate in and benefit from this digital transformation (Yu, et al., 2017; Zachariadis, Hileman & Scott, 2019).This disparity, widely known as the digital gap, stems from intersecting issues such as unequal distribution of resources, gaps in academic preparation, and ingrained institutional discrimination, all of which restrict opportunities to acquire and engage with modern technologies (Kuerbis et al., 2017). Closing this gap requires enhancing digital competence, which encompasses a broad spectrum of knowledge areas essential for navigating the digital environment. These capabilities extend beyond foundational tech usage to include skills such as discerning credible information, critical online reasoning, and effective virtual collaboration.

As innovation in digital platforms continues to accelerate, the role of digital fluency becomes more significant—it equips individuals with the tools to effectively adapt and succeed in a dynamic technological world (Malloy & Smith, 2019). Additionally, knowledge of digital safety protocols has become indispensable. In a world increasingly susceptible to online threats, users must be equipped to detect malicious online activities such as deceptive emails and malicious websites, and adopt behaviors that ensure the integrity of personal data and digital interactions (Chandarman& Niekerk, 2017; Rahman et al., 2020).

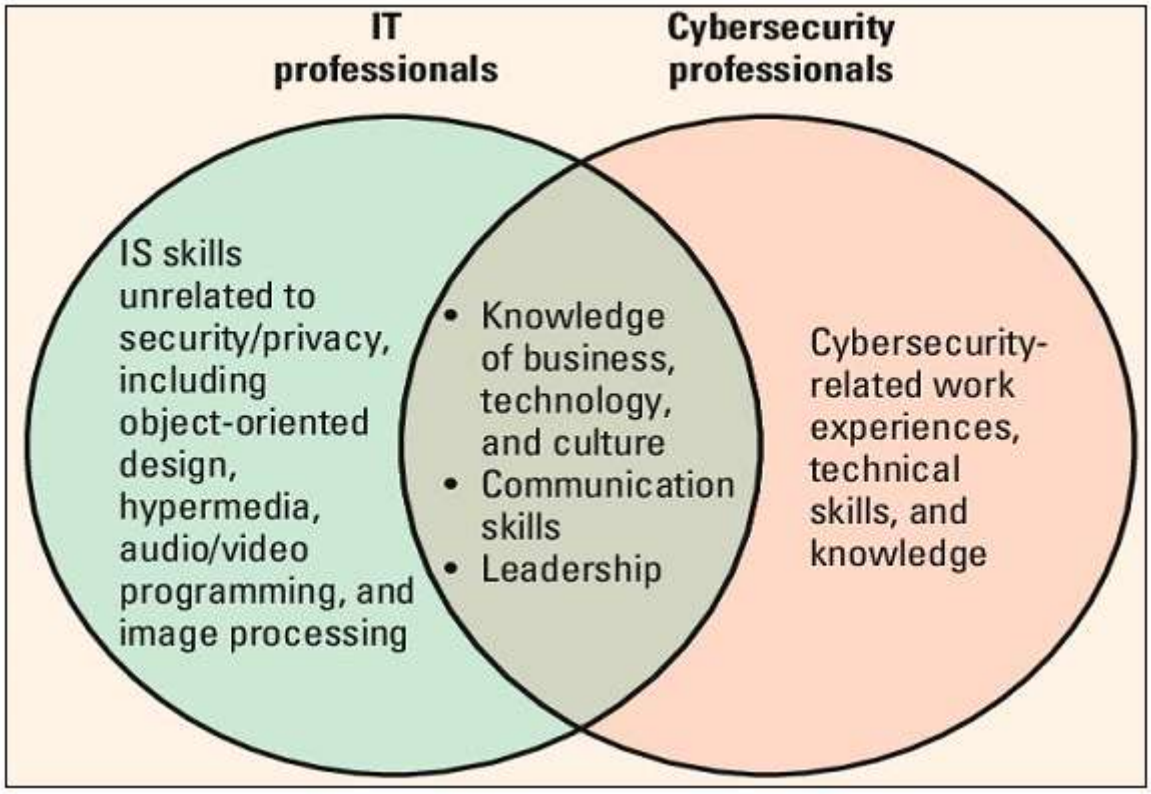

Fig 1: Factors affecting career advancement of women in IT versus those in cybersecurity (Bagchi-Sen, et al., 2010).

The challenges impeding marginalized communities from acquiring digital competencies are layered and deeply rooted. A primary obstacle is the limited availability of devices and reliable internet, especially in economically disadvantaged and remote locations where connectivity remains inconsistent or absent. This initial technological shortfall creates a significant hurdle, restricting individuals from engaging with tools essential for digital fluency and knowledge of cybersecurity principles, thereby deepening pre-existing disparities (Brough et al., 2020). Compounding this issue are disparities in the education system, where institutions serving underfunded populations often lack both the hardware and specialized instruction needed to teach digital subjects effectively. The scarcity of qualified teachers and the absence of modern digital infrastructure curtail opportunities for learners to acquire vital skills, leaving them at a disadvantage in an increasingly digital workforce (Adrion et al., 2010).

