Synergizing Human Behavior and Cybersecurity: A Literature Review

Author:

Syeda Areej Asif
Shahreen Sheikh
Farees Fatima

Affiliation: Hamdard University

Date of Submission: 17th January 2025

Abstract

The growing complexity of cybersecurity challenges necessitates a dual focus on technological advancements and human-centric strategies. Human error continues to be a critical vulnerability in the cybersecurity chain, with issues such as phishing attacks, weak password management, and low compliance with security protocols contributing to security breaches. This literature review integrates insights from multiple studies, examining frameworks such as the Security Behavior Intentions Scale (SeBIS) and the Human Aspects of Information Security Questionnaire (HAIS-Q). Emerging methodologies like biometric tracking and real-time behavioral monitoring are also discussed, reflecting the integration of advanced tools for understanding human factors in cybersecurity.

Key findings highlight the significant role of cognitive biases, organizational culture, and training effectiveness in shaping user behavior and enhancing cybersecurity resilience. Typologies, such as those identifying expert and non-expert user behaviors, offer pathways for tailored interventions. However, critical gaps persist, including limited applicability to IoT ecosystems, lack of cross-cultural validations, and inadequate adaptive tools capable of addressing evolving threats. Research also reveals a disproportionate focus on Western populations, which limits the generalizability of existing studies.

Future directions emphasize the integration of real-time behavioral tracking, AI-driven analytics, and culturally adaptive frameworks to bridge the divide between technological and human-centered approaches. By addressing these gaps and leveraging multidisciplinary perspectives, the field can advance toward a robust cybersecurity culture. This review advocates for a shift from viewing humans as the weakest link to recognizing their potential as proactive contributors to cybersecurity resilience.

Table of Contents

1. Introduction

1.1 Understanding the Topic

Cybersecurity is no longer just about technology—it's about people. While encryption, artificial intelligence (AI), and real-time threat detection have significantly improved security, human error remains one of the biggest weaknesses. Studies show that over 90% of successful cyberattacks exploit human mistakes rather than technical flaws.

Phishing scams, weak passwords, and social engineering attacks prove that even the most advanced security systems can be compromised if people aren't careful. This is why modern cybersecurity isn't just about firewalls and antivirus software—it's about understanding human behavior, decision-making, and the way people interact with technology.

To address this, researchers have developed tools like the Security Behavior Intentions Scale (SeBIS) and the Human Aspects of Information Security Questionnaire (HAIS-Q). These frameworks assess how users behave in security-sensitive situations, offering insights that help organizations improve security policies. However, as the digital landscape evolves—especially with interconnected systems like the Internet of Things (IoT)—new challenges arise, requiring cybersecurity strategies that adapt to both technological changes and human tendencies.

1.2 Objectives

This literature review focuses on understanding how human behavior influences cybersecurity and evaluating the effectiveness of existing tools designed to measure security awareness and behavior. Specifically, it aims to:

Examine SeBIS, HAIS-Q, and other emerging frameworks to see how they assess security behavior.
Identify the strengths and limitations of these tools, especially in different organizational and cultural settings.
Explore gaps in real-time behavioral tracking and how AI-driven security systems can improve user safety.
Suggest future research directions, focusing on more adaptive cybersecurity strategies that integrate both human and technological factors.
By combining insights from psychology, data science, and cybersecurity, this review aims to help organizations develop smarter, more people-centered security strategies.

1.3 How This Paper is Structured

To present a clear and logical discussion, this paper is organized into five sections:

Introduction – Sets the stage for understanding the human side of cybersecurity.
Thematic Review – Traces how cybersecurity has evolved, discusses the latest research on security behavior, and explores tools used to measure user awareness.
Critical Analysis – Evaluates the strengths and weaknesses of existing tools, identifying key research gaps.
Future Directions – Proposes new approaches, such as AI-driven security assessments, real-time monitoring, and gamified cybersecurity training.
Conclusion – Summarizes key findings and provides recommendations for improving cybersecurity through a human-centered approach.

2. Thematic Review

2.1 A Look Back: How Cybersecurity Evolved

In the past, cybersecurity was all about technology—firewalls, antivirus software, and network security. But over time, major security breaches revealed a critical flaw: technology alone isn't enough.

A prime example is the 2013 Target data breach, where hackers gained access to sensitive customer information by exploiting weak security practices within a third-party vendor. The breach wasn't due to a failure in technology, but rather a human mistake—a lapse in password security and vendor oversight.

