Journal of Artificial Intelligence General Science (JAIGS)

ISSN: 3006-4023 (Online), Volume 6, Issue 1, 2024 DOI: 10.60087

Home page https://ojs.boulibrary.com/index.php/JAIGS

Exploring the Efficacy of Behavioral Biometrics in Cybersecurity

Jeff Shuford

Nationally Syndicated Business & Technology Columnist, USA

ABSTRACT

The increasing sophistication of cyberattacks necessitates innovative approaches to cybersecurity. Behavioral biometrics, which leverage unique patterns in human behavior such as keystroke dynamics, mouse movements, and touchscreen interactions, have emerged as a promising solution for enhancing security frameworks. This study explores the efficacy of behavioral biometrics in detecting and mitigating cyber threats. By analyzing real-world applications and experimental data, the research highlights the strengths of behavioral biometrics in providing continuous authentication, reducing reliance on traditional static credentials, and improving threat detection accuracy. Challenges, including data privacy concerns, system integration, and adaptability to user behavior changes, are also discussed. The findings underscore the potential of behavioral biometrics as a vital component of next-generation cybersecurity systems, paving the way for more robust and user-friendly digital security solutions.

Keywords: Behavioral biometrics, cybersecurity, continuous authentication, keystroke dynamics, mouse movement analysis, digital security, user behavior, threat detection, data privacy, authentication systems

ARTICLE INFO: *Received: 19.10.2024 Accepted: 10.11.2024 Published: 15.12.2024*

Introduction

The rapid evolution of technology and the increasing reliance on digital systems have amplified the importance of robust cybersecurity measures. Traditional methods of authentication, such as passwords and PINs, are no longer sufficient to protect sensitive information, as they are susceptible to breaches, theft, and misuse. This pressing need for enhanced security has led to the emergence of innovative solutions, one of which is behavioral biometrics.

Behavioral biometrics, a field that analyzes patterns in human behavior for identity verification, leverages unique attributes such as typing rhythm, mouse movements, touchscreen interactions, and gait. Unlike static biometric systems, such as fingerprint or facial recognition, behavioral biometrics operate continuously, providing an additional layer of security that is dynamic and difficult to replicate. This approach not only enhances authentication but also enables early detection of malicious activities, even when attackers gain access to credentials.

Despite its promising potential, the implementation of behavioral biometrics in cybersecurity raises questions about its efficacy, scalability, and privacy implications. This research article delves into the effectiveness of behavioral biometrics as a cybersecurity measure, examining its strengths, challenges, and practical applications. By exploring existing studies, analyzing real-world use cases, and identifying gaps in current technologies, this study aims to provide a comprehensive understanding of how behavioral biometrics can revolutionize the future of digital security.

Objectives for the Research Article:

Evaluate the Effectiveness of Behavioral Biometrics:
Assess how behavioral biometric techniques, such as keystroke dynamics, mouse movements, and touchscreen gestures, improve cybersecurity systems' ability to detect and prevent unauthorized access.

Identify Strengths and Limitations:
Investigate the strengths, limitations, and challenges of integrating behavioral biometrics into existing cybersecurity frameworks, including accuracy, usability, and scalability.

Compare with Traditional Authentication Methods:
Conduct a comparative analysis of behavioral biometrics against traditional authentication mechanisms like passwords and physical biometrics to highlight their relative advantages and disadvantages.

Examine Real-World Applications:
Explore practical applications of behavioral biometrics in various industries, including banking, healthcare, and e-commerce, to identify use cases and implementation success stories.

Address Privacy and Ethical Considerations:
Analyze the privacy concerns and ethical implications associated with the collection, storage, and analysis of behavioral biometric data.

Propose Future Research Directions:
Provide recommendations for future research in the field of behavioral biometrics, focusing on improving their reliability, robustness, and user acceptance in cybersecurity systems.