Additionally, entrenched structural inequalities contribute to sustaining the technological skills gap. Biases in recruitment and career advancement practices have historically excluded women, ethnic minorities, and other marginalized groups from technical domains. The resulting lack of diversity and visible leadership within these sectors discourages participation and hinders the development of mentorship networks that are instrumental for career growth in tech-driven professions (Kuerbis et al., 2017; Montgomery, 2013). Confronting and dismantling these barriers is key to building a more inclusive digital ecosystem that actively promotes engagement from a variety of social backgrounds (Ruiz, 2020; Adrion et al., 2008).

The intersection of digital competency and cybersecurity understanding holds transformative potential for historically excluded populations. As digital tools increasingly influence both economic activity and daily interactions, individuals equipped with relevant skills gain greater access to employment opportunities and upward mobility. Furthermore, raising cybersecurity awareness among these communities is vital to ensuring not only their digital safety but also the protection of sensitive organizational data—particularly in sectors reliant on secure information systems

(Chandarman& Niekerk, 2017; Rahman et al., 2020). Ensuring equitable access to digital learning pathways and technological tools can facilitate full participation in the evolving digital economy and help democratize opportunities in science, technology, and innovation (Charleston, 2012).

To summarize, bridging the digital skills gap for marginalized populations is essential to achieving a diverse and resilient tech workforce. Though these challenges are substantial, coordinated efforts and multi-sectoral partnerships can help eliminate these inequities (Al-Ali et al., 2016; Jones et al., 2020). Equipping disadvantaged individuals with practical digital tools and cyber-awareness not only improves security and inclusion but also builds a foundation for a fairer and more balanced technological future.

THEORETICAL FRAMEWORK

This study report included comprehensive analysis and examination of peer-reviewed articles and literature about behaviours and practices in cybersecurity, including organisational security as well as government and military information security [2]. An interest was expressed in peer-reviewed research papers and articles that examine cybersecurity risks to organisations and the optimal techniques for protecting the organisation from external attacks by enhancing employee awareness on the subject. The academic publications were particularly helpful in elucidating the significance of information security. The majority of the papers presented a bottom-up strategy by ensuring that every employee is informed on the latest security best practices. If each person fulfils their specific role in this security chain, the whole organisation will remain secure.

A chain's strength is determined by its weakest link. [4]. Inadequate information security practices among current and former employees of the organisation have been the primary source of cyber threats, vulnerabilities, and breaches, with 72% to 95% of these threats originating from these individuals, as indicated by research findings from Price Waterhouse Coopers [5, 6, 23]. The majority of assaults occur via unsupervised internet use, when information systems are compromised by malware. Malware is a prevalent instrument used by hackers to execute attacks and exploit vulnerabilities systematically. A notable vulnerability to a system is the possibility of human mistake, referred to as social engineering, when individuals are coerced into divulging critical system information, including their authentication credentials. Even the most sophisticated systems may be compromised by social engineering techniques, including phishing, vishing, and impersonation [7]. Therefore, people inside the organisation must get current cybersecurity protection skills and understanding of countermeasures [8].

TECHNOLOGY ACCEPTANCE MODEL

This research used the Technology Acceptance Model (TAM) to assess the factors. In 1989, the author Davis developed the technology adoption model, which played a significant role in information management. Davis et al. characterise the TAM model as a framework used to delineate the drivers of computer adoption that is dominant and capable of elucidating user behaviour across a wide spectrum of end-users. In the first edition of the Technology Acceptance Model (TAM) (refer to Figure 1), the word 'attitude' includes an additional connotation shaped by technology and its use. The TAM defines "attitude" as the phase in which the end-user has aggressive (or negative) opinions of the technology or process.