This incident, among others, forced organizations to rethink their approach. Instead of focusing only on technical solutions, they started incorporating human behavior research into their security strategies. This shift led to the development of SeBIS and HAIS-Q, which measure security awareness and behavioral tendencies, helping organizations understand and mitigate human-related risks.

2.2 Recent Developments: How Research is Evolving

With cyber threats growing more sophisticated, researchers have expanded their focus beyond just user awareness. New studies have classified users into categories based on their security behavior. For example:

"Naïve Greenhorns" – Individuals with little to no security awareness, prone to falling for phishing scams.
"Reliable Troupers" – People with strong security habits who regularly update passwords and recognize threats.
By identifying these behavioral patterns, organizations can create customized security training programs instead of using a one-size-fits-all approach.

Another major advancement is the use of AI-driven tools for real-time security monitoring. Unlike traditional surveys, which only capture self-reported data, AI can track actual user

behavior—like how often someone clicks on suspicious links or how they respond to security warnings.

Other innovations include:

Biometric tracking – Using eye movement and stress detection to measure a user's response to cyber threats.
IoT security enhancements – Implementing machine learning models to detect anomalies in smart devices.
These advances show that cybersecurity is becoming more dynamic, moving beyond simple surveys to real-time, behavior-driven solutions.

2.3 How We Measure Cybersecurity Behavior

Researchers use different methods to assess human behavior in cybersecurity:

Surveys & Questionnaires – Tools like SeBIS measure security habits, while HAIS-Q evaluates organizational awareness and compliance.
AI & Machine Learning – Algorithms analyze user activity, detect anomalies, and predict potential risks.
Simulated Attacks – Organizations conduct controlled phishing tests to measure how employees respond to security threats.
Biometric Tracking – Eye movement tracking during simulated attacks can reveal how quickly and accurately users identify phishing attempts.
Interviews & Observations – Researchers conduct ethnographic studies to understand the reasoning behind security decisions.
Each of these approaches provides valuable insights, but together, they create a more complete picture of how people engage with cybersecurity.

2.4 Challenges & Unsolved Problems

Despite advancements, several challenges remain:

IoT security is still a major concern – Most cybersecurity frameworks weren't designed for smart home devices, industrial IoT, or connected cars, leaving gaps in how we protect these systems.
Static approaches don't adapt to real-time risks – Surveys provide useful insights but don't capture live behavioral changes, making them less effective in dynamic environments.
Security strategies don't always account for cultural differences – A security policy that works well in the U.S. may not be as effective in Asia or Europe, highlighting the need for cross-cultural validation.
As cyber threats evolve, researchers must focus on creating more adaptive security measures that integrate behavioral insights with real-time monitoring.Cross-Cultural Challenges and Biases

A major issue with current cybersecurity research is its narrow focus on Western contexts, which neglects the diverse cultural and organizational settings around the world. Cultural differences can significantly influence cybersecurity practices, yet many studies fail to address this, limiting the global applicability of their findings.

Another challenge lies in the reliance on self-reported data, which introduces biases. For example, people may overstate how compliant they are with security practices or downplay risky behaviors. This creates a gap between reported and actual behaviors, leading to skewed results.

To address these issues, there's a growing need for adaptive tools that combine real-time monitoring with culturally inclusive designs. Incorporating AI-driven analytics can help provide more accurate insights and actionable data, reducing the impact of biases and improving the reliability of findings.

3. Critical Analysis

3.1 Strengths and Weaknesses of Current Research

Frameworks like SeBIS and HAIS-Q offer structured ways to evaluate cybersecurity behavior, providing useful insights into habits, compliance, and awareness. These tools have been instrumental in designing targeted security interventions.

However, their heavy reliance on static, self-reported data is a major limitation. Self-reports are often influenced by social desirability bias, where participants might exaggerate their adherence to security protocols or minimize risky actions. This can lead to unreliable results.

For instance, tools like PCSASS work well in academic environments but lack scalability for broader contexts, such as corporate settings or small and medium-sized enterprises (SMEs). Businesses often face unique challenges, like resource constraints and varying levels of technical expertise, which aren't adequately addressed by these frameworks.

Despite these limitations, recent advancements in real-time behavioral monitoring and AI-driven tools offer promising solutions. Phishing simulations, for example, can dynamically adapt to user behavior, providing more precise and actionable feedback.

