Human-Centric Cybersecurity in Healthcare: Bridging the Gap Between Awareness and Action

ENIOLA AKINOLA ODEDINA[1], ADETAYO ABRAHAM-ADEYEMO[2]
[1]*Researcher, Covenant University, Human-Centric Cybersecurity, Artificial Intelligence, Security Risk Management and Compliance, Nigeria.*
[2]*Psychologist, Birbeck College, University of London.*

Abstract- The healthcare industry now recognizes cybersecurity as an issue which extends beyond technological defenses because it combines social and technical dimensions. The deployment of advanced security measures within hospitals fails to eliminate human mistake as a fundamental risk factor in high-risk medical environments. Scientists examine three domains of factors that influence healthcare staff performance in secure practices. The research implements Protection Motivation Theory and Theory of Planned Behavior to assess cognitive obstacles such as risk evaluation together with environmental challenges from inadequate UX design and time stress and cultural mismatches. Empirical studies show that researchers have identified a need for better assessment methods of long-term behavior change while developing interventions tailored to healthcare workflows. The proposed intervention framework consists of four levels which include behavioral nudges, gamified training, user-centered design and organizational change strategies for developing a security-first culture. The method considers human needs to overcome gaps between patient understanding and daily practice while establishing lasting safe practices in medical facilities.

Indexed Terms- Cybersecurity awareness, healthcare security, human factors, behavior change, user-centered design, organizational culture, cognitive barriers, cybersecurity training, healthcare IT, secure usability.

I. INTRODUCTION

1.1 Overview of Human-Centric Cybersecurity in Healthcare

Human-centric cybersecurity represents the upcoming cyber security strategy model where individual users remain central to protection efforts instead of relying on system security systems alone. This approach demonstrates how users and their security tool usage interacts with their behaviors within systems that heavily depend on human error defenses. Professionals who use complex digital healthcare infrastructure must develop this approach under time-sensitive working conditions. Conventionally used security methods that focused on things like firewalls and encryption alone displayed limited understanding of how users interact with information systems (Grobler, Gaire, & Nepal, 2021). Strong systems become vulnerable to security breaches because employees make mistakes when they click phishing links and when they adjust access settings improperly.

Organizations shifted to human-centric security methods because cyber incidents caused by human mistakes keep increasing. Numerous scientific studies demonstrate that user actions lead to a majority of healthcare data breaches which exceed system-based failures. Security protocols now combine educational programs, user conduct observation methods along with system function evaluation processes (Tambe-Jagtap, 2023). They implement these measures to develop a security-oriented environment that transforms staff from system consumers to security protectors of important healthcare data. Companies now follow proactive risk reduction approaches that require equal knowledge of human behavior to maintain technical defenses.

Human-centered cybersecurity has become more critical as Healthcare 4.0 moves forward because of its emphasis on connected tech and artificial intelligence in healthcare. Healthcare providers together with patients who are also administrators require consistent secure interactions throughout their digital health use as it becomes a critical requirement. Through the human-centric model organizations focus on both personal security knowledge and the implementation of security design elements which promote safe operations by default (Kioskli et al., 2023). Healthcare systems becoming able to strike the right balance between innovation and resilience through integrating human factors within cybersecurity perspectives since security has evolved into a fundamental human challenge beyond technical remediation.

Figure 1. Principles of human-centric cybersecurity.

Source: Keepnet Labs. Human-Centric Cybersecurity: Building Stronger Defenses by Focusing on People. https://keepnetlabs.com/blog/human-centric-cybersecurity-prioritizing-people-in-cyber-defense

1.2 Importance of Bridging Awareness and Action

The security of healthcare data requires more than basic awareness since it does not lead to successful breach prevention or protection of sensitive information. The healthcare workforce demonstrates basic understanding of security principles though these concepts do not transform into steady safe practices. Medical research demonstrates that human errors involving malicious links and improper patient data management continue to frequently occur despite general healthcare personnel being made aware through promotional initiatives (Alhuwail et al., 2021). The gap in behavioral interventions requires training that educates healthcare staff while simultaneously developing secure behavioral patterns which they will sustain with consistency.

The phishing attack persistence remains active even though it has received significant recognition within the industry. The results of several healthcare organizations demonstrate that security training did not protect employees from simulated phishing attacks even though they underwent the training (Nifakos et al., 2021). Internal security threats stemming from either careless or malicious actions prove why organizations must build working environments where security measures become automatic. The implementation of psychological controls with immediate performance indicators together with simulated procedural scenarios helps healthcare staff transition theory into consistent action. Implementing a healthcare environment through which both cybersecurity understanding and correct implementation will reduce meaningful risks.

Figure 2. Cybersecurity strategies enhancing healthcare information systems.

Source: Stefanini. How Cybersecurity Improves Healthcare Information Systems. https://stefanini.com/en/insights/news/how-cybersecurity-improves-healthcare-information-system

1.3 Objectives and Scope of the Study

This research examines how human-centric cybersecurity methods integrate into healthcare facilities by addressing healthcare professionals' error-related issues and behavioral compliances. The main goal targets an evaluation of how understanding combined with system design decisions and behavioral programs affect medical facility cybersecurity resilience. The technological examination for this study focuses on healthcare digital systems that include electronic health records (EHRs), clinical decision support systems and communication platforms. The investigation explores three human elements that include user awareness methods along with descriptions of urgent decision-making and resistance towards social engineering attacks. Research explores three organizational aspects about policy enactment and training programs alongside healthcare readiness to implement security protocols.