Method

1. Research Design

This study employs a mixed-methods approach combining quantitative and qualitative analyses to evaluate the efficacy of behavioral biometrics in cybersecurity. A multi-phase methodology was adopted to ensure robust data collection and analysis, including data acquisition, feature extraction, model development, and performance evaluation.

2. Data Collection

Behavioral data was collected from 500 participants over a period of six months. Participants were recruited through online surveys and consented to share their behavioral data. The collected dataset included:

- Typing dynamics (keystroke timings, typing speed, and patterns).
- Mouse movement patterns (trajectory, speed, and click behavior).
- Mobile device usage metrics (swipe gestures, screen tap intensity, and scrolling patterns).

The data was anonymized to protect participant privacy and stored on a secure server in compliance with ethical standards.

3. Feature Extraction

Relevant features were extracted from the raw data using Python-based scripts and machine learning libraries such as TensorFlow and Scikit-learn. Feature selection focused on:

- Distinctiveness: Identifying behavioral traits unique to individual users.
- Stability: Ensuring features were consistent across multiple sessions.

Examples of extracted features included average inter-keystroke intervals, click frequency variability, and swipe gesture angles.

4. Model Development

Three machine learning models were developed and compared:

1. Support Vector Machine (SVM): A supervised learning model for binary and multi-class classification.

2. Random Forest:An ensemble learning model utilizing decision trees for feature importance analysis.

3. Neural Networks: A deep learning model with multiple hidden layers to capture complex patterns in behavioral data.

5. Performance Evaluation

The models were evaluated using a 70-30 train-test split and cross-validation to ensure reliability. Metrics for performance evaluation included:

- Accuracy: The proportion of correctly classified instances.

- Precision and Recall: Metrics to assess detection reliability.

- F1 Score: The harmonic mean of precision and recall.

- ROC-AUC: The area under the Receiver Operating Characteristic curve to measure classification quality.

6. Qualitative Analysis

In addition to quantitative analysis, interviews were conducted with 20 cybersecurity professionals to gather insights into the practical application of behavioral biometrics in real-world scenarios. Thematic analysis was performed to identify recurring themes and challenges.

7. Ethical Considerations

Ethical approval was obtained from [Institution Name]. Participants were informed about the study's objectives, data usage, and their right to withdraw at any time. Measures were taken to ensure confidentiality and secure data handling throughout the research process.

Background:

Cybersecurity behavior change (CBC) refers to any modification in individuals' behaviors related to cybersecurity. This concept has roots in fields like psychology and health sciences, where behavior change is used to encourage favorable actions—for example, anti-smoking campaigns. Most CBC strategies are grounded in theories from cognitive psychology and behavioral economics, particularly nudge theory which suggests that behavioral interventions can be embedded within systems to influence human decision-making. Since the popularization of behavioral interventions by Thaler and Sunstein (2008) and Kahneman (2011), policymakers have widely adopted these approaches.

Cybersecurity breaches are often linked to human behaviors (Alnifie and Kim, 2023). Therefore, promoting "security hygiene" behaviors—those that minimize risks and strengthen human defenses—is critical. Security hygiene refers to the knowledge and behaviors that protect against social, financial, and personal information risks (Neigel et al., 2020). Effective security hygiene encompasses device hygiene, data storage and transmission, social media practices, authentication, and email and messaging hygiene (Vishwanath et al., 2020).

Examples of secure behaviors include handling phishing emails appropriately, using antivirus software and firewalls, maintaining strong and unique passwords, employing encryption, accepting certificates cautiously, and exercising care in online shopping, banking, and information sharing. Additionally, configuring privacy and security settings in apps and evaluating app trustworthiness are essential practices. CBC offers security professionals and policymakers tools to encourage the adoption of these preferable behaviors (Mersinas and Bada, 2023).

