Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 11, 2025

HUMAN-CENTRIC CYBERSECURITY: A REVIEW OF ADAPTIVE AWARENESS AND BEHAVIORAL APPROACHES TO DATA PRIVACY

Mehwish Javed[*1], **Sana Iqbal**[2]

[*1]*Department of Software Engineering, National University of Modern Languages, Islamabad*
[2]*Department of Computer Science, COMSATS, Islamabad*

[*1]mehwish.javed@numl.edu.pk, [2]sanakhanzadi86@gmail.com

DOI: https://doi.org/10.5281/zenodo.17528416

Keywords
Human-centric cybersecurity, adaptive awareness, behavioral approaches, gamification, AI personalization, data privacy.

Article History
Received: 13 September 2025
Accepted: 23 October 2025
Published: 05 November 2025

Corresponding Author: *
Mehwish Javed

Abstract

The evolution of digital technologies and artificial intelligence has amplified cybersecurity and data privacy challenges, making human behavior a central concern in contemporary protection frameworks. This study explores human-centric cybersecurity through adaptive awareness and behavioral approaches, emphasizing the role of individuals in mitigating cyber risks. Human factors such as cognition, stress, and social influence significantly shape cybersecurity vulnerabilities and resilience. Adaptive awareness models like iCAT integrate gamification, simulations, and real-time feedback to enhance learning, engagement, and retention among users. Behavioral strategies, including psychological nudges, incentives, and transparent privacy communications, further influence secure online behavior. The research highlights the critical intersection between human psychology, education, and technology, arguing that effective cybersecurity depends not only on technical systems but also on adaptive human engagement. Future directions underscore the integration of AI-driven adaptive learning, continuous monitoring systems, and global data privacy regulations to develop proactive, ethical, and resilient cybersecurity ecosystems.

INTRODUCTION

Prioritizing individuals is critical in protecting individuals' personal data. This is because understanding people's behaviors, relationships, and decisions in the context of data vaults is essential. More than data technology risks, human behavior, and data vault interaction trends are the most critical risks in data privacy. For instance, sophisticated Artificial intelligence (AI), systems and the Internet of Things tools and technologies are currently inadequately reviewed data privacy spillover risks (Huang *et al.*, 2022; Sivakumar *et al.*, 2024). Human behavior focused will allow data privacy protection systems the needed balance of transparency, control, and consent. Third, human centric computing involves adjusting protections of personal data according to personal data vault interaction tendencies and systems and technologies. For instance, data seams and silos are technologies systems that could easily enable users to trade data and information silos. Personal data and information systems can exploit users at any moment and give personal data vault holders the permission to exploit data holders. User education on data protection and the prediction of data and information system exploitation is very crucial (Sivakumar *et al.*, 2024).

This would also improve security mechanisms that recognize human error as a weak point in the system. In cloud computing and visual sensor networks which require security against improper disclosure of sensitive information, it is critical to design systems where the user can configure security features in a safe and error-proof manner (Raja, 2024; Winkler & Rinner, 2014). Integrating ethical considerations and user-centered design in the context of privacy-centered mechanisms in AI and big data environments corresponds with the human-centric strategy in data protection. For example, implementing the GDPR not only serves a compliance function, but also protects privacy in an active and positive manner through the enhancement of transparency and accountability (Zangana *et al.*, 2025).

There are a number of demonstrable human-centered strategies which have become critical owing to a number of core challenges. In health systems, as complexity increases, it is more difficult to achieve and maintain a patient-centered focus. The human-centered design discipline enables systems thinkers to drive the implementation of more patient-centered interventions in pharmacy and health services (Flood *et al.*, 2021). User-centered interventions offer strategic opportunities to mitigate some of them is information onslaught in society. Adaptations to new platforms and emerging forms of misinformation such as videos and images complicate the showing of misinformation indicators and the provision of corrections. For older adults and adolescents, comprehensibility and the promotion of media literacy hinge on the user-centered balance of automation, human expertise, and feedback mechanisms, as well as other interventions designed to ease adaptiveness (Hartwig *et al.*, 2024).

Human-centered design, combined with the integration of AI technologies in educational fields, such as college music education in China, aims to enhance student experience optimization. This involves the challenge of balancing technological rationality with the humanistic dimension of teaching. Other considerable challenges are the need for intuitive user interfaces, aligning curricula to collaborative teaching, ethical AI deployment, and student engagement (Qian, 2023). In translational research, human-centered design facilitates stakeholder engagement, research design, and team management; however, such approaches still need to pioneer solutions to institutional resistance and tensions prior to fully realizing the benefits (Norman *et al.*, 2021)

Human-Centric Cyber security

Human-centered cybersecurity turns the focus away from territoriality and underscores the importance of the individual. It takes the human rights perspective that networks are part of the infrastructure of rights and needs access to information and free thought. It calls for the nets to be secured. And, monitoring should be done at the global level (Deibert, 2018). This model conceptualizes the integration of human behavior and cognition paradigms within the scope of cybersecurity. Organizational approaches to human error within the systems should be figured out in order to design specific and effective organizational strategies to respond to the human factors that challenge the efficacy of cybersecurity (Hakimi *et al.*, 2024). It addresses the gaps that are beyond the technology through the recognition of the psychosocial factors at the interactions of the people and the systems of technology (Pollini *et al.*, 2021).

The value of human-initiated cyber security simply confirms the attempts to controlling the sheer volume of human-initiated errors that are part and parcel of any organizational cyber security risk (Nobles, 2018). It aims to build cyber security culture which is a product of the organizational belief system and the socio-structural framework of the institution in order to uplift resilience (Aksoy, 2024). Adaptive cyber security culture is critical in threat mitigation to ensure alignment in cyber security efforts from top management to employees (Triplett, 2022). Understanding human elements - such as stress and burnout - and security fatigue can help organizations counteract some vulnerabilities that cybercriminals tend to go for (Nobles, 2022). In this regard, implementing human-centric approaches is imperative to protect organizations from cyber threats that pose the unprecedented challenges (Hakimi *et al.*, 2024).