The main research inquiries within this field ask how human factors lead to healthcare cybersecurity vulnerabilities and how human vulnerabilities affect cybersecurity. Does any existing intervention successfully move security-awareness into actual security behavior execution? Industrial organizations require strategies to merge automated security solutions with people-focused policies for developing robust cybersecurity awareness within their culture. The research questions guide both analytical and practical work of the study.

1.4 Significance of the Study

The increase of cyber threat targeting healthcare systems demands urgent research now especially during COVID-19 pandemic and its aftermath. Healthcare organizations urgently implemented digital tools for remote care administration which led to expanded cybersecurity weaknesses. Human error has become the main entrance point for cybercriminals because they effectively use these security gaps. This investigation uses human-centric methods to deliver essential information about improving both technology infrastructure and user conduct that strengthens overall cybersecurity protection for the digital healthcare environment.

II. LITERATURE REVIEW

2.1 Historical Development of Human-Centric Cybersecurity

The development of human-focused security strategies emerged because people became understood as fundamental components in cybersecurity vulnerabilities. The primary cybersecurity features until recently concentrated on technical security tools including firewalls and intrusion detection systems because they served to block unauthorized access and protect data from theft. Technical systems evolved to include advanced security features yet they demonstrated their vulnerability against human error which consists of poor password management and exposure to phishing attacks according to Gopireddy and Bodipudi (2022). The rise of security compromises motivated changes in cybersecurity approaches especially within healthcare which maintains vital patient information as its core priority.

The emergence of human-centric cybersecurity occurred during the early 2000s as experts recognized people as the main security vulnerability point. Deibert (2018) led multiple scholars who called for a fundamental change in cybersecurity frameworks which required behavior and decision-making elements from humans. The healthcare sector needed this fundamental change since pressure-stressed healthcare personnel often made security mistakes while working under time limits. Security strategy evolution required organizations to implement defense mechanisms beyond technology which involved human-centric approaches such as education initiatives and practical system designs to reduce errors made by staff.

The late 2010s through early 2020s brought human-centric cybersecurity as an essential strategic element for healthcare cybersecurity programs. The COVID-19 pandemic increased healthcare system exposures which led to faster digital tool adoption and compelled healthcare organizations to develop complete cybersecurity programs that accounted for user engagement (Tambe-Jagtap, 2023). Security experts focus on developing systems with human-friendly features that learn user conduct while offering preventative solutions to user mistakes to make cybersecurity work together between technology platforms and the people using them.

2.2 Theoretical Foundations and Behavioral Models

Several behavioral science and psychological theories provide explanations and methodologies to manipulate cybersecurity behavior regarding compliance and risk management frameworks. Protection Motivation

Theory (PMT) and the Theory of Planned Behavior (TPB) represent the two most influential models which apply to these scenarios. Protection Motivation Theory established by Rogers (1975) explains that people decide to protect themselves against threats through understanding their risk exposure combined with threat seriousness and their prevention capability. The theory explains that people will follow security policies better when they recognize critical threats to themselves while understanding safety methods such as strong passwords and secure logins truly protect against these threats (Khan et al., 2022).

According to the Theory of Planned Behavior (Ajzen, 1991) intended behaviors and attitudes and subjective norms as well as perceived behavioral control influence how people behave in cybersecurity situations. According to the Theory of Planned Behavior model, security protocol adoption intentions of individuals depend on their measure evaluations, social pressures and behavioral self-confidence (Kim, Yang, & Park, 2014). When applied to healthcare both theories demonstrate the need to establish settings in which people both understand security risks and obtain both capability and motivation to practice secure behavior.

The Behavioral Compliance Framework established by Onumo (2020) delivers a practical framework for cybersecurity governance because it joins psychological aspects to organizational practices. The comprehensive approach identifies that individual mental processes together with systemic elements influence human conduct so cybersecurity strategies need to combine psychological elements with organizational structures to achieve compliance goals and prevent risks. Once behavioral science enters cybersecurity training it will improve policy effectiveness and establish a complete compliance environment.

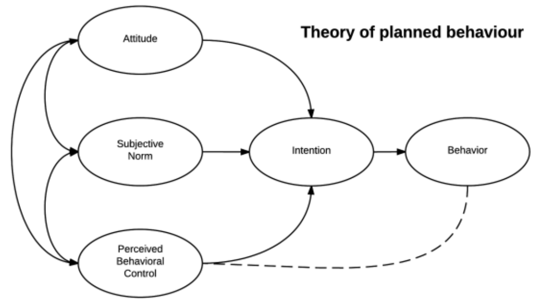

Figure 3. Theory of Planned Behavior model illustrating the relationships among attitude, subjective norms, perceived behavioral control, intention, and behavior.

Source: Wikipedia contributors. Theory of planned behavior. Wikipedia. https://en.wikipedia.org/wiki/Theory_of_planned_behavior

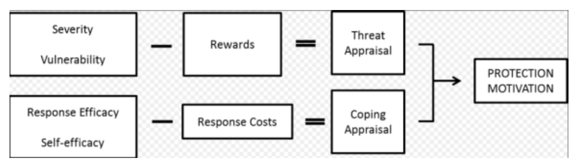

Figure 4. Protection Motivation Theory framework illustrating threat and coping appraisal components.