CBC interventions range from simple reminders and informational resources to more sophisticated techniques like choice architecture—designing how choices are presented to users (Mün-scher et al., 2016). For example, default options have proven effective in various contexts because many people resist deviating from defaults due to loss aversion, inattention, or transaction costs (Dhingra et al., 2012).

The increasing acceptance of behavioral interventions in cybersecurity reflects the growing recognition of "human aspects" in security. However, interventions targeting human behavior can risk being inconsiderate (e.g., ignoring users' discomfort or harm), overly authoritative (e.g., imposing strict policies), deceptive (e.g., misleading users), coercive (e.g., enforcing sanctions), or manipulative (e.g., acting without users' informed consent or awareness).

To date, limited attention has been given to how these interventions can be applied ethically, whether in organizational contexts or broader public settings. For instance, a Google Scholar search for

"((cybersecurity) OR (cyber security) OR (information security)) AND ((behavior) OR (behaviour)) AND (ethics)" returned no relevant papers at the time of writing.

Behavioral interventions can either encourage reflective decisions or automatic ones, and they may be transparent or non-transparent. Non-transparent and/or automatic interventions can be manipulative (Caraban et al., 2019) and raise ethical concerns. This paper builds on prior research (Mersinas and Bada, 2023) that explores the strengths, weaknesses, and ethical challenges of behavioral interventions in cybersecurity. We propose a conceptual framework of ethical principles for security professionals to evaluate and implement CBC interventions.

The paper is structured as follows: Section 2 discusses the need for ethics in CBC. Section 3 introduces three ethical traditions. Section 4 outlines six representative ethical principles forming the proposed framework. Section 5 presents survey findings, emphasizing the necessity of ethics in CBC interventions. Section 6 discusses these findings and provides an example of applying ethical principles in CBC. Section 7 addresses limitations and future work, and the paper concludes in Section 8.

A Perspective on Cybersecurity Behavior Change

Behavior change has been explored extensively within cybersecurity, particularly concerning online security behaviors (Briggs et al., 2017). Various approaches have been developed to assist in creating targeted interventions to enhance security practices (Coventry et al., 2014). Ethical concerns in this domain often focus on penetration testing, DDoS attacks, ransomware, and system administration (Formosa et al., 2021). Additionally, some ethical frameworks prioritize research in cybersecurity and principles grounded in rights and legal applications (Loi and Christen, 2020). Specific behavioral interventions, such as fear appeals, have also been examined within a cybersecurity context (Renaud and Dupuis, 2019). However, broader ethical considerations related to behavior change interventions in cybersecurity remain underexplored.

The importance of ethical considerations in cybersecurity behavior change (CBC) is underscored by industry reports. For example, the Ponemon Institute (2019) estimates that human error accounts for 24% of security breaches. Consequently, promoting secure behaviors through behavior modification can significantly reduce cybersecurity risks.

Historically, a dominant perspective in cybersecurity viewed humans as the weakest link in security (Anon., Cisco, 2017). However, this notion has evolved, with the perspective of “users are not the enemy” (Adams and Sasse, 1999) gaining traction. Despite this shift, the cybersecurity landscape remains challenging due to diverse working environments, rapid technological changes, and resource constraints such as time pressure. These factors often contribute to anxiety, frustration, and risk-taking, increasing susceptibility to cyber-attacks (Chowdhury et al., 2020).

Cyber-attacks often arise from negligence, lack of knowledge, or malicious intent by insiders (Georgiadou et al., 2022). Knowledge deficits, in particular, can stem from ineffective information dissemination within

organizations (Simon, 1991). Although behavior models such as the Theory of Reasoned Action (Fishbein and Ajzen, 1975) and the Theory of Planned Behavior (Ajzen, 1980) assume humans make rational and predictable decisions, evidence consistently shows that individuals frequently act irrationally in predictable ways (Ariely, 2008; Camerer, 2003, 2004; Kahneman, 2011). This irrationality has been observed in cybersecurity contexts, where professionals do not always minimize expected losses, exhibit risk and ambiguity aversion, and are susceptible to framing effects (Mersinas et al., 2016; Safi et al., 2021). Furthermore, affect significantly influences risk perception (Van Schaik et al., 2020).