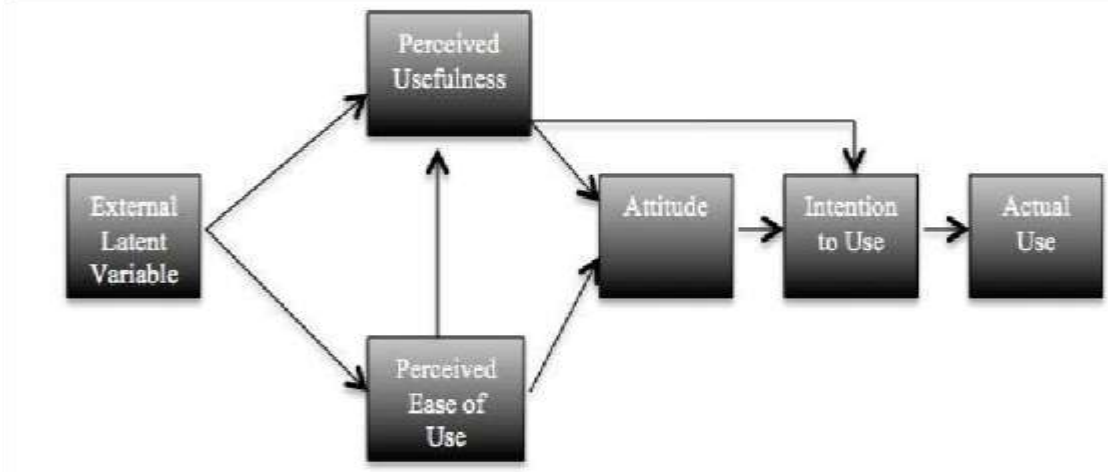

Fig -2: Technology Acceptance Model: Initial Version

TAM'S MODIFICATION

Employing the original TAM model, investigators executed many analyses. Davis et al. (1989) authenticated that perceived usefulness and ease of usage undeviatingly influence a new variable: behavioral intention [9]. Venkatesh and Davis (1996) eradicated the attitude variable and replaced it with behavior intention to develop the TAM's final version (see Figure 2) after further testing [10]. In both TAM's older and new versions, external variables are crucial in demonstrating perceived usefulness and ease of use. External variables usually entail user training, user engagement throughout the study, and execution [11].

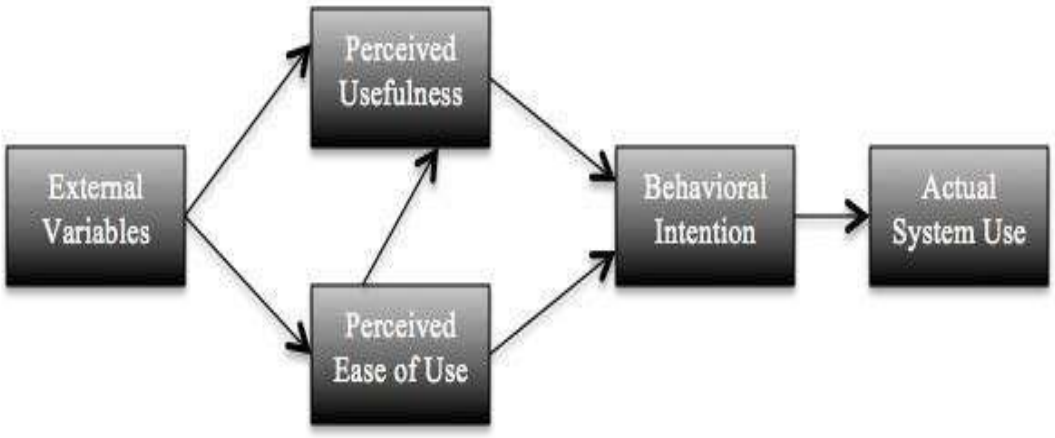

Figure 3 represents the finalized form of the Technology Acceptance Model, emphasizing the essential role of cybersecurity awareness within institutional frameworks. This awareness reflects how well-prepared an organization is to handle digital threats and the extent to which its personnel are knowledgeable about such dangers [12]. For cybersecurity consciousness to be considered embedded, both the workforce and the institution must be exposed to various threat scenarios, gaining insight into the origins, impacts, and preventive responses associated with each potential risk [13]. This exposure instills a sense of personal accountability across departments, reducing the reliance on information system officers as the sole custodians of data security.

Addressing technological threats requires not only proactive barriers but also robust reactionary strategies. These may include fostering employee vigilance, implementing structured Security Education, Training, and Awareness (SETA) initiatives, and deploying surveillance mechanisms and user restrictions [14]. Consequently, it becomes essential for companies to identify the cyber risks they are most vulnerable to and tailor strategic responses by drafting detailed cybersecurity protocols and digital safety frameworks.

No matter how sophisticated a firm's technological defenses—be it next-generation firewalls, or advanced detection and prevention systems—they can all fall short without factoring in the human dimension. Workers must be educated and enabled to defend both their personal interfaces and broader network systems [15]. SETA programs frequently utilize methods that demonstrate real-world attack scenarios to convey the seriousness of digital threats and their consequences, often employing impactful approaches such as persuasive visuals or scenario-based learning [16]. Combining virtual modules with hands-on workshops ensures that crucial safety practices are retained and internalized.

The format of awareness training may vary across different corporate environments based on staff composition, but the priority remains consistent: all participants must recognize the potential consequences of individual negligence on organizational safety. To be truly impactful, these programs must be aligned with internal security frameworks and risk mitigation policies. Fundamental elements, including protocols for protecting data, recognizing shared exposure points, and managing credentials, should form the core of the program's curriculum [17]. As a guiding reference, ISO/IEC 27002 [18] offers a comprehensive set of standards for establishing effective information protection guidelines, which can be adapted even by entities with unique operational requirements.