Source: HandWiki. Protection Motivation Theory. Encyclopedia. https://encyclopedia.pub/entry/28091

2.3 Review of Key Empirical Studies

Various empirical research investigating healthcare cybersecurity awareness programs has examined human behavior's contribution to defending against cyberattacks in these facilities. Alhuwail et al. (2021) conducted research which evaluated how public health facility healthcare professionals understood cybersecurity hazards as well as their behavioral responses. Staff members showed high security policy awareness but failed to adopt secure practices in password management alongside phishing attempt identification. Better training initiatives must be developed because awareness programs currently do not lead to behavioral changes in healthcare workers.

A systematic review completed by Nifakos et al. (2021) analyzed human factor effects on cybersecurity throughout healthcare institutions. Various human mistakes during data management and security protocol noncompliance turned out to be primary contributors to cyber events in hospital settings based on review findings. Security training needs human-focused solutions including training through role-playing exercises and performance evaluation to solve these human errors in cybersecurity systems. The researchers from Kioskli et al. (2023) found that implementing cybersecurity hygiene measures is vital for healthcare 4.0 systems that use AI-connected information systems to stop human errors. The authors discovered that when cybersecurity training focused on the work responsibilities and duties of medical staff it enhanced both service compliance and risk identification abilities.

Tambe-Jagtap (2023) carried out recent research that extended previous findings to show healthcare organizations need behavioral intervention approaches above basic awareness programs in hospital cybersecurity programs. Research established that prevention of cyber incidents succeeded better through programs which focused on mental and decision-making processes. The research indicates healthcare cybersecurity programs need to educate while developing behavioral changes in professionals for better security compliance and reduced human mistakes.

2.4 Research Gaps and Emerging Issues

Current research on human-centric cybersecurity in healthcare faces important gaps which include the assessment of long-term behavioral changes and cultural obstacle management. Short-term awareness programs usually succeed according to studies conducted by Nifakos et al. (2021) but information remains limited about the long-term sustainability of these implemented behavioral changes. Current investigations about security behavior focus only on immediate changes following training programs yet lack sufficient data demonstrating the long-term impact of interventions when healthcare providers face high demands under dynamic situations. Future research must assess how well healthcare professionals keep cybersecurity practices and their ongoing commitment to security policies since digital health tools keep developing.

Several studies neglect the existing cultural and organizational obstacles that stand in the way of implementing human-centric cybersecurity strategies. The wide range of organizational cultures and leadership support levels alongside varying resources in healthcare institutions directly influence the outcome of their cybersecurity awareness and compliance efforts (Kioskli et al., 2023). Hierarchical organization structures that block open risk communication within healthcare facilities result in unwilling or unwilling security compliance from staff members. Research has not provided sufficient evidence regarding the full effect cultural factors have on cybersecurity results or effective training program solutions for these factors.

The continuation of healthcare cybersecurity frameworks brings obstacles due to the integration of new emerging technologies comprising artificial intelligence (AI) and machine learning (ML). Emerging technologies demonstrate effective potential in threat detection but existing research remains sparse about their influence on human behavior for compliance purposes. The implementation of advanced technologies creates complex issues regarding how healthcare workers relate to AI-based cybersecurity tools both in perception and trust and during usage. The development of future-proof cybersecurity strategies for healthcare must tackle known barriers for their effective implementation.

The healthcare sector requires additional research to bridge existing gaps which will help sustain human-centered cybersecurity solutions both in the immediate term and long-term.

III. KEY CHALLENGES IN BRIDGING AWARENESS AND ACTION

3.1 Cognitive and Behavioral Barriers

Psychological resistance, forgetfulness, and risk perception represent significant cognitive barriers to cybersecurity compliance, especially in high-pressure environments like healthcare. Security policies get compromised through psychological factors even though individuals maintain knowledge of security threats and risks. The barriers create actions that oppose training program directions thus failing to deliver intended cybersecurity effectiveness.

The main obstacle hindering cybersecurity adherence derives from psychological resistance because employees think these practices slow down their workflow and occupy too much time. Healthcare professionals face continuous time constraints according to the analysis of Chowdhury, Adam, and Skinner (2019) which results in "cybersecurity fatigue." Staff members develop cognitive obstacles to following security protocols because these policies coupled with frequent password requirements and heightened alertness seem to interfere with clinical duties. The continuous resistance causes healthcare professionals to take shortcuts which leads to deliberate security measure avoidance through improper logout procedures and easy password management.

Forgetfulness is another common barrier. The heavy cognitive burden in high-stress healthcare facilities frequently causes memory and attention failures which make healthcare professionals fail to properly implement security procedures. According to Andrade and Yoo (2019) cognitive load actions on decision making enable people to forget basic cybersecurity requirements such as data backup operations and software update protocols due to mental strain. Healthcare staff who manage patient care as well as documentation and communication tasks commonly decide to postpone security work which results in a higher probability of failing to meet compliance.

The perception of risks by individuals becomes the decisive factor for their adoption of secure behaviors. Numerous healthcare professionals view cyber threats as improbable and distant when they have never encountered a security breach personally. According to Raywood-Burke (2023) people under stress make subjectively pressured decisions in specific contexts which cause them to choose urgent necessities instead of securing their future stability. Healthcare professionals who do not accurately perceive security risks together with underestimating the severity of data breaches develop resistances to take proactive security actions.