3.2 Contradictory Findings

There's also inconsistency in how effective cybersecurity training programs are. Some studies show that training improves awareness and reduces risky behaviors, like falling for phishing scams or using weak passwords. However, these positive effects often fade over time, with users reverting to insecure practices after the training ends.

Targeted interventions—such as those tailored to specific user types, like “Naïve Greenhorns” or “Reliable Troupers”—show promise but face scalability issues. A program that works in one organization or culture may not be effective in another.

Traditional training models also tend to focus on delivering knowledge rather than fostering practical, long-term behavior changes. Research suggests that experiential and gamified training environments—which immerse users in real-world scenarios—are more likely to produce lasting results.

3.3 Research Gaps

Several important gaps in cybersecurity research need to be addressed:

IoT-Specific Challenges: As IoT devices proliferate, they bring unique security risks that current tools like SeBIS and HAIS-Q aren’t equipped to handle. Issues such as device compatibility and rapidly changing threat landscapes require specialized frameworks.

Lack of Cross-Cultural Research: Most studies are based on Western populations, overlooking the cultural and organizational differences that influence cybersecurity behavior globally. This lack of diversity limits the development of universally applicable tools.

Static Assessments: Current tools fail to capture the dynamic nature of user behavior, especially in high-stress or rapidly evolving situations. Real-time monitoring systems powered by AI could fill this gap.

Leadership and Culture: The role of organizational leadership in fostering a culture of cybersecurity is underexplored. Top-down policies, leadership commitment, and workplace norms play a significant role in shaping user behavior.

4. Future Directions

4.1 Emerging Trends in Cybersecurity

Cybersecurity is evolving, with exciting new trends pointing the way forward.

IoT-Focused Frameworks: The rise of interconnected devices has created new vulnerabilities. Future tools need to address these risks with real-time monitoring and adaptive learning algorithms that can keep pace with evolving threats.

Gamified Training Programs: Introducing competition and rewards into training helps users stay engaged while practicing secure behaviors in simulated real-world scenarios. These programs are gaining popularity for their effectiveness in retaining user attention.

Biometric Insights: Data such as gaze tracking, stress analysis, and voice recognition is providing deeper insights into how users make decisions under pressure. This information can help predict vulnerabilities before they're exploited.

Blockchain for Data Security: Blockchain technology is being explored to improve the transparency and integrity of cybersecurity data, ensuring that behavioral insights are securely handled.

4.2 Key Research Questions

Future research should address the following questions:

1. How can cybersecurity tools adapt to IoT environments to tackle the unique risks posed by interconnected devices?
2. What methods can reduce biases in AI-driven security tools, ensuring they work effectively across different user demographics?
3. How can gamified and scenario-based training models improve the long-term adoption of secure practices?
4. What role can biometric data play in real-time monitoring and predicting cybersecurity risks?
5. How can ethical AI frameworks be implemented in cybersecurity without compromising user privacy?
6. What strategies can enhance the cross-cultural applicability of cybersecurity frameworks?
7. How can leadership and organizational culture foster better cybersecurity practices?
8. Can hybrid frameworks combining self-reported and real-time behavioral data improve the accuracy of risk assessments?

4.3 New Approaches and Methodologies

To address these challenges, researchers are exploring innovative methods:

Blockchain for Secure Data Handling: This ensures transparency and protects the integrity of behavioral data collected for cybersecurity purposes.
Dynamic Behavioral Analytics: AI-driven models with real-time feedback capabilities can help organizations identify risks as they happen and adapt their defenses accordingly.
Hybrid Tools: Combining traditional self-reported surveys with real-time monitoring allows for a more comprehensive view of user behavior. Machine learning algorithms can analyze patterns and predict vulnerabilities, enabling proactive interventions.
By integrating these new approaches, organizations can build more robust and adaptive security systems that address both technological and human-centric challenges.

5. Conclusion

5.1 Summary of Key Findings

Human-centric approaches, such as psychometric assessments and factor analysis, are indispensable for robust cybersecurity strategies. Tools like SeBIS and HAIS-Q provide foundational insights into user behaviors and organizational practices. However, these tools must evolve to incorporate IoT-specific capabilities and account for cross-cultural dimensions. Emerging methodologies, including AI-driven analytics and biometric data integration, promise to enhance cybersecurity frameworks by offering real-time adaptability and precision.