SETA DESIGN AND ITS EFFECTIVENESS

Although many companies are increasingly adopting programs aimed at enhancing employee awareness regarding digital threats, there is still limited empirical evidence available to evaluate the tangible effects of these initiatives on workplace dynamics [19]. Serving as a foundational layer within an organization's information security architecture, awareness training is considered a critical initial step. For such initiatives to be truly impactful, the theoretical approach behind them must fulfill three essential criteria—Consistency, Synergy, and Substitutability [20]. Additionally, these

awareness frameworks must strike a balance between cost-efficiency, high accessibility, and the level of protection they deliver. While some training models are highly sophisticated, they often overlook foundational components—such as the complete structure and cycle of phishing education modules. Fundamental principles for a successful awareness initiative include straightforward messaging and minimal intrusion. Therefore, training should aim to educate without heavily interfering with employees' daily routines. Innovative approaches like gamified cybersecurity modules have recently shown promising results, particularly in increasing digital security comprehension among learners [21].

However, an excessive dependence on awareness programs can be problematic. Some enterprises integrate these initiatives so deeply into their security culture that they begin to overestimate their effectiveness. As noted by Proctor [22], the central issue arises when companies view these awareness models as all-encompassing solutions for data breaches. Such unrealistic expectations, especially from upper management, can potentially undermine a balanced and proactive security framework.

To achieve meaningful outcomes, security education must be tailored to individual behavioral responses and should fundamentally reinforce the core principles of digital protection—Confidentiality, Integrity, and Availability (CIA) [23]. Organizations that successfully implement such structured initiatives, which bolster employee adaptability and resilience in the face of evolving threats, are on the right path to cultivating a robust cybersecurity posture.

USE OF AI IN CYBERSECURITY TRAINING

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools for contemporary businesses in understanding and combating digital security risks. These technologies are employed in both proactive and reactive strategies to address cyber vulnerabilities. With AI now deeply integrated into nearly every digital framework, experts caution that its malfunction—particularly in high-stakes environments like finance—could lead to irreversible consequences [24]. This concern raises an essential pedagogical question: what is the most effective way to incorporate AI into cybersecurity learning and practice?

Researchers propose two instructional pathways to address this challenge: (1) maintaining a conventional focus on cybersecurity fundamentals while introducing AI elements where applicable, and (2) centering the entire cybersecurity curriculum around AI-driven capabilities [25]. The first route serves learners aiming for a broad, foundational grasp of the cybersecurity landscape. In contrast, the second is better suited for industry professionals seeking advanced, AI-powered defense mechanisms against evolving cyber threats.

In recognition of the growing need for widespread cybersecurity awareness, a variety of Massive Open Online Courses (MOOCs) have been launched to equip both novices and experts with relevant knowledge. However, these offerings frequently fall short in delivering hands-on, applicable strategies to counter real-world threats. As a result, numerous organizations have begun designing customized training modules to meet their specific security needs and operational contexts.

NICE FRAMEWORK AND VICYBER MODEL

In an effort to design the best cybersecurity curriculum using AI tools, organizations are using the models developed by the National Institute of Standards and Technology (NIST), USA. The effective model developed by NIST is called the National Initiative for Cybersecurity Education (NICE) framework. It is a fullproof model developed by industry experts and academicians for cybersecurity education, training, and workforce development [26]. The NICE framework consists of seven categories, 31 specialty areas, and 369 Knowledge. Skills and Abilities areas (KSAs), 65 competencies, and 444 tasks under various specialty areas [27]. Hodhod et al. [27] described the detailed NICE framework as shown in Figure 3, and it has a wide acceptance in many industries.