The collective strength of cognitive barriers causes cybersecurity programs to become less effective because people understand security needs yet do not consistently execute them because of psychological influences. Healthcare interventions must adopt strategies to decrease cognitive strain while making decisions more relevant in hospital settings that determine how healthcare providers behave.

3.2 Organizational Culture and Leadership

Healthcare cybersecurity outcomes together with leadership approaches and institutional culture determine how staff members behave in matters of cybersecurity. The approach of treating cybersecurity as solely a technical matter exists in numerous institutions where security fails to take permanent root as an organizational value. The methods leaders employ together with the cultural environment of an organization determine whether staff members get support or obstacles when performing security tasks.

Leadership effectiveness stands as the primary element to create an organization-wide cybersecurity consciousness. Leaders implementing a top-down method have substantial power to shape workplace actions through decisive expectations about cybersecurity while making this security crucial for operational routines. According to Watkins (2023) healthcare organizations led by visible executives who support cybersecurity through funding allocation and team responsibility systems alongside security best practice promotion achieve superior compliance standards. The emphasis on traditional management duties alongside rewards without motivation becomes a hindrance to achieving employee commitment to cybersecurity behavior in organizations that display transactional leadership attributes. Leaders who stay inactive in cybersecurity practices or demonstrate insincere support for security cause their employees to lower their priority of security measures.

The way in which people conduct themselves in terms of cybersecurity depends strongly on both the culture of their organization and leadership styles in place. Security-first culture programs within institutions link cybersecurity practices to all operational areas starting from patient care to administrative processes leading to superior compliance outcomes and risk reduction. Branley-Bell, Coventry and Sillence (2021) demonstrate the need to create workplace conditions that make employees responsible for system security maintenance. The defined culture must teach employees both how to follow security protocols while also demonstrating how patient and organizational safety will suffer from security failures. Willie (2023) advocates for building an organizational culture which prioritize proactive security behavior because this approach improves institutional readiness against cyber threats.

Hierarchical cultures operating in numerous healthcare organizations work against implementing effective cybersecurity practices. Employees within these cultures avoid reporting cybersecurity incidents for the fear of negative consequences which obstructs the creation of an open-learning context. Security risks become difficult to implement consistent policies and achieve compliance because the insufficient collaboration exists between IT staff members and healthcare professionals.

The adoption of secure behaviors depends on healthcare organizations that have committed engaged leaders who take proactive actions to develop security as an essential organizational value at every level. Nor can secure cybersecurity governance exist without correct cultural and leadership doctrine alignment because both technical framework and human conduct need to blend seamlessly.

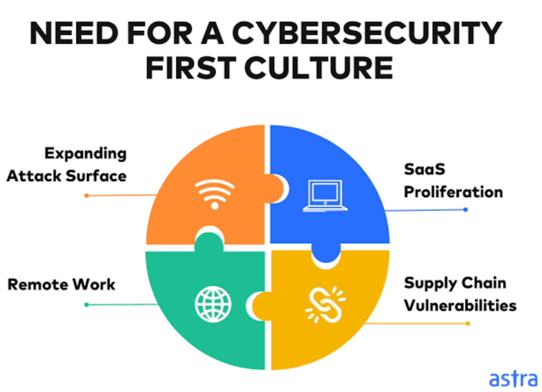

Figure 5. Key components of building a cybersecurity culture.

Source: Jain, S. How to Build a Cyber Security Culture? Astra Security. https://www.getastra.com/blog/security-audit/building-a-cyber-security-culture/

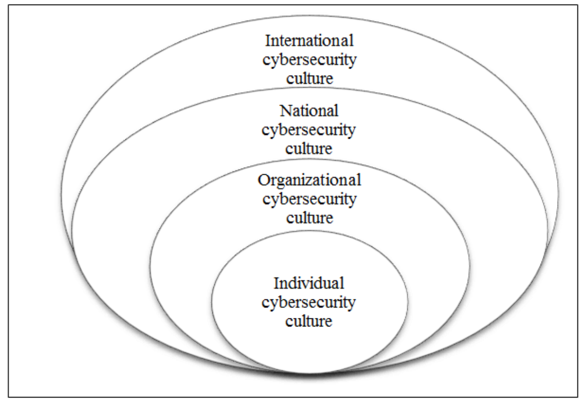

Figure 6. Cybersecurity culture levels across international, national, organizational, and individual domains.

Source: Von Solms, R., & Van Niekerk, J. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. Proceedings of the 11th International Conference on Cyber Warfare and Security, 307–314. https://www.researchgate.net/figure/Cybersecurity-culture-levels_fig1_306407687

3.3 Technological Usability and Design Flaws

Careful design and usability of healthcare information systems strongly influence the practices of cybersecurity. Complex system designs along with bad user interface elements establish strong obstacles which cause users to break security protocols leading to more cybersecurity risks. Users who focus on patient care tend to bypass security measures through noncompliance when healthcare workflows do not smoothly integrate with difficult-to-use systems.

Complexity of healthcare information systems stands as a primary source behind employees developing poor cybersecurity behaviors. Stobert et al. (2020) reported that emergency departments confront complicated systems which make it challenging for staff to complete various tasks including security procedures since quick decisions and efficient communications represent their most pressing needs within this environment. Hospital staff members in high-pressure situations tend to skip security measures because they need to focus on patient needs before security protocols like encryption and logout procedures. Simplified security procedures combined with repeated authenticity tests frequently lead to user dissatisfaction which drives users to create unsupported security methods. Medical workers expose themselves to cyber risks by using the same passwords multiple times while neglecting software updates and distributing password information to others.