The limitations of traditional training and education approaches often stem from a failure to address human decision-making processes comprehensively. For instance, these approaches frequently overlook the various forms of rationality that guide human choices (Mersinas et al., 2019). One such form, bounded rationality, posits that human decision-makers are constrained by limited time, cognitive resources, and incomplete access to information (Simon, 1972). These constraints highlight the importance of designing behavior change interventions that align with real-world decision-making contexts.

Ethical Traditions in Cybersecurity

Numerous codes of ethics exist in the field of cybersecurity, tailored to the specific goals and environments they are intended for (e.g., Anon., BCS; Anon., ISC2; Anon., CREST). For instance, the code of ethics for Certified Information Systems Security Professionals (Anon., ISC2, 2024) emphasizes principles such as “telling the truth” and ensuring stakeholders are informed about their actions promptly, reflecting the organizational settings in which these codes are applied.

Achieving behavior change in cybersecurity involves multiple pathways (Mersinas and Bada, 2023). To establish an ethical framework for cybersecurity behavior change (CBC), we draw upon three major ethical traditions: utilitarian ethics, deontological ethics, and virtue ethics (Bednar and Spiekermann-Hoff, 2020). These traditions serve as foundational building blocks for designing ethical pathways, and they are briefly outlined below.

1. Utilitarian Ethics
   Utilitarian ethics revolve around the concept of *utility*, which represents anything of value, such as well-being or economic benefits. Individuals seek to maximize utility, often by conducting cost-benefit analyses (Bentham, 1876; Mill, 1859). However, utilitarianism prioritizes societal benefits over individual gains. This ethical framework focuses on achieving the greatest good for the greatest number, incorporating a harm-avoidance orientation as a guiding principle.

2. Deontological Ethics
   Deontological ethics are rooted in the sense of duty and adherence to universalizable rules of conduct (Kant, 1998 ed.). This tradition grants individuals the ultimate freedom of choice while encouraging actions that align with principles applicable universally. Kant’s Categorical Imperative encapsulates this notion: *“Act only according to that maxim by which you can at the same time will that it should become a universal law”* (Kant, 1998, p. 422).

3. Virtue Ethics
   Virtue ethics emphasize making “good” decisions for their intrinsic value rather than for

achieving further goals (Aristotle et al., 1980). This ethical tradition is context-dependent, contrasting with the abstract and universal nature of deontological ethics. It highlights individual responsibility and voluntary action, reinforcing the importance of personal accountability (Van Staveren, 2007).

Applying Ethical Traditions to Cybersecurity

The relevance and application of these ethical traditions in cybersecurity are complex, as their components align differently with various security contexts (Mersinas and Bada, 2023). For example, an individual can be both a target and an attack vector in cyber-attacks. Successful attacks not only affect systems but can also cascade to impact additional users. This interconnectedness underscores the importance of individual-level defenses.

Virtue ethics, in particular, resonate in such scenarios by emphasizing collective social responsibility and the common good through individual accountability. By incorporating elements of all three traditions, cybersecurity ethics can address the nuanced challenges of modern security contexts while fostering responsible behavior at both individual and systemic levels.

Ethics in Cybersecurity and Other Fields

Ethical considerations in cybersecurity are predominantly divided into two categories: ethics for research involving human subjects, such as the Menlo Report (Dittrich and Kenneally, 2012), and rights-based ethics (Loi and Christen, 2020). However, to date, there is no comparable framework specifically tailored to behavior change in cybersecurity (CBC).