The lack of human involvement in addressing challenges, especially in cyber security, is due to the nature of the defenses that are built. The efforts of malicious actors focus on the human side of security where inconsistencies behavior and psychology can be used to bypass advanced technical defenses. To mitigate such cyber security threats human behavioral studies, especially from the fields of psychology and sociology, positioned in conjunction with computer science, pivot cyber security to less advanced promiscuous and risky approaches (Nobles & Mcandrew, 2023).

In the field of healthcare, the application of Human Factors Engineering (HFE) is the best example on the extent to which managing human involvement is necessary so as not to leave behind unusable products and risk situations. The lack of human factors focus in healthcare IT projects not only affects user satisfaction but can also transform patient safety in a negative way. Usability studies ought to be a part of the system development process so that technically sound systems are also user friendly and safe for patient interactions (Beuscart *et al*., 2007).

Integrating AI, into scholarly work is another case in point. Advancements in AI models like GPT-4 leads to overly optimistic expectations. While GPT-4 is capable of retrieving information quickly, in many cases, it lacks adequate understanding of information, has problems with accuracy, and produces irrelevant and wrong answers. Human researchers, on the other hand, are not only capable of providing answers to these problems but can also work to develop the required contextual understanding. This is a clear case of how there combining the automating and the human efforts can yield the most precise and dependable scholarly work (Mostafapour *et al*., 2024). Taking climate change adaptation as another example, the limited human abilities to thermoregulate and acclimatize suggests that the human adaptation to global warming is solely reliant on behavioral and technological changes (Hanna & Tait, 2015). These examples serve to highlight that the human factor is important in order to supplement technical interventions. The human factor is required to provide alignment on the technological, ethical, emotional, psychological, and practical dimensions of human interaction and decision-making. Human conduct constitutes both risks and protections in data privacy and security. As an example, users of wearable health monitoring devices like fitness trackers do not realize how sensitive data can be shared and perhaps misappropriated (Sivakumar *et al*., 2024). This type of unguarded access and sharing through devices can amplify data privacy risks, much like AI-driven data management systems which can manifest unmonitored bias and substantial data misuse risks (Ijaiya, 2024).

In addition, organizational and interpersonal relationships and behaviors related to the holding and governance of data can expand risks to data privacy. For example, insufficient legal protection or non-compliance with legally defensible data protection governance like the European Union's General Data Protection Regulation (GDPR) can cause the violation of individual's privacy rights (Gilbert & Gilbert, 2024). People's ignorance of privacy controls and consent tools can be a key driver in the imposition of ungoverned and unmonitored circulation and commercialization of personal data (Shafik, 2024).

Conversely, organizational human behavior may also act as a positive influence concerning data privacy. Strengthening data protection frameworks, such as adopting privacy-preserving AI technologies, PII data protection, and individual privacy preservation, can improve data protection measures (Ijaiya, 2024). In a like manner, the enactment of comprehensive privacy regulations and governance frameworks also safeguards the alignment of data management practices with ethics and protection (Cha & Yeh, 2018; L. Huang, 2023; L. Huang, 2023). Being protectively proactive can entail positive legal regulations and the comprehensive privacy governance frameworks empowering data controllers to put in place better data protection measures. Encouraging data subjects through risk mitigation and increased protection as a result of informed consent through transparent collection and usage policies in addition to consent provision and consent withdrawal mechanisms, safely empower data subjects (Shafik, 2024).

Adaptive Awareness Approaches

The reason Adaptive Awareness in Cybersecurity Training is important is because it helps implement customized training programs in accordance with the goals and needs of every user or user group in an organization. Since users have varying skill levels and learning approaches gaps from end-users to users with advanced Cybersecurity skills, customized training serves individual participants, but understanding these gaps also builds an organization's training programs in their entirety. Furthermore, programs that build in flexible design features can modify training materials in accordance with the user's skills and track their progress and results, which can enrich the user's experience significantly (Hatzivasilis *et al*., 2020). Adaptive Awareness in Cybersecurity Training can also be realized through design elements that include systems of feedback, interactivity, and controlled tasks in which adaptive models of content would be based on user output. Then the learning approach, based on these systems of interactivity, can keep the user from disengaging due to repetition (He & Zhang, 2019). The Integrated Cybersecurity Awareness Training (iCAT), model is an example of a training frame that uses these instructional design approaches to enhance user participation through gamification. Users can focus on their tasks more and apply concepts of Cybersecurity more efficiently with this model, which is centered around modern instructional design concepts in training as given in (Table-1) (Taherdoost, 2024).

Adaptive training frameworks can gain an experiential learning enhancement through the incorporation of game-based and scenario-based approaches that imitate real-world cyber threats. This strategy improves the theoretical understanding of the concepts while helping the learners resolve real cyber incidents (He *et al.*, 2019; Nagarajan *et al.*, 2012). The development of adaptive awareness in cyber training as a resilient strategy integrates individualized cyber training approaches the flexibility of content in cyber training that is dynamically changing and the development of active participation in a training approach through personalization and interactivity in content presentation. This ensures that the cyber workforce is responsive in the changing landscape of cyber threats (Hatzivasilis *et al.*, 2020). Principles of gamification, use of simulations and providing real-time feedback has acknowledged potential in improving the human side of cyber security. The use these techniques improves interactivity and active participation of learners which in turn enhances the understanding and application of cyber security frameworks (He *et al.*, 2019).