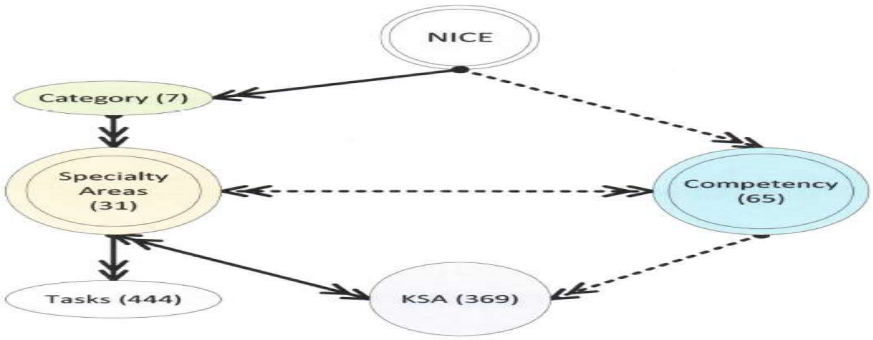

Fig-4: NICE framework diagram

The NICE framework broadly guides curriculum development, but significant companies face difficulties using it due to the lack of domain experts who can utilize it to the fullest. The large competencies need to be considered along their relationships to develop a practical framework. To overcome this challenge, Amazon presents a cloud-based system: viCyber, an intelligent system capable of rapid cybersecurity curriculum and training development using AI and visual mappings [28]. This service can be used anytime and anywhere to develop, train, and collaborate easily when keeping the infrastructure safe from threats. The viCyber model design is governed based on the NICE framework with feedback and recommendation engine considering user perspective [27, 29]. This AI-based model has a decision support system based on the human-computer interaction to describe the building up process, which helps to modify the conceptual understanding of the user when going through the training with real-time feedback.

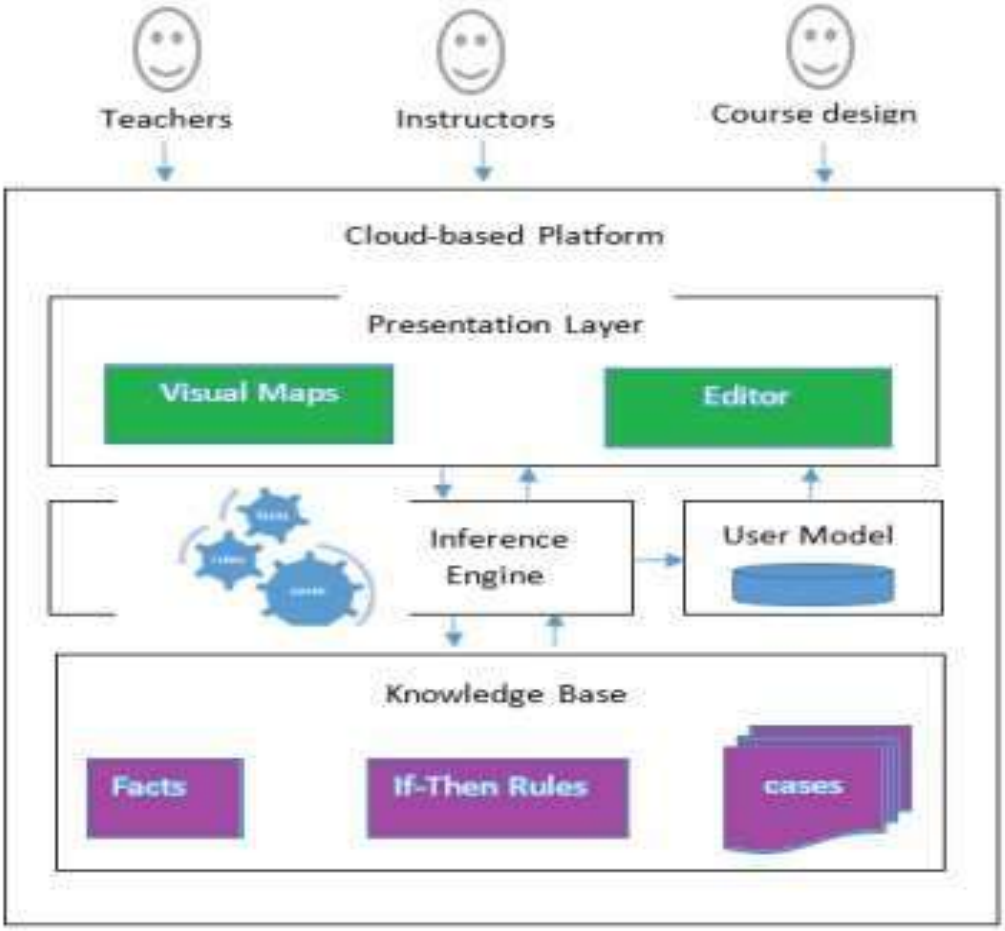

Fig-5: viCyber architecture with AI-enabled rules engine [27]

Note: Adapted from Cybersecurity curriculum development using AI and decision support expert system, by Hodhod, R., Wang, S., & Khan, S., 2018, International Journal of Computer Theory and Engineering, 10(4), 111. Copyright 2018 by International Journal of Computer Theory and Engineering.

USABILITY AND RELIABILITY OF VICYBER TOOL

This viCyber smart system presents a work in progress to develop cybersecurity curricula rapidly and reliably. This project contributes to changing the status of cybersecurity education by helping instructors develop the best cyber security programs. The viCyber uses a twodimensional visual mapping technique that maps competencies with KSAs. The visual mapping connects the knowledge base with the skills and abilities of the NICE framework. The learners will select the specialty areas according to the skill levels that they should master to succeed in the cybersecurity market. Each course in viCyber is an incremental tree according to the expert level of course content. The evaluation piece in viCyber framework measures how good the curriculum design is and what level of audiences should attempt the particular training [27, 30]. Overall, the feedback with scores explains user expertise levels for further recommendations on how to make the design better. The output module in the viCyber tool gathers data from the curriculum and push to the cloud for future performance evaluation. Also, the powerful feature of this tool is its reusability to accommodate the existing curriculum as per industry needs. Users can match their behavior to fetch the highest matching curriculum using the nearest neighbor classification algorithm to match the course's tags and

keywords [30]. This system can store the peerreview curriculum following the NICE framework using AI. The automatic curricula evaluation in this tool provides users with confidence to design and redesign modules as time passes.