The quality of user experience in healthcare systems works to intensify the existing security problems. Alhakami et al. (2022) explain that security measures including multi-factor authentication (MFA) together with encrypted communications become counterproductive when they obstruct workflow or function poorly thus forcing users to ignore security procedures. Heathcare professionals fail to understand the worth behind security measures that slow down their normal workflow. Systems inefficiencies lead organizations to approve security risks which damages the overall cybersecurity defense of their institution.

User-centered design functions critically to establish both security effectiveness and friendly usability of measures for systems. According to Nifakos et al. (2021) security protocols that match healthcare professional workflows result in higher compliance levels. Single sign-on (SSO) solutions enable better security while decreasing user login requirements for the complete day. User experience and security need equal priority during healthcare system development because it boosts both patient compliance and ensures staff safety from errors.

System usability along with complicated interfaces act as major obstacles to health care staff adopting secure behaviors. Developing user-friendly technology with embedded security elements goes hand in hand with improving cybersecurity performance and minimizing operational errors that threaten data security. To establish safety-as-a-part-of-natural-workflows healthcare systems must combine security enhancement mechanisms with usability improvements for easy adoption of secure practices by medical staff.

IV. SOLUTIONS AND MITIGATION STRATEGIES

4.1 Behavioral and Psychological Interventions

The use of behavioral science-based intervention methods proves vital for developing effective cybersecurity practices in healthcare organizations. People represent the primary cybersecurity vulnerability because their behaviors frequently fail to defend systems effectively so behavioral science methods help train healthcare staff better. These interventions function to modify and control user behavior so healthcare professionals adopt sustainable integrated cybersecurity procedures that support their daily work practices.

True behavioral interventions employ nudging as a method to prompt secure behaviors through indirect warning signals which function beyond traditional instructions. The implementation of nudges in healthcare cybersecurity creates automatic notification systems together with visual warning signals and default configuration selections which promote secure conduct. According to Khan et al. (2022) security functions activated as system defaults through strong password requirements and automatic session timeout help minimize human-related security breaches. Secure password upgrading and regular security training for users can be promoted through automated monitoring which helps users maintain adherence while avoiding forced submission requirements. Nudges serve as a system that makes desired security behaviors such as secure login practices simpler to carry out for users in order to improve cybersecurity results.

Through gamification Healthcare organizations create effective training solutions that use game-like methods to engage users within cybersecurity training programs. Healthcare institutions establish employee training motivation through strategies involving rewards together with challenges and tracking performance levels. Security training becomes more effective when organizations implement gamification through the research findings of Silic and Lowry (2020). Healthcare organizations should create security challenges that give rewards to users when they demonstrate adequate security skills in tasks like phishing identification and secure communication practice execution. Through gamified rewards such as points or badges and rankings employees develop both competitive engagement and a lasting memory of security protocols in a rewarding environment. Programs that offer game-based training stimulate behavioral retention because they supply instant feedback as users learn along with rewarding activities that rigorously develop secure procedures.

Habit-formation techniques create essential pathways to develop secure behaviors into automatic operations that become routine practice. The implementation of regular small progressions enables healthcare organizations to develop safe cybersecurity practices which employees will naturally carry out. Habit formation as a process needs regular repetition and repeated activation to develop secure actions into automated practices. Healthcare workers should complete password changes and logouts as predetermined time intervals happen throughout their duties which could include both patient interactions and shift conclusions. Repetitive performance of these security protocols creates automatic responses so users will follow security protocols without deliberate thought. Khan et al. (2022) explain that micro-learning sessions help healthcare staff practice small security tasks during their work breaks to develop regular security habits leading to lasting cybersecurity practice compliance.

Behavioral science-based approaches of nudging and gamification and habit formation serve as effective instruments which modify healthcare professionals' cybersecurity behaviors. The security practices embedded into work culture maintain higher patient data protection through these methods which additionally enhance both engagement and compliance rates. Healthcare institutions should include these behavioral science-based interventions into their existing training system alongside organizational practices to handle cybersecurity human elements and safeguard sensitive patient information.

4.2 Organizational Policies and Change Management

Both nudging and gamification alongside habit formation interventions draw powerful strength from behavioral science to build cybersecurity behaviors within the healthcare professional workforce. The security practices embedded into work culture maintain higher patient data protection through these methods which additionally enhance both engagement and compliance rates. Healthcare institutions should include these behavioral science-based interventions into their existing training system alongside organizational practices to handle cybersecurity human elements and safeguard sensitive patient information.

Policy Implementation Strategies

The beginning of policy implementation rests on creating complete cybersecurity policies which specifically address healthcare environments and express clear definitions for all aspects. According to Moustafa, Bello and Maurushat (2021) the policy development process should begin early with involvement of key stakeholders including IT staff as well as department heads and end-users to create usable and executable policies. Security policies need to focus on solving the main risks from human mistakes caused by poor password practices and vulnerability to phishing attacks together with device non-security when unattended. Decision makers must update company policies at regular intervals because it allows them to adapt security measures to contemporary cyber risks and new rules.