Gamification in Cybersecurity

Gamification incorporates elements of game design in non-game settings, such as training in cybersecurity, to increase motivation and improve learning goals. Studies show that incorporating game elements such as storytelling, leaderboards, and interactive scenarios can increase non-IT people's interest and learning in cybersecurity (Gwenhure & Sapty Rahayu, 2024). In addition, Cyber-Hero, a gamified framework for high school students, illustrates how learning can be transformed into a series of interactive narratives, and gamification will also improve young people's cybersecurity skills, as mentioned in (Figure-1) (Qusa & Tarazi, 2021).

Gamification also helps to address the problem of knowledge stagnation in cybersecurity.

With thoughtful design, gamified models can effectively and enjoyably increase user cybersecurity awareness and knowledge for people of all ages (Fatokun *et al.*, 2024).

Simulations

Simulations create immersive spaces in which users can enact responses to cyber threats. Hands-on training helps to develop practical skills and muscle memory for recognizing threats, navigating potential breaches of security, and applying relevant countermeasures. Although the specific use of simulations in training for cybersecurity was not mentioned in the materials I retrieved, the overall educational value of simulation environments coincides with the principles discussed in adaptive and gamified educational technologies (Pollini *et al.*, 2021).

Immediate responses during the interaction with users in cyber security training programs are essential in reinforcing the positive behavior and correcting errors in real-time. Such immediate responses enhance the adjustment of training focus to suit the user's needs as well as the retention of information. For instance, the iCAT, model adopts real-time training adjustment with progress monitoring systems (Taherdoost, 2024).

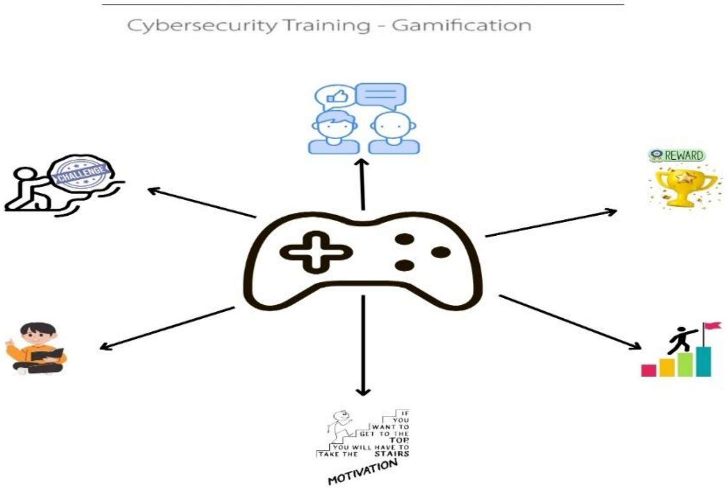
Cybersecurity Training - Gamification
CHALLENGE
REWARD
IF YOU WANT TO GET TO THE TOP YOU WILL HAVE TO TAKE THE STAIRS
MOTIVATION

Figure 4.1. Cybersecurity Training- Gamification

Evidence Supporting Adaptive Awareness Programs

The iCAT, model is an excellent embodiment of combining gamification with flexible adaptive learning. Engagement and knowledge retention improvements are significant indicators in determining the model's success in meeting the challenges of Cybersecurity training (Taherdoost, 2024). Studies targeting gamification in educational environments, particularly the adaptive features of gamification, state that it noticeably drives motivation and engagement. This can encourage the development of practical cyber security applications by automated adaptive systems that respond to the level of user engagement, thus, enabling personalization of the learning journey (Zourmpakis *et al.*, 2023). The above methodologies promote cyber security with the human factor in focus. By bridging the human behavior gap with cyber security practices, these frameworks strengthen the defenses of cyber systems that are under threat, making it particularly relevant in today's landscape of cyber security (Pollini *et al.*, 2021; Triplett, 2022).

Table 6.1: Comparison of Adaptive Awareness Training Models

Feature	CATRAM	iCAT	Reference
Training Customization	Groups content for organizational teams	Uses knowledge graphs and gamification	Sabillon *et al.*, 2019; Taherdoost, 2024
Engagement Method	Tailored content for specific goals	Serious games and real-time feedback	Sabillon *et al.*, 2019; Taherdoost, 2024
Focus	Organizational-level awareness	Individual engagement and knowledge retention	Sabillon *et al.*, 2019; Taherdoost, 2024
Interactivity	Moderate, team-based	High, with gamified and scenario-based tasks	Taherdoost, 2024

Behavioral Approaches to Data Privacy

Behavioral approaches are highly influential within the domain of data privacy. They define the individuals' and the organizations' perception of the behavioral privacy approaches and the management of behaviors. Within the domain of privacy practices in online social networks, the actions of individuals within the social network are influenced by the network. When considering how different sources of influence operate within the networks, the roles of official organizations and peers have been the focus of attention. In terms of the privacy behaviors of individuals, the findings indicated that the perceived privacy influence social behavioral privacy practices. More individuals show what is called perceived behavioral control, and are more influenced by peers. Moreover, individuals that are likely to adopt privacy practices are more likely to encourage other members to adopt privacy protective practices as well, mentioned in (Table-2) (Mendel & Toch, 2017).

Conversational AI, Systems have behavioral approaches and their influence is evident in the practices around the privacy of these systems. Privacy biases and other heuristics influence users to make privacy decisions that have a tendency to cause frustration or regret, even when control is exercised over the data. The integration of conversational privacy and issues of privacy debiasing frameworks within the privacy practices offers a way of behavioral modification. Such practices allow rational decision making and facilitate the sending of data deletion requests as determined by users (Leschanowsky *et al.*, 2023). Rational privacy decision making is encouraged, but most users' perceptions of privacy are still not modifiable. Furthermore, privacy regulations, and the communication strategies designed around them, shape how individuals perceive and trust the handling of their personal data. One study noted that privacy policies describe and communicate unethical data practices and that the policies' language could be enough to shift a user's perception to the point of "consent" (or lack thereof). These findings emphasize the need to communicate in a more responsible and transparent manner (Pollach, 2005).