CASE STUDIES AND PILOT PROGRAMS

Bridging the digital divide through enhanced cyber awareness and digital proficiency among marginalized communities has become a pivotal component of creating an equitable technological ecosystem. In recent years, several targeted initiatives have emerged to empower individuals from underrepresented backgrounds with the tools, knowledge, and confidence needed to participate fully in a digitally driven economy (Ibrahim, 2015; Tezel et al., 2020). These efforts have not only equipped participants with relevant skills but also fostered inclusivity by creating pathways to careers in technology. By examining such transformative programs, we gain insight into how strategic education and training can serve as catalysts for societal change.

One particularly notable example is the Digital Literacy Program established by the National Digital Inclusion Alliance (NDIA), which aims to reduce the technological gap by offering tailored digital education to low-access populations across the United States. NDIA's approach ranges from foundational computing tutorials to more nuanced topics such as online privacy practices and safe digital communication (Kabirifar&Mojtahedi, 2019; Thamrin, 2017). Its collaborations with grassroots organizations, libraries, and learning centers have been instrumental in ensuring that these services reach individuals who might otherwise be excluded from technological progress. By addressing basic competencies like navigating the internet, utilizing communication platforms, and responsibly managing digital assets, NDIA has enabled participants to experience tangible improvements in their ability to access remote education, employment resources, and government services. These gains have proven especially valuable among socioeconomically disadvantaged populations, senior citizens, and persons with disabilities, reflecting the program's broader mission to democratize digital access.

In parallel, the Creating IT Futures Foundation, established by Comp TIA, has spearheaded efforts to introduce cybersecurity knowledge to individuals from historically marginalized backgrounds. Targeting minority and low-income participants, the foundation's curriculum encompasses a full spectrum of instruction—from rudimentary IT principles to complex cybersecurity concepts, including safeguarding data, identifying threats, and securing networks (Liu, Wang & Wilkinson, 2016; Thumburu, 2020). What distinguishes this initiative is its commitment to experiential learning. Through simulated scenarios, interactive labs, and real-time problem-solving, participants are immersed in environments that mimic industry conditions. Supplementary services such as mentorship and career navigation ensure holistic development, equipping learners not just with hard skills but also with the social capital needed to succeed in tech-oriented careers. Hundreds have transitioned into cybersecurity roles through this route, entering positions within major enterprises, governmental bodies, and nonprofit sectors. The dual focus on addressing the cybersecurity labor shortage and promoting inclusion illustrates the effectiveness of such structured interventions (Micheli & Cagno, 2016; Toutounchian et al., 2018).

Smaller-scale but equally impactful programs have also emerged, often with highly targeted missions. The Women in Cybersecurity (WiCyS) initiative, for example, has made significant strides toward increasing female participation in the cybersecurity domain. Through offerings such as scholarships, structured mentorship, and access to networking opportunities, WiCyS assists women in navigating and establishing themselves within what has traditionally been a male-dominated arena (Mohanty, Choppali&Kougianos, 2016; Van Zyl, Mathafena& Ras, 2017). The program's annual conferences serve not only as networking hubs but also as platforms for celebrating the contributions of women in cybersecurity, thereby encouraging broader participation. A growing number of women have pursued certifications and technical degrees as a result of their involvement with WiCyS, indicating the initiative's effectiveness in both skill development and confidence building. The emphasis on guidance, community, and visibility underscores the vital role of supportive ecosystems in enabling women to ascend in tech-centric professions.

Likewise, the Techbridge Girls Program addresses STEM inequities by focusing on adolescent girls from marginalized demographics. This initiative integrates digital skill-building with after-school and seasonal workshops in subjects like robotics, programming, and web design. By facilitating hands-on learning in a collaborative setting, Techbridge encourages participants to engage actively with technological problem-solving while simultaneously nurturing self-efficacy (Vehviläinen, 2019; Vilasini, Neitzert& Rotimi, 2011). The program also underscores the importance of early exposure, aiming to ignite a lasting interest in scientific inquiry and innovation during formative years. This strategy has yielded a measurable uptick in the number of program graduates who pursue university-level education and careers in STEM fields, affirming the value of early and sustained engagement in fostering future technologists.