Organizations need to use gradual stages for implementing policies effectively. Creating employee awareness about cybersecurity along with data protection education stands as the first step to implement effective security measures. The training program needs proper organization and customization of content to help various staff types including administrative workers and healthcare providers learn their cybersecurity contribution roles. After widespread employee training the organizational policies must be enforced by conducting audits as well as regular monitoring and compliance evaluations. The implemented measures verify that staff members maintain adherence to procedural standards while shouldering their cybersecurity duties.

Communication Practices

An organization needs clear and consistent communication in order to execute cybersecurity policies effectively. The delivery of security practices and organizational security standards becomes possible through effective communication methods. Organizations should employ various communication channels that include email newsletters with in-person meetings and intranet platforms for promoting cybersecurity policies and best practices according to Moustafa et al. (2021). Visual materials presented as posters or infographics support the clarification of significant concepts. Security cultures should receive active leadership endorsement through the implementation of dialogue support systems which address worker security concerns.

The process of communication requires receiving information from others known as "feedback." By implementing feedback systems that combine staff surveys with individual meetings organizations achieve two objectives: they evaluate policy success and detect operational weaknesses. The feedback methodology helps find training deficiencies together with points in which employees experience trouble upholding security standards. The ability to collect such feedback helps companies maintain their cybersecurity policies while making sure that these policies help employees stay secure.

Incentives for Secure Behavior

Organizations should establish incentive programs for their employees to reward them when they follow security protocols. Organizations use many forms of incentive programs which incorporate both official accolades and substantial financial bonuses that result in added time off for employees. According to Moustafa et al. (2021) positive reinforcement serves as an effective motivational tool for employees to ensure their security behavior remains consistent despite their patient care responsibilities.

Organizations need incentives that reinforce both their business targets and cybersecurity mission. A "security champion" program should acknowledge healthcare workers who both identify phishing incidents and maintain proper password rules because these behaviors demonstrate essential security responsibilities. Such programs use leaderboards showing departmental or individual achievement of compliance levels to promote healthy competition followed by incentives.

The successful execution of security-focused organizational policies together with structured communication systems and motivational incentives creates vital structures for spreading human-centric cybersecurity behavior throughout healthcare facilities. These combined factors enable health systems to build an environment that allows staff members to prioritize cybersecurity thus generating a safer organizational culture. By continuously evaluating policies and providing feedback for policy adjustments organizations maintain security efforts that stay linked to developing threats and business goals while providing long-term cybersecurity management solutions.

4.3 Human-Centered Design and UX Approaches

HCD and UX strategies function as vital cybersecurity risk reduction tools which minimize potential user errors in healthcare IT systems. These methods ensure proper focus on what healthcare professionals need by addressing their capabilities while enhancing their work processes in their demanding settings. Security failures within this context mainly result from subpar system structure that makes secure conduct challenging. Healthcare IT systems that follow HCD principles will merge security measures optimally with user interfaces to develop easy and natural safe operating practices.

Human-centered design requires complete empathy towards users as one of its fundamental principles. Healthcare professionals need to be acknowledged for their time constraints while working with multiple tasks and their main goal being patient welfare instead of information technology compliance. According to Tremosa (2023) unthoughtful interface construction results in deaths affecting both patient care delivery and cyber security. Hispanic clinicians fail to perform essential security actions because they get distracted by complex layouts and unclear system notifications placed on healthcare interfaces. Users create unsafe methods such as password sharing and MFA disabling because security procedures slow down workflow and require additional cognitive work.

Security features embedded in systems have the goal of preventing user behavior that could lead to vulnerabilities while offering functions which are both powerful for security and disruptive to the user experience at a minimum level. Systems which use biometric authentication together with single sign-on (SSO) protocols let users bypass the need for password changes that create user dissatisfaction. These security tools provide users with convenient access through secure functionality. Users will achieve better compliance while maintaining speed by following contextual warnings and tooltips which prompt them before completing dangerous operations like sending unsecured data.

Security prompt perception and user reaction are strongly affected by both the way information is presented visually and the manner in which users interact with the system. The use of color-based indicators together with symbolic images and structured presentation helps users locate important security features. The visual placement of an expired certificate warning in prominent red-colored emphasis helps users avoid unintentionally skipping the precaution. The method of progressive disclosure by which advanced controls are hidden until required helps users maintain focus on significant security options while lowering the visual complexity and mental effort.

Healthcare UX development uses iterative testing methods that require user feedback. The evaluation of health staff using actual systems identifies system trouble points and error-prone locations for users. Designers use these findings to make interface improvements based on user actual implementation instead of hypothetical projections. According to Tremosa (2023) "design for error" principles should be adopted because they foresee user mistakes by adding confirmation dialogs and undo capabilities with clear feedback to help users avoid errors.

Effectively designed systems provide major benefits to both onboarding and training because users can easily understand the platforms. The ease of understanding an interface directly reduces user barriers to secure system use since they do not require additional teaching. System-based tutorials provide more effective teaching of security principles than standardized or broad training methods because they present content in real-world contexts.

Healthcare IT systems need human-centered design and UX approaches as fundamental components for reducing user error frequency and securing information systems. This approach establishes security protocols as the simplest way to accomplish tasks which decreases attacks that originate from human mistakes. Instructional UX design mechanisms both enhance clinical operational speed and instill a security-oriented cultural framework which makes regulatory compliance natural and effortless for healthcare staff.