On another note, the PP Checker system is an example of a more systematic approach to evaluating the trustworthiness of privacy policies, in this case, of popular applications. It describes how most applications contain problematic policy documents. Such frameworks are essential in encouraging the privacy practices of organizations to be more self-regulatory. (Yu *et al.*, 2021).

Research demonstrates that behavioral approaches impact data privacy practices through the adoption of privacy behaviors, the articulation of user practices, and the transparency and accountability of communication frameworks (Leschanowsky *et al.*, 2023; Mendel & Toch, 2017; Pollach, 2005; Yu *et al.*, 2021).

Psychological nudges, incentives, and interventions are crucial in affecting individuals' behavior concerning the human factors that slip through in every cybersecurity incident. A psychological nudge refers to an unobtrusive intervention that guides individuals to a specific behavior while still maintaining their freedom to choose. In the context of cybersecurity, nudges could be designed to promote heightened awareness of the dangers associated non-compliance and best practices. For example, presenting security measures using the 'loss' frame could spur individuals, under the 'loss aversion' principle, to embrace more security (Hakimi *et al.*, 2024).

Incentives promote behavior through the provision of anticipated rewards. In cybersecurity, some organizational behavior frameworks provide incentives for employees to practice and defend the organizational perimeter. Rewards for reporting suspicious activities and maintaining good security practices could serve to mitigate security fatigue to a great extent (Fatokun *et al.*, 2019). Including educational programs and awareness initiatives seeks to foster a culture of security mindfulness and consciousness within the organization. These initiatives can consider socially and psychologically driven characteristics such as age, gender, and educational attainment to be more effective. Tailored training increases self-efficacy-the belief of an individual in their competence to carry out given cybersecurity tasks-which is critical in promoting positive security behavior (Borgert *et al.*, 2024).

Due to the perception of the human factor as the weakest link in cybersecurity, interventions should primarily improve psychological literacy to predict and alleviate human error in cybersecurity. By coupling human elements and technological tools, organizations can engineer more comprehensive and robust cyber security systems (Nobles & Mcandrew, 2023). To establish a culture of privacy for the long haul, organizations must develop and implement fully integrated systems that include ongoing training and the promotion of general organizational cybersecurity awareness. The design of user interfaces that reduce complexity and encourage right user actions can help reduce the friction that leads to human error. Actively promoting engagement with organizational cybersecurity policies and frameworks entails ongoing training that includes recent threat analyses, which can help cultivate privacy-positive attitudes. Equally, the integration of privacy as a strong organizational culture element through leadership and incentives systems further embeds these as the norm in day-to-day functionality (Oladipo *et al.*, 2024).

Table 7.1: Behavioral Approaches to Data Privacy

Behavioral Approach	Impact on Data Privacy	Example/Application	Reference
Social Influence	Peers and organizations shape privacy behaviors	Social networks encourage privacy practices	Mendel & Toch, 2017
Psychological Nudges	Guides users to secure behaviors without restricting choice	Loss-framed messages for security adoption	Hakimi *et al.*, 2024
Incentives	Rewards promote secure practices	Reporting suspicious activities	Fatokun *et al.*, 2019
Privacy Policy Communication	**Transparent policies enhance trust and consent**	**PPChecker evaluates policy trustworthiness**	**Pollach, 2005; Yu *et al.*, 2021**

Integration of Awareness and Behavioral Strategies

Incorporating adaptive awareness as well as training and behavioral approaches to human-centric cybersecurity requires knowledge of human factors and training models. This intersection requires understanding human behavior, the mind, and the relevant technologies. From the human-centric perspectives of security fatigue and the shortage of psychology-oriented cybersecurity professionals, the need for understanding human behavior in cybersecurity is critical (Hakimi *et al.*, 2024). Models such as the Cybersecurity Awareness training Model (CATRAM) and iCAT, are examples of structured approaches to improving awareness at the organizational level. For example, CATRAM groups training content for different organizational teams, tailoring the content to specific goals. On the other hand, iCAT increases training engagement and knowledge retention with knowledge graphs, serious games, and gamification (Sabillon *et al.*, 2019; Taherdoost, 2024).

Holistic integration requires a human factors (HF) framework that integrates personal, organizational, and technological elements. Such a framework helps assess organizational maturity with respect to cyber threat exposure and encourages non-technical measures, particularly user awareness, to bolster a cyber threat resilience culture (Pollini *et al.*, 2021). Organizations encounter some integration challenges such as alignment of the culture of cybersecurity with the behavior patterns of the individuals within the organization; conflicting, interwoven cybersecurity rules; and the counterbalancing view of the 'weak link'

(Triplett, 2022). This underscores the importance of complementing human integration with the various technological approaches and counterbalancing the human factors of education and awareness and communication on the integration issues. The integration of adaptive awareness and behavior patterns, as described in the approaches to cybersecurity, consists of the use of predictive analytics to create adaptive cybersecurity techniques at the individualized level, the use of behavioral user data to construct adaptive cybersecurity mechanisms, and fostering a climate of perpetual learning and change (Addae *et al.*, 2019).

Future Directions

Adaptive awareness training can leverage AI, and personalization to improve learning efficiency and provide customized training. AI, technology makes it possible to develop adaptive learning systems that assess training loses and gain and customize training to fit learner profiles (Aggarwal *et al.*, 2023; Mahmoud & Sørensen, 2024). AI, personalization makes it possible for educational systems to adapt content and delivery in real time to make learning more efficient. AI, personalization makes learning more engaging and instructional time more efficient by using predictive algorithms that assess learner performance data and assess instructional feedback and learning activity suggestions that close learning gaps (Akavova *et al.*, 2023). Learning analytics powered by AI, can provide personalized feedback and assessments in real-time, further refining the learning experience and improving educational outcomes. These systems can provide personalized formative assessments that sufficiently meet the evaluative criteria and assess learner knowledge and skills (Vashishth *et al*., 2024).