Evaluating the outcomes of these programs requires looking at both immediate educational gains and long-term socio-economic impacts. NDIA's initiatives, for instance, include diagnostic assessments before and after program completion to monitor changes in digital competency, such as effectively handling email communication, completing

web-based forms, or conducting virtual job hunts. Many participants report heightened confidence and improved navigation of online environments following the training (Abdallah &Alnamri, 2015; Osland, 2017). Furthermore, longitudinal follow-ups reveal that numerous graduates have capitalized on their newfound abilities to enroll in online courses or secure employment, showcasing how foundational digital education can lead to upward mobility.

Similarly, CompTIA's Creating IT Futures Foundation collects extensive feedback to evaluate the real-world applicability of its training modules. The program's high job placement rates—often within months of graduation—reflect the strong alignment between the instruction provided and the requirements of the cybersecurity workforce. In addition, regular consultations with employers help validate the preparedness of alumni, bolstering the program's reputation as a viable solution to the skills gap in information security (Abu-Nimer & Smith, 2016; Pasic, 2020). This dual metric of employment outcomes and industry feedback confirms the program's success in nurturing both technical acumen and workforce readiness.

WiCyS also utilizes a data-driven approach to track its impact. Metrics such as the rise in women attaining cybersecurity qualifications, the number of employment offers received, and the incidence of female leadership in tech firms provide a snapshot of the program's effectiveness. Participant testimonials often cite WiCyS as instrumental in shaping their professional journey, from expanding their networks to securing promotions (Ora, 2016). These qualitative and quantitative insights collectively affirm the initiative's contribution to gender equity within the digital security field.

For Techbridge Girls, key indicators include not just enrollment in STEM programs but also qualitative shifts in attitudes toward tech disciplines. Many participants show increased enthusiasm and confidence in their ability to thrive in science and technology, with follow-up data pointing to a marked rise in female representation in computer science and engineering studies (Ora, 2016). Such metrics are vital in understanding how early encouragement and skill-building can translate into tangible career paths for historically overlooked groups.

Ultimately, these case studies reveal that impactful training and education programs can drive systemic change when designed thoughtfully. Initiatives from NDIA, CompTIA, WiCyS, and Techbridge Girls offer compelling evidence that targeted, inclusive approaches to digital literacy and cybersecurity awareness can transform not only individual lives but also the broader workforce landscape (Anttila, 2015; Steers &Nardon, 2014). The use of comprehensive assessment tools—ranging from knowledge retention evaluations to job placement metrics—ensures that these efforts remain outcome-oriented and responsive to evolving technological needs. As digital technologies become ever more central to economic and social life, expanding access to these kinds of programs will be critical in ensuring no community is left behind in the digital revolution.

SUMMARY AND CONCLUSION

The issue of cybersecurity is prime among individuals and professionals of all domains. The main aim of this research study was to figure out the best method of planning and implementing cybersecurity awareness programs among users and employees in organizations. To do this, research was conducted to answer the questions; Who or what is the weakest link in the security chain? What are the necessary components to develop positive security habits? What are the employee's responsibilities for protecting the company's assets? The results were found, and the weakest link in the security chain of any organization was determined to be the least aware employee in the organization. This employee's behavior can be defined as the measure of the strength of the information system, as a lack of awareness can bring down even the most reliable information systems. The second question in the research was determined to be by developing a SETA program that was custom to the organization. The last result was that each employee is responsible for the organization's security. By using a bottom-up approach where each employee is accountable for their section of the information system by the end of it, the whole system would be secure. The viCyber tool with the NICE framework is somehow the best workable framework in the marketplace to build a robust training and feedback system. The use of AI-enabled behavioral security training is rising in some startups and hi-tech firms that are gaining more popularity with young audiences as it studies an employee's behavior for a few days or weeks before prompting to take the training. This paper will motivate future scholars and guide them to build their SETA model integrating AI, Deep learning, and Natural language processing (NLP) for better outcomes.

REFERENCES

[1]. Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). Social engineering in social networking sites: How good becomes evil. Proceedings of the Pacific Asia Conference on Information Systems, 1–10.
[2]. Ansari, M. F. (2021). The relationship between employees' risk scores and the effectiveness of the AI-based security awareness training program (Doctoral dissertation, University of the Cumberlands).