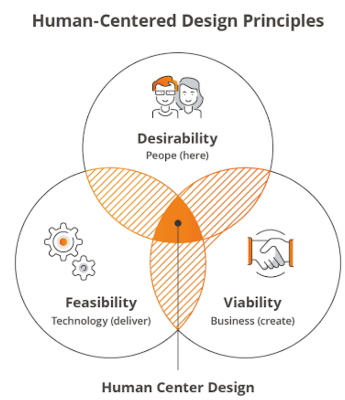

Figure 7. Human-Centered Design principles: Desirability, Feasibility, and Viability.

Source: Future Processing. Human-Centered Design: How Empathy and Innovation Shape IT Products. https://www.future-processing.com/blog/human-centered-design-as-key-to-an-it-products-success/

CONCLUSION

5.1 Summary of Key Findings

Security practices in healthcare need more than practical cybersecurity training to bridge awareness gaps because they need a human-oriented comprehensive system. The study has realized three main barriers to cybersecurity awareness including cognitive and behavioral memory problems coupled with risk misinterpretation alongside staff unwillingness to adapt. System weaknesses also develop unsafe operating procedures because of poor usability. Behavioral science-based interventions are missing from most awareness programs leading to their inability to achieve lasting behavioral change according to literature findings. Merges between behavior change methods like nudges with gamification methods and habit-forming training strategies and secure-by-design user experience approaches which link security measures effectively to clinical operational requirements lead to successful outcomes. The combination of organizational policies with supporting communication and leadership backing boosts security compliance. Studies fail to capture lasting behavioral changes in healthcare staff and they need better approaches to analyze behavior patterns in different medical environments. Both evidence-based approaches and human elements working together in alignment create the path to move beyond awareness into actual action.

5.2 Implications for Healthcare Stakeholders

The study findings produce immediate implications which benefit various participants in healthcare systems. At the front lines of healthcare service both user interfaces and security protocols should remain intuitive so workers can practice safe behaviors while still delivering patient care. The implementation of human-centered design principles and behavioral insights by IT professionals enables them to create cybersecurity solutions which match user conduct thus producing better results. Policy administrators and makers gain value from recognizing the need for security culture development through psychological training and leadership support and incentive-based systems because mandatory requirements alone prove insufficient. Healthcare institutions can produce secure yet user-friendly policies and systems through a comprehensive interdisciplinary implementation method. Security strategies become sustainable and maintain their appropriate context through staff collaboration which combines members from clinical departments, technical teams and administrative roles. The achievement of healthcare cybersecurity resilience stems from shared human responsibility which design and patient behavior intersect with organizational culture.

5.3 Recommendations and Future Research Directions

Longitudinal research needs to become a priority for assessing how well safety behaviors maintain themselves after training and understanding cultural factors that affect cybersecurity practices in various healthcare settings. Healthcare institutions need to invest in default-secure system designs together with supported behaviorally informed training programs while working to create one unified security culture. Research should analyze adaptive training technologies that use AI for personalization while determining their practicality for healthcare clinics. Stakeholders need to work together in developing standards that unite UX practices with behavioral science theories along with organizational psychology to form resilient systems. Interdisciplinary innovation that originates from healthcare realities must become the foundation for the transformation of awareness into secure action habits.

REFERENCES

[1] Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & AlDuaij, S. (2021). Information security awareness and behaviors of health care professionals at public health care facilities. Applied Clinical Informatics, 12(4), 924–932. https://doi.org/10.1055/s-0041-1730373

[2] Alhakami, H., Baz, A., Alhakami, W., Pandey, A. K., Agrawal, A., & Khan, R. A. (2022). A usability management framework for securing healthcare information system. Computer Systems Science & Engineering, 42(3), 1015–1030. https://doi.org/10.32604/csse.2022.021155

[3] Andrade, R. O., & Yoo, S. G. (2019). Cognitive security: A comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications, 48, 102352. https://doi.org/10.1016/j.jisa.2019.102352

[4] Branley-Bell, D., Coventry, L., & Sillence, E. (2021, June). Promoting cybersecurity culture change in healthcare. In Proceedings of the 14th PErvasive Technologies Related to Assistive Environments Conference (pp. 544–549). https://doi.org/10.1145/3453892.3461310

[5] Cherukuri, B. R. (2019). Future of cloud computing: Innovations in multi-cloud and hybrid architectures.

[6] Malhotra, S., Saqib, M., Mehta, D., & Tariq, H. (2023). Efficient Algorithms for Parallel Dynamic Graph Processing: A Study of Techniques and Applications. International

Journal of Communication Networks and Information Security (IJCNIS), 15(2), 519-534.

[7] Chowdhury, N. H., Adam, M. T., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. Behaviour & Information Technology, 38(12), 1290–1308. https://doi.org/10.1080/0144929X.2019.1581251

[8] Deibert, R. J. (2018). Toward a human-centric approach to cybersecurity. Ethics & International Affairs, 32(4), 411–424. https://doi.org/10.1017/S0892679418000665

[9] Gopireddy, R. R., & Bodipudi, A. (2022). Human-centric cybersecurity: Addressing the human element in cyber defense and ethical considerations in cybersecurity. Journal of Artificial Intelligence & Cloud Computing, 1(4), 2–5. https://doi.org/10.47363/JAICC/2022(1)E118

[10] Kilari, S. D. (2022, February). Optimizing manufacturing systems with AI: Reducing human errors and enhancing response times in MES and supply chain ordering systems. International Journal of Engineering Technology Research & Management, 6(2). IJETRM.