AI, extends into personalized learning via intelligent tutoring systems and predictive analytics. The goal of these systems is to provide inclusive and effective educational engagements, addressing socio-emotional and cognitive development in a more human-centered framework ("Beyond Algorithms: Humanizing Artificial Intelligence for Personalized and Adaptive Learning," 2024). The use of AI, in educational training does bring some challenges. The ethical challenges of privacy and possible bias in algorithms can threaten responsible use of these technologies. In addition, to successful adoption of these technologies, ongoing training of staff is crucial to ensure that educators possess AI, tools to optimize educational outcomes while preserving human touch elements of empathy and situational awareness (Jane *et al*., 2024; Xiao *et al*., 2025).

The potential of AI, and personalization in adaptive awareness training is enormous in terms of improving learning outcomes, increasing engagement, and providing education in a scalable manner. With AI's, challenges and ethical issues sufficiently addressed in the use technology, there is potential to significantly change training delivery in education as given in (Figure-2) (Aggarwal, 2023). In human-centric cybersecurity, the tailoring of protective measures to the nuances of human behavior, as well as the range of potential cyber risks, necessitates the adoption of continuous monitoring systems, as well as the use of adaptive learning methodologies. Such systems support the evolving nature of cyber defense technologies by providing real-time responses to adaptive cyber threats. Continuous monitoring systems in human-centric cybersecurity consist of real-time tracking of user cyber behaviors and predictive technologies in order to identify and deter threats. The most substantial value of continuous monitoring systems lies in the active elimination of threats. Human-centric continuous monitoring systems are based on user-initiated cyber behavior patterns, and learning systems predict a range of user behaviors by learning via automated systems (Shelke & Hamalainen, 2024).

In contrast, Adaptive Learning employs machine learning and AI, to revise security measures in real-time and respond to newly recognized patterns of behavior and new data. Self-learning Cybersecurity systems evaluate responses to prior incidents and fine-tune responses to threats in the future. These systems focus on the complex behavioral patterns of users and contextualize the patterns for more accurate threat detection and minimal false alarms. (Meng, 2024; Vemuri *et al*., 2024). Being capable of evaluating human actions in a nuanced manner, especially in ambiguous digital spaces, is a crucial feature of Adaptive Learning. Since human blunders are a leading cause of security breaches, adaptive learning systems predicting and preempting security flaws are of high potential. Predictively, these systems learn adaptive 'normal' user behaviors and identify abnormal patterns, (Hakimi *et al*., 2024). Adaptive Cybersecurity systems, have developed 'Active' Threat strategies; continuously monitoring and learning in real-time from the environment to detect evolving threats and dynamically shifting counter measures for robust protection from a wide range of known and unknown cyber threats, effectively learning and adapting to the complex and evolving threat (Babu and Simon P, 2023).

Incorporating ongoing surveillance coupled with adaptive learning capabilities encourages a shift from reactive to proactive engagement with the cybersecurity elements. Organizations gain the ability to detect and mitigate threats in real time and then predict future attacks and modify approaches to avert potential breaches (Thawait, 2024). The global policy implications that will shape future behavioral approaches to data privacy in cross-border contexts will likely stem from new regulatory frameworks, rapid advances in technology, and geopolitical issues. The global data privacy policies, such as the European Union (EU) General Data Protection Regulation (GDPR) and regional frameworks like the California Consumer Privacy Act (CCPA), are critical in shaping modern data protection policies within the borders of the EU and the US. These policies reflect the relationship between technological advancements and the protection of privacy at the individual level (Ehimuan *et al*., 2024).

The rapid innovation of technologies such as AI, and big data analytics impacts the privacy of data in new and un-chartered ways. AI, technologies can be used to strengthen protection measures of data through privacy-preserving machine learning, but they also facilitate new forms of data protection abuses, such as algorithmically biased decisions and biased data (Ijaiya, 2024). AI, also raises the stakes in privacy protection due to the absence of ethical, transparent, and accountable frameworks (governance) to handle the potential adverse impacts (Lami *et al*., 2024).