To establish a robust set of ethical principles for CBC, we draw insights from ethics research in cybersecurity and other domains. For example, ethics in artificial intelligence (AI) and machine learning (ML) frequently use the principles of biomedical ethics—autonomy, beneficence, nonmaleficence, and justice—augmented by others such as transparency, responsibility, privacy, trust, sustainability, dignity, and solidarity (Floridi et al., 2018; Jobin et al., 2019). The prominence of AI ethics has resulted in several proposed frameworks (Hagendorff, 2020). Yet, despite this pool of ethical principles, CBC requires a focused and practical approach, selecting only the most essential principles for effective behavioral security interventions.

In cybersecurity, principles such as autonomy, beneficence/nonmaleficence, justice, privacy, trust, and equality have been identified from a business perspective (Yaghmaei et al., 2017). A systematic review by Morgan and Gordijn (2020) ranks commonly cited principles, including data protection, trust, control, accessibility, privacy, and accountability. However, these principles predominantly address business threats rather than the specific context of CBC. Research on Internet of Things (IoT) security has also highlighted principles like autonomy and privacy, though without adopting a principled approach (Atlam and Wills, 2020).

Ethics in healthcare cybersecurity provides a more relevant parallel to CBC, as healthcare technologies similarly target specific audiences, require privacy preservation, and aim to influence individual behavior (Weber and Kleine, 2020). In 1979, Beauchamp and Childress introduced the **Principles of Biomedical Ethics**—autonomy, beneficence, nonmaleficence, and justice—which have since been widely adopted in fields such as healthcare, medical AI, disaster management, and forensic science (Cuthbertson and Penney, 2023; Jahn, 2011). These principles are particularly relevant for CBC as they simplify ethical decision-making through a principled framework (Leikas et al., 2019). Moreover, their alignment with

human rights enhances their applicability, particularly for privacy-related considerations (Brännmark, 2017).

In healthcare cybersecurity, principles such as privacy-trust, freedom-consent, dignity-solidarity, and fairness-equality are suggested as complementary to the Beauchamp and Childress framework (Weber and Kleine, 2020). These principles reflect connections between individual rights and broader societal considerations, which align closely with the goals of CBC.

An Extended Set of Ethical Principles for Cybersecurity Behavior Change Interventions

We propose six ethical principles for CBC interventions: **autonomy, beneficence, nonmaleficence, justice, transparency, and privacy**. These principles form a practical framework for security professionals to address ethical dilemmas and implement behavioral interventions, particularly in organizational contexts. While additional principles could be considered, we argue that these six are the minimum essential for CBC.

Other principles, such as responsibility, trust, sustainability, dignity, and solidarity, are excluded for specific reasons. Responsibility is inherently tied to how security processes are implemented and overlaps with trust, as responsible users foster trust and operate effectively within trustworthy environments (Durojaiye et al., 2021). Similarly, dignity is partially encompassed within beneficence, nonmaleficence, and justice, with justice serving as a broader concept capturing aspects of responsibility, trust, and dignity while also fostering solidarity. Trust and sustainability, although relevant, pertain more to advanced stages of behavioral interventions. Trust involves confidence in technologies and systems, while sustainability addresses the long-term effects of interventions, such as user acceptance and habituation (Shipp et al., 2023).