5.2 Unresolved Issues

Despite advancements, several critical gaps remain unresolved. IoT-specific assessments require further development to address the unique challenges posed by interconnected devices. Cross-cultural validation of existing frameworks is limited, necessitating more inclusive research to improve global applicability. The role of organizational leadership and its influence on cybersecurity culture has also been underexplored, leaving opportunities for future studies. Additionally, building trust in AI systems is vital for their effective adoption in cybersecurity practices. Addressing these issues is critical for advancing the field and fostering a resilient cybersecurity culture.

References

1. Egelman, S., & Peer, E. (2015). **Behavior Ever Follows Intention: Validation of the SeBIS.** Journal of Cybersecurity.
2. Baltuttis, D., Müller, L., & Reiter, A. (2024). **A Typology of Cybersecurity Behavior Among Knowledge Workers.** Computers & Security.
3. Parsons, K., Calic, D., Butavicius, M., & McCormac, A. (2017). **Determining Employee Awareness Using the HAIS-Q.** Journal Article.
4. Johnson, R., & Bowman, T. (2024). **Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale.** Educational Sciences.
5. Prümmer, J., Schilling, M., & Peters, L. (2024). **Establishing a Model for the User Acceptance of Cybersecurity Training.** Future Internet.
6. **The Psychology of Phishing: Understanding Why Users Get Hooked.** (2015). Human Factors Journal.
7. Baltuttis, D., Schilling, M., & Mayer, C. (2024). **Driving Behaviour Change with Cybersecurity Awareness.** Computers & Security.
8. Baltuttis, D., Schilling, M., & Mayer, C. (2025). **Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review.** Computers & Security.
9. Parsons, K., Calic, D., & McCormac, A. (2017). **Human Factors in Cybersecurity: Internet Addiction and Impulsivity.** Human Factors Journal.
10. **Trust as a Human Factor in Holistic Cyber Security Risk Assessment.** (2015). IEEE Conference.
11. **Human-Centered Cybersecurity: Designing for Humans.** (2015). IEEE Security & Privacy.
12. **Behavior Change Interventions for Cybersecurity.** (2017). ACM CHI Conference.
13. **An Integrated Model for Assessing Cyber-Safety Behaviors.** (2019). Computers & Security.
14. **Applying Behavioral Science to Address Cybersecurity Vulnerabilities.** (2015). Behavioral Science Journal.
15. **Human–Computer Interaction and Cybersecurity.** (2017). HCI International.
16. **Human Factors in Cybersecurity and the Role for AI.** (2015). AI and Cybersecurity Journal.
17. **The Human Factor in Cybersecurity: Robust & Intelligent Defense.** (2015). Proceedings of the International Cybersecurity Summit.
18. Baltuttis, D., & Others (2024). **A Typology of Cybersecurity Behavior Among Knowledge Workers.** Computers & Security.
19. Khaw, T. Y., Amran, A., & Teoh, A. P. (2024). **Building a Thematic Framework of Cybersecurity: A Systematic Literature Review Approach.** Journal of Systems and Information Technology.
20. Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). **Design Principles for Cognitively Accessible Cybersecurity Training.** Computers & Security.

21. Various Authors (2023). **State of the Art in AI and Machine Learning for Cybersecurity.** Cybersecurity Applications Journal.
22. Straub, D. W., & Ang, S. (2011). **Bridging Research-Practice Gaps in Cybersecurity.** MIS Quarterly.
23. Siponen, M., & Baskerville, R. (2018). **Behavioral Frameworks in Cybersecurity Training.** Information Systems Journal.
24. Abu Al-Haija, Q., & Al-Masri, H. (2024). **Human Factors in Cybersecurity.** IGI Global. https://doi.org/10.4018/979-8-3693-3451-5.ch011
25. Sutton, A., & Tompson, L. (2025). **Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review.** Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110
26. European Union Agency for Network and Information Security (ENISA). (2017). **Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.**
27. Schein, E. H. (2004). **Organizational Culture and Leadership.** Jossey-Bass.
28. Veiga, A., & Eloff, J. H. P. (2010). **A Framework and Assessment Instrument for Information Security Culture.** Computers & Security, 29(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002
29. Ajzen, I. (1991). **The Theory of Planned Behaviour.** Organizational Behaviour and Human Decision Processes, 50(2), 179–211.
30. Quinn, R. E., & Rohrbaugh, J. (1983). **A Spatial Model of Effectiveness Criteria: Towards a Competing Values Approach to Organizational Analysis.** Management Science, 29(3), 363–377.