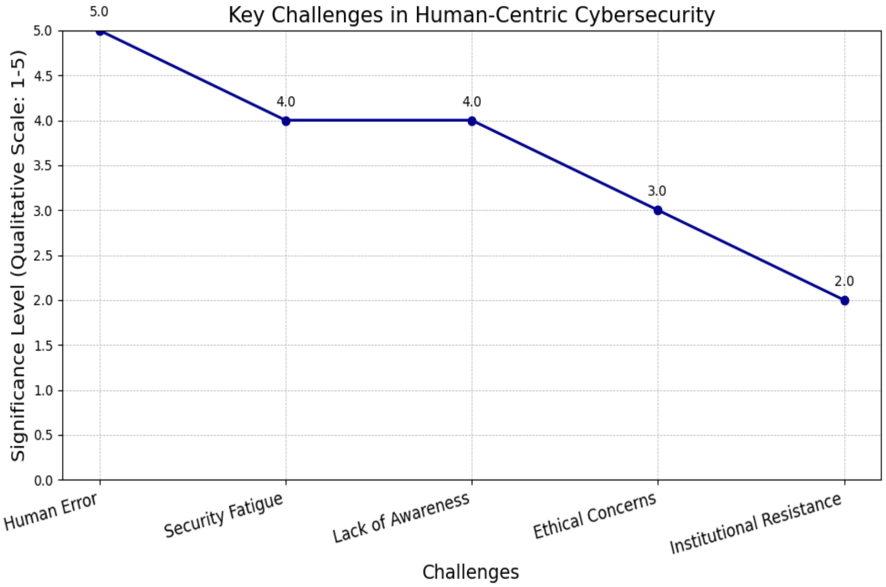

Figure 9.1 Key Challenges in Human-Centric Cybersecurity

The introduction of diverse national regulations Geo-political factors of diverse national regulations on data related to privacy pose considerable geopolitical challenges to data privacy regulation. China exemplifies a national jurisdiction with comprehensive geo-political challenges to privacy regulation. Its western counterparts unwilling to align on unified rules of data regulation. The mismatched data governance frameworks of the West with China will impact international data governance, international data privacy governance, and international relations (Zhang, 2024). International enforcement and data protection frameworks will incorporate cross-border data compliance to create an inclusive global regulation on cross-border data flow. There is a need to ensure compliance to defend citizen's rights, automated compliance monitoring, and enforcement around regulations (Ochigbo *et al*., 2024). The advancement of digital technologies boosts global conversations around privacy and the legislation needed to regulate privacy. This escalation calls for policies that enhance the frameworks of legal regulation towards improving user access, accountability, and broad adaptability of the regulation (Ehimuan *et al*., 2024; Reis *et al*., 2024).

Conclusion

Human-centric cybersecurity represents a transformative shift from technology-focused defense to an inclusive model where human behavior, cognition, and ethics are equally prioritized. This study demonstrates that integrating adaptive awareness programs and behavioral frameworks fosters proactive cybersecurity cultures, enhances data protection, and mitigates human-induced vulnerabilities. Gamified and adaptive learning models empower users with dynamic, engaging, and personalized cybersecurity education, while behavioral approaches leverage psychological and social insights to promote responsible data practices. As AI and machine learning evolve, continuous monitoring and adaptive systems can anticipate and counter emerging threats in real time. However, technological progress must align with ethical governance, privacy protection, and cross-border data compliance. Ultimately, cybersecurity resilience in the digital era depends on the synergy between human adaptability, awareness, and technological innovation—creating a secure, transparent, and human-centered digital environment.

REFERENCES

Addae, J. H., Towey, D., Sun, X., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, *29*(3), 701–750. https://doi.org/10.1007/s11257-019-09236-5.

Aggarwal, D. (2023). Exploring the Scope of Artificial Intelligence (AI) for Lifelong Education through Personalised &amp; Adaptive Learning. *Journal of Artificial Intelligence, Machine Learning and Neural Network*, *41*, 21–26. https://doi.org/10.55529/jaimlnn.41.21.26.

Aggarwal, D., Sharma, D., & Saxena, A. B. (2023). Adoption of Artificial Intelligence (AI) For Development of Smart Education as the Future of a Sustainable Education System. *Journal of Artificial Intelligence, Machine Learning and Neural Network*, 36, 23–28. https://doi.org/10.55529/jaimlnn.36.23.28.

Akavova, A., Lorsanova, Z., & Temirkhanova, Z. (2023). Adaptive learning and artificial intelligence in the educational space. *E3S Web of Conferences*, *451*, 06011. https://doi.org/10.1051/e3sconf/202345106011.

Aksoy, C. (2024). BUILDING A CYBER SECURITY CULTURE FOR RESILIENT ORGANIZATIONS AGAINST CYBER ATTACKS. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96–110. https://doi.org/10.33416/baybem.1374001.

Babu, C. V. S., & Simon P, A. (2023). *Adaptive AI for Dynamic Cybersecurity Systems* (pp. 52–72). Igi Global. https://doi.org/10.4018/979-8-3693-0230-9.ch003.

Beuscart, R., Pelayo, S., Elkin, P., & Beuscart-Zéphir, M.-C. (2007). The Human Factors Engineering Approach to Biomedical Informatics Projects: State of the Art, Results, Benefits and Challenges. *Yearbook of Medical Informatics*, *16*(01), 109–127. https://doi.org/10.1055/s-0038-1638535.

Beyond Algorithms: Humanizing Artificial Intelligence for Personalized and Adaptive Learning. (2024). *International Journal of Innovative Research in Engineering and Management*, *11*(5), 40–47. https://doi.org/10.55524/ijirem.2024.11.5.6.

Borgert, N., Elson, M., Sasse, M. A., Jansen, L., Friedauer, J., & Böse, I. (2024). *Self-Efficacy and Security Behavior: Results from a Systematic Review of Research Methods*. *5*, 1–32. https://doi.org/10.1145/3613904.3642432.

Cha, S.-C., & Yeh, K.-H. (2018). A Data-Driven Security Risk Assessment Scheme for Personal Data Protection. *IEEE Access*, *6*, 50510–50517. https://doi.org/10.1109/access.2018.2868726.

Deibert, R. J. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics &amp; International Affairs*, *32*(4), 411–424. https://doi.org/10.1017/s0892679418000618.

Ehimuan, B., Reis, O., Ob, O., Oguejiofor, B., & Akagha, O. (2024). Global data privacy laws: A critical review of technology's impact on user rights. *World Journal of Advanced Research and Reviews*, *21*(2), 1058–1070. https://doi.org/10.30574/wjarr.2024.21.2.0369.

Fatokun, F. B., Norman, A., Hamid, S., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098.

Fatokun, F., Fatokun, J., Awang, Z., Norman, A., & Hamid, S. (2024). Cybersecurity Knowledge Deterioration and the role of Gamification Intervention. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *43*(1), 66–94. https://doi.org/10.37934/araset.43.1.6694.