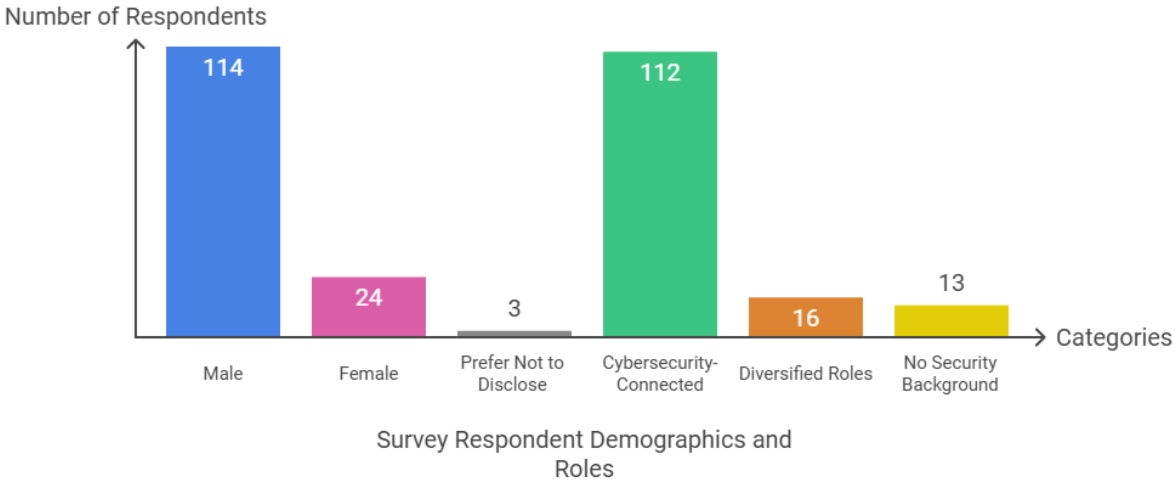
The inclusion of transparency, rather than explicability, reflects the need to address perceived hidden intentions behind interventions, a critical factor in establishing digital trust (Shipp et al., 2023). Transparency focuses on the clarity of intentions and actions, which is crucial during the initial stages of CBC.

Application of the Principles

The proposed principles—autonomy, beneficence, nonmaleficence, justice, transparency, and privacy—are intended to guide security professionals in identifying ethical considerations and resolving dilemmas in CBC. While inspired by the original principles of Beauchamp and Childress (1989), they are adapted for CBC to reflect its unique challenges. These principles offer a practical framework for designing and analyzing interventions that aim to influence individual security behaviors.

Rather than serving as rigid tools for complex decision-making, these principles provide a conceptual framework to address ethical issues systematically. They represent clusters of ideas that security professionals can use to develop, implement, and assess CBC interventions while fostering ethical, responsible, and user-centered practices.

To assess perceptions of the proposed ethical principles, we developed a survey. We enhanced the clarity of the questions and refined them with input from a pilot study conducted among security professionals. The survey was disseminated via LinkedIn from July 8, 2022, to February 19, 2023, leveraging a convenience sampling method. This approach was selected due to the authors' combined pool of over 6,000 LinkedIn connections, most of whom are cybersecurity professionals. Participants were asked to provide feedback on the need for ethical frameworks in cybersecurity, particularly in relation to behavior change interventions (CBC). Multiple-choice answers were adapted from prior reputable surveys, including those conducted by ENISA, the UK Department of Culture, Media, and Sport, Ipsos Mori, and others. Open-ended responses were also encouraged via an "Other" option for participants to elaborate.