[11] Grobler, M., Gaire, R., & Nepal, S. (2021). User, usage and usability: Redefining human centric cyber security. Frontiers in Big Data, 4, 583723. https://doi.org/10.3389/fdata.2021.583723

[12] Kaushik, P., Jain, M., Patidar, G., Eapen, P. R., Sharma, C. P., Department of ECE, Institute of Technology, Nirma University, Ahmedabad, India, & Department of CSE, Rajasthan Technical University, Kota, India. (2018). Smart Floor Cleaning Robot Using Android. In International Journal of Electronics Engineering (Vol. 1100, Issue 22, pp. 502–506). https://www.csjournals.com/IJEE/PDF10-2/64.%20Puneet.pdf

[13] Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. Computers & Security, 120, 102826. https://doi.org/10.1016/j.cose.2022.102826

[14] Kilari, S. D. (2016). A novel approach to control corrosion behaviour on bio materials using Taguchi method (design of experiments). The University of Texas at El Paso.

[15] Kim, S. H., Yang, K. H., & Park, S. (2014). An integrative behavioral model of information security policy compliance. The Scientific World Journal, 2014, 463870. https://doi.org/10.1155/2014/463870

[16] Cherukuri, B. R. Enhancing Web Application Performance with AI-Driven Optimization Techniques.

[17] Kioskli, K., Fotis, T., Nifakos, S., & Mouratidis, H. (2023). The importance of conceptualising the human-centric approach in maintaining and promoting cybersecurity-hygiene in healthcare 4.0. Applied Sciences, 13(6), 3410. https://doi.org/10.3390/app13063410

[18] Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, 561011. https://doi.org/10.3389/fpsyg.2021.561011

[19] Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119. https://doi.org/10.3390/s21155119

[20] Onumo, A. O. (2020). A behavioural compliance framework for effective cybersecurity governance and practice (Doctoral dissertation, University of Bradford). http://hdl.handle.net/10454/18236

[21] Raywood-Burke, G. (2023). Cognitive load and subjective time pressure: How contextual factors impact the quality of cyber-security decision making (Doctoral dissertation, Cardiff University). https://orca.cardiff.ac.uk/id/eprint/160860

[22] Kaushik, P., Jain, M., Patidar, G., Eapen, P. R., & Sharma, C. P. Smart Floor Cleaning Robot Using Android.

[23] Kilari, S. D. (2022, February). Optimizing manufacturing systems with AI: Reducing human errors and enhancing response times in MES and supply chain ordering systems. International Journal of Engineering Technology Research & Management, 6(2). IJETRM.

[24] Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. Journal of Management Information Systems, 37(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

[25] Stobert, E., Barrera, D., Homier, V., & Kollek, D. (2020, April). Understanding cybersecurity practices in emergency departments. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1–8). https://doi.org/10.1145/3313831.3376716

[26] Tambe-Jagtap, S. N. (2023). Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents. SHIFRA, 2023, 53–59.

[27] Tremosa, L. (2023). Healthcare UX—Design that saves lives. Interaction Design Foundation. https://www.interaction-design.org/literature/article/healthcare-ux-design-that-saves-lives

[28] Cherukuri, B. R. (2024). Serverless computing: How to build and deploy applications without managing infrastructure. World Journal of Advanced Engineering Technology and Sciences, 11(2).

[29] Triplett, W. (2021). Establishing a cybersecurity culture organization. Acta Scientific Computer Sciences, 3(8).

[30] Watkins, M. E. (2023). Designing an effective organizational culture to guard against the cyber risks of emerging technologies. Journal of Healthcare Management, 68(4), 239–250. https://doi.org/10.1097/JHM-D-22-00162

[31] Willie, M. M. (2023). The role of organizational culture in cybersecurity: Building a security-first culture. Journal of Research, Innovation and Technologies, 2(2(4)), 179–198.

[32] Dixit, S., & Jangid, J. (2024). Asynchronous SCIM Profile for Security Event Tokens. Journal of Computational Analysis and Applications, 33(6).

[33] (Figure 1) Keepnet Labs. Human-Centric Cybersecurity: Building Stronger Defenses by Focusing on People. https://keepnetlabs.com/blog/human-centric-cybersecurity-prioritizing-people-in-cyber-defense

[34] (Figure 2) How Cybersecurity Improves Healthcare Information Systems. https://stefanini.com/en/insights/news/how-cybersecurity-improves-healthcare-information-system

[35] (Figure 3) Wikipedia contributors. Theory of planned behavior. Wikipedia. https://en.wikipedia.org/wiki/Theory_of_planned_behavior

[36] (Figure 4) HandWiki. Protection Motivation Theory. Encyclopedia. https://encyclopedia.pub/entry/28091

[37] (Figure 5) Jain, S. . How to Build a Cyber Security Culture? Astra Security. https://www.getastra.com/blog/security-audit/building-a-cyber-security-culture/

[38] (Figure 6) Von Solms, R., & Van Niekerk, J. (2016). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. Proceedings of the 11th International Conference on Cyber Warfare and Security, 307–314. https://www.researchgate.net/figure/Cybersecurity-culture-levels_fig1_306407687

[39] (Figure 7) Future Processing. Human-Centered Design: How Empathy and Innovation Shape IT Products. https://www.future-processing.com/blog/human-centered-design-as-key-to-an-it-products-success/