Flood, M., De Brún, A., Mellon, L., Ennis, M., Boland, F., Morgan, S., Clarke, C., Carroll, P., Holton, A., Sweeney, F. F., Moriarty, F., Hanratty, M., Mohamed, S., & Ludlow, A. (2021). Research methods from human-centered design: Potential applications in pharmacy and health services research. *Research in Social and Administrative Pharmacy*, *17*(12), 2036–2043. https://doi.org/10.1016/j.sapharm.2021.06.015.

Gilbert, C., & Gilbert, M. A. (2024). The Convergence of Artificial Intelligence and Privacy: Navigating Innovation with Ethical Considerations. *International Journal of Scientific Research and Modern Technology (IJSRMT)*, *3*(9), 9–17. https://doi.org/10.38124/ijsrmt.v3i9.45.

Gwenhure, A. K., & Sapty Rahayu, F. (2024). Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review. *International Journal of Serious Games*, *11*(1), 83–99. https://doi.org/10.17083/ijsg.v11i1.719.

Hakimi, M., Quchi, M., & Fazil, A. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, *3*(01), 20–33. https://doi.org/10.58471/esaprom.v3i01.3832.

Hanna, E. G., & Tait, P. W. (2015). Limitations to Thermoregulation and Acclimatization Challenge Human Adaptation to Global Warming. *International Journal of Environmental Research and Public Health*, *12*(7), 8034–8074. https://doi.org/10.3390/ijerph120708034.

Hartwig, K., Reuter, C., & Doell, F. (2024). The Landscape of User-centered Misinformation Interventions - A Systematic Literature Review. *ACM Computing Surveys*, *56*(11), 1–36. https://doi.org/10.1145/3674724.

Hatzivasilis, G., Frati, F., Koshutanski, H., Goeke, L., Spanoudakis, G., Oikonomou, F., Leftheriotis, G., Hildebrandt, T., Tsakirakis, G., Smyrlis, M., & Ioannidis, S. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702.

He, W., & Zhang, Z. (Justin). (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, *29*(4), 249–257. https://doi.org/10.1080/10919392.2019.1611528.

He, W., Xu, L., Li, L., Ash, I., Tian, X., Yuan, X., & Anwar, M. (2019). Improving employees' intellectual capacity for cybersecurity through evidence-based malware training. *Journal of Intellectual Capital*, *21*(2), 203–213. https://doi.org/10.1108/jic-05-2019-0112.

Huang, C., De Albuquerque, V. H. C., Chen, S., Zhou, W., Zhang, Y., & Rodrigues, J. J. P. C. (2022). A Robust Approach for Privacy Data Protection: IoT Security Assurance Using Generative Adversarial Imitation Learning. *IEEE Internet of Things Journal*, *9*(18), 17089–17097. https://doi.org/10.1109/jiot.2021.3128531.

Huang, L. (2023). Ethics of Artificial Intelligence in Education: Student Privacy and Data Protection. *Science Insights Education Frontiers*, *16*(2), 2577–2587. https://doi.org/10.15354/sief.23.re202.

Ijaiya, H. (2024). Harnessing AI for data privacy: Examining risks, opportunities and strategic future directions. *International Journal of Science and Research Archive*, *13*(2), 2878–2892. https://doi.org/10.30574/ijsra.2024.13.2.2510.

Jane, O. C., Ezeonwumelu, C. G., Barah, C. I., & Jovita, U. N. (2024). Personalized Language Education in the Age of AI: Opportunities and Challenges. *NEWPORT INTERNATIONAL JOURNAL OF RESEARCH IN EDUCATION*, *4*(1), 39–44. https://doi.org/10.59298/nijre/2024/41139448.

Lami, B., Rajamanickam, R., Mohd Hussein, S., & Emmanuel, G. K. (2024). The role of artificial intelligence (AI) in shaping data privacy. *International Journal of Law and Management*. https://doi.org/10.1108/ijlma-07-2024-0242.

Leschanowsky, A., Popp, B., & Peters, N. (2023). *Privacy Strategies for Conversational AI and their Influence on Users' Perceptions and Decision-Making*. *23*, 296–311. https://doi.org/10.1145/3617072.3617106.

Mahmoud, C. F., & Sørensen, J. T. (2024). Artificial Intelligence in Personalized Learning with a Focus on Current Developments and Future Prospects. *Research and Advances in Education*, 3(8), 25–31. https://doi.org/10.56397/rae.2024.08.04.

Mendel, T., & Toch, E. (2017). *Susceptibility to Social Influence of Privacy Behaviors*. 581–593. https://doi.org/10.1145/2998181.2998323.

Meng, X. (2024). Advanced AI and ML techniques in cybersecurity: Supervised and unsupervised learning, reinforcement learning, and neural networks in threat detection and response. *Applied and Computational Engineering*, *82*(1), 24–28. https://doi.org/10.54254/2755-2721/82/2024glg0054.

Mostafapour, M., Fortier, J. H., Pacheco, K., Murray, H., & Garber, G. (2024). Evaluating Literature Reviews Conducted by Humans Versus ChatGPT: Comparative Study. *JMIR AI*, *3*, e56537. https://doi.org/10.2196/56537.

Nagarajan, A., Sood, A., Allbeck, J. M., & Janssen, T. L. (2012, May 1). *Exploring game design for cybersecurity training*. https://doi.org/10.1109/cyber.2012.6392562.

Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA – Journal of Business and Public Administration*, 9(3), 71–88. https://doi.org/10.2478/hjbpa-2018-0024.

Nobles, C. (2022). Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *HOLISTICA – Journal of Business and Public Administration*, *13*(1), 49–72. https://doi.org/10.2478/hjbpa-2022-0003.

Nobles, C., & Mcandrew, I. (2023). The Intersectionality of Offensive Cybersecurity and Human Factors: A Position Paper. *Scientific Bulletin*, *28*(2), 215–233. https://doi.org/10.2478/bsaft-2023-0022.