[3]. EA Bhardwaj, RK Sharma, EA Bhadoria, A Case Study of Various Constraints Affecting Unit Commitment in Power System Planning, International Journal of Enhanced Research in Science Technology & Engineering, 2013.
[4]. Preet Khandelwal, Surya Prakash Ahirwar, Amit Bhardwaj, Image Processing Based Quality Analyzer and Controller, International Journal of Enhanced Research in Science Technology & Engineering, Volume 2, Issue 7, 2013.
[5]. Bhardwaj, Amit. "Literature Review of Economic Load Dispatch Problem in Electrical Power System using Modern Soft Computing," International Conference on Advance Studies in Engineering and Sciences, (ICASES-17), ISBN: 978-93-86171-83-2, SSSUTMS, Bhopal, December 2017.
[6]. Singh, V., & Yadav, N**.** (2024). Enhancing Capacity Planning in Data Centers through Probabilistic Workload Modeling. (2024). International IT Journal of Research, ISSN: 3007-6706, 2(2), 15-21. https://itjournal.org/index.php/itjournal/article/view/15
[7]. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
[8]. Ghazvini, A., & Shukur, Z. (2016). Awareness training transfer and information security content development for healthcare industry. International Journal of Advanced Computer Science and Applications, 7(5), 361–370.
[9]. Goode, J., Levy, Y., Hovav, A., & Smith, J. (2018). Expert assessment of organizational cybersecurity programs and the development of vignettes to measure cybersecurity countermeasures awareness. Online Journal of Applied Knowledge Management, 6(1), 67–80.
[10]. Banerjee, Dipak Kumar, Ashok Kumar, and KuldeepSharma."Artificial Intelligence on Supply Chain for Steel
[11]. Demand." International Journal of Advanced Engineering Technologies and Innovations 1.04 (2023): 441-449. [32]. Kandlakunta, Avinash Reddy and Simuni, Govindaiah, Cloud-Based Blockchain Technology for Data Storage and Security (December 02, 2024). Available at SSRN: https://ssrn.com/abstract=5053342 or http://dx.doi.org/10.2139/ssrn.5053342
[12]. Hodhod, R., Wang, S., & Khan, S. (2018). Cybersecurity curriculum development using AI and decision support expert system. International Journal of Computer Theory and Engineering, 10(4), 111.
[13]. IBM Global Technology Services. (2014). IBM security services 2014 cybersecurity intelligence index. http://www-03.ibm.com/security/services/2014-cybersecurityintelligence-index-infographic/
[14]. ISO/IEC. (2013). ISO/IEC 27002:2013 - Information technology—Security techniques—Code of practice for information security controls. https://www.iso.org/obp/ui/#iso:std:isoiec:27002:ed-2:v1:en
[15]. Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning (EduLearn), 12(1), 150–158.
[16]. Kranz, J., &Haeussinger, F. (2014). Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. International Conference on Information Systems, Auckland, New Zealand.
[17]. Landress, A. D., Parrish, J., & Terrell, S. (2017). Resiliency as an outcome of SETA programs. In Proceedings of the 23rd Americas Conference on Information Systems, Boston, MA.
[18]. Lin, W. C., &Saebeler, D. (2019). Risk-based vs. compliance-based utility cybersecurity—a false dichotomy? Energy Law Journal, 40(2), 243–282.
[19]. **Yadav, N.** (2024). "A Study on AI-Driven Predictive Maintenance for Distributed Systems". International Journal of Global Tech Management, vol. 1, no. 1, Mar. 2024, pp. 1-14, https://pgrpublication.com/index.php/ijgtm/article/view/2.
[20]. Lykou, G., Anagnostopoulou, A., &Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. Sensors, 19(1), 19. https://doi.org/10.3390/s19010019
[21]. NIST. (2017, April 8). National Institute of Standards and Technology. https://www.nist.gov/
[22]. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of Internet security. Journal of Homeland Security & Emergency Management, 15(3), NP.
[23]. Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. Journal of Information Systems Education, 26(4), 281–294.
[24]. PricewaterhouseCoopers. (2016). The global state of information security survey 2016. http://www.pwc.com/gx/en/issues/cybersecurity/information-securitysurvey.html
[25]. Proctor, W. R. (2016). Investigating the efficacy of cybersecurity awareness training programs (Unpublished master's thesis). Utica College, New York.
[26]. Amit Bhardwaj. (2023). Time Series Forecasting with Recurrent Neural Networks: An In-depth Analysis and Comparative Study. Edu Journal of International Affairs and Research, ISSN: 2583-9993, 2(4), 44–50. Retrieved from https://edupublications.com/index.php/ejiar/article/view/36
[27]. Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. Decision Sciences, 27(3), 451–481.
[28]. Wang, P., & Kelly, W. (2015). A novel threat analysis and risk mitigation approach to prevent cyber intrusions. Colloquium for Information System Security Education (CISSE, 3), 157–174.

[29]. Yampolskiy, R. V., & Spellchecker, M. (2016). Artificial intelligence safety and cybersecurity: A timeline of AI failures. arXiv preprint arXiv:1610.07997. https://arxiv.org/abs/1610.07997

[30]. Laato, S., Farooq, A., Tenhunen, H., Pitkamaki, T., Hakkala, A., & Airola, A. (2020). AI in cybersecurity education—A systematic literature review of studies on cybersecurity MOOCs. In 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT) (pp. 6–10). https://doi.org/10.1109/ICALT49669.2020.00009