Norman, M. K., Reis, S. E., Hamm, M. E., Hierholzer, W., Schenker, Y., Rubio, D. M., & Mayowski, C. A. (2021). Assessing the application of human-centered design to translational research. *Journal of Clinical and Translational Science*, *5*(1). https://doi.org/10.1017/cts.2021.794.

Ochigbo, A., Labake, T., Layode, O., & Tuboalabo, A. (2024). Regulatory compliance in the age of data privacy: A comparative study of the Nigerian and U.S. legal landscapes. *International Journal of Applied Research in Social Sciences*, 6(7), 1355–1370. https://doi.org/10.51594/ijarss.v6i7.1297.

Oladipo, J., Nwankwo, E., Elufioye, O., Falaiye, T., & Okoye, C. (2024). Human factors in cybersecurity: Navigating the fintech landscape. *International Journal of Science and Research Archive*, *11*(1), 1959–1967. https://doi.org/10.30574/ijsra.2024.11.1.0258.

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics*, *62*(3). https://doi.org/10.1007/s10551-005-7898-3.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work (Online)*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y.

Qian, C. (2023). Research on Human-centered Design in College Music Education to Improve Student Experience of Artificial Intelligence-based Information Systems. *Journal of Information Systems Engineering and Management*, *8*(3), 23761. https://doi.org/10.55267/iadt.07.13854.

Qusa, H., & Tarazi, J. (2021). *Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students*. *1*, 0677–0682. https://doi.org/10.1109/ccwc51732.2021.9375847.

Raja, V. (2024). Exploring Challenges and Solutions in Cloud Computing: A Review of Data Security and Privacy Concerns. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, 4(1), 121–144. https://doi.org/10.60087/jaigs.v4i1.86.

Reis, O., Ehimuan, B., Anyanwu, A., Abrahams, T., Olorunsogo, T., & Eneh, N. (2024). PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, *6*(1), 73–88. https://doi.org/10.51594/ijarss.v6i1.733.

Sabillon, R., Serra-Ruiz, J., Cavaller, V., & M, J. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program. *Journal of Cases on Information Technology*, *21*(3), 26–39. https://doi.org/10.4018/jcit.2019070102.

Shafik, W. (2024). *Data Privacy and Security Safeguarding Customer Information in ChatGPT Systems* (pp. 52–86). Igi Global. https://doi.org/10.4018/979-8-3693-1239-1.ch003.

Shelke, P., & Hamalainen, T. (2024). Analysing Multidimensional Strategies for Cyber Threat Detection in Security Monitoring. *European Conference on Cyber Warfare and Security*, *23*(1), 780–787. https://doi.org/10.34190/eccws.23.1.2123.

Sivakumar, C. L. V., Mone, V., & Abdumukhtor, R. (2024). Addressing privacy concerns with wearable health monitoring technology. *WIREs Data Mining and Knowledge Discovery*, *14*(3). https://doi.org/10.1002/widm.1535.

Taherdoost, H. (2024). Towards an Innovative Model for Cybersecurity Awareness Training. *Information*, *15*(9), 512. https://doi.org/10.3390/info15090512.

Thawait, N. (2024). Machine Learning in Cybersecurity : Applications, Challenges and Future Directions. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *10*(3), 16–27. https://doi.org/10.32628/cseit24102125.

Triplett, W. J. (2022). Addressing Human Factors in Cybersecurity Leadership. *Journal of Cybersecurity and Privacy*, *2*(3), 573–586. https://doi.org/10.3390/jcp2030029.

Vashishth, T. K., Sharma, V., Chaudhary, S., Sharma, K. K., Panwar, R., & Kumar, B. (2024). *AI-Driven Learning Analytics for Personalized Feedback and Assessment in Higher Education* (pp. 206–230). Igi Global. https://doi.org/10.4018/979-8-3693-0639-0.ch009.

Vemuri, N., Thaneeru, N., & Tatikonda, V. (2024). Adaptive generative AI for dynamic cybersecurity threat detection in enterprises. *International Journal of Science and Research Archive*, *11*(1), 2259–2265. https://doi.org/10.30574/ijsra.2024.11.1.0313.

Winkler, T., & Rinner, B. (2014). Security and Privacy Protection in Visual Sensor Networks. *ACM Computing Surveys*, *47*(1), 1–42. https://doi.org/10.1145/2545883.

Xiao, N., Cai, Z., Yuan, C., Pei, Y., & Bu, Y. (2025). Transforming Education with Artificial Intelligence: A Comprehensive Review of Applications, Challenges, and Future Directions. *International Theory and Practice in Humanities and Social Sciences*, *2*(1), 337–356. https://doi.org/10.70693/itphss.v2i1.211.

Yu, L., Chang, H., Zhang, T., Chen, J., Leung, H. K. N., Luo, X., & Zhou, H. (2021). PPChecker: Towards Accessing the Trustworthiness of Android Apps' Privacy Policies. *IEEE Transactions on Software Engineering*, *47*(2), 221–242. https://doi.org/10.1109/tse.2018.2886875.

Zangana, H. M., Omar, M., & Al-Karaki, J. N. (2025). *Data Privacy and Security Standards in AI-Powered Scientific Research* (pp. 1–42). Igi Global. https://doi.org/10.4018/979-8-3373-4252-8.ch001.

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*(1). https://doi.org/10.1007/s44216-024-00028-2.

Zourmpakis, A.-I., Papadakis, S., & Kalogiannakis, M. (2023). Adaptive Gamification in Science Education: An Analysis of the Impact of Implementation and Adapted Game Elements on Students' Motivation. *Computers*, *12*(7), 143. https://doi.org/10.3390/computers12070143.