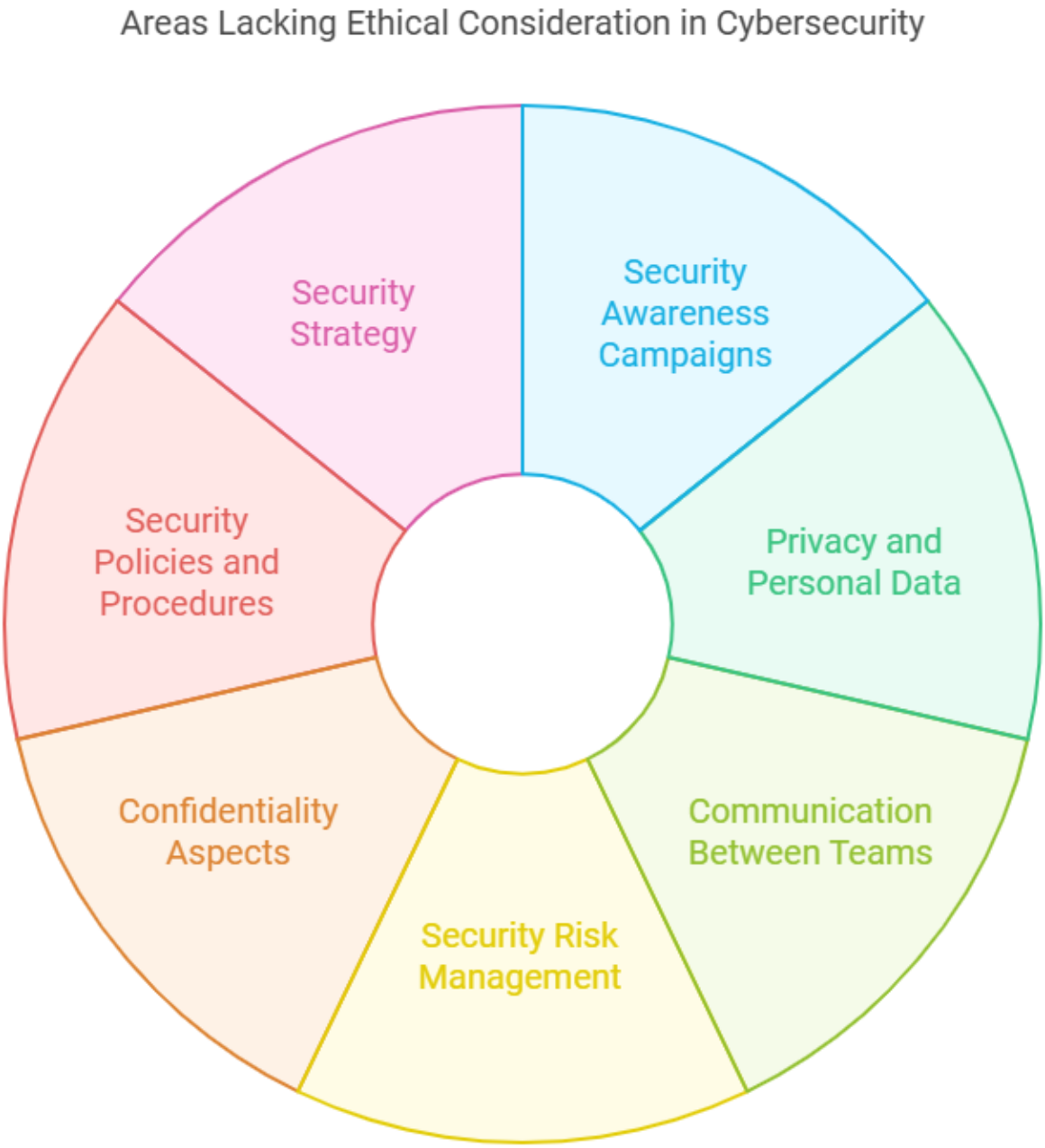
Respondent Demographics and Roles

The survey recorded 141 non-empty responses, with 114 male participants, 24 female participants, and 3 preferring not to disclose their gender. Of the total respondents, 112 (80%) were directly or indirectly connected to cybersecurity, 16 (11%) had diversified roles (e.g., in defense), and 13 (9%) had no explicit security background. No participants were excluded. The majority of respondents (68%) fell within the 31–40 (33%) and 41–50 (35%) age groups, with an average of 14.5 years of security experience (M = 14.41, SD = 9.37). Participants' professional roles are illustrated in Figure 1.

Key Results

A significant majority (82%) of participants expressed that ethical frameworks are either needed (40%) or somewhat needed (42%) in cybersecurity behavior change. Responses to the question, "In which area(s) of cybersecurity are ethical principles currently not being considered?" were distributed across all categories, ranging from 12% to 17% (multiple selections allowed). These categories included:

- Security awareness campaigns
- Privacy and personal data
- Communication between senior management and other teams
- Security risk management
- Confidentiality aspects
- Security policies and procedures
- Security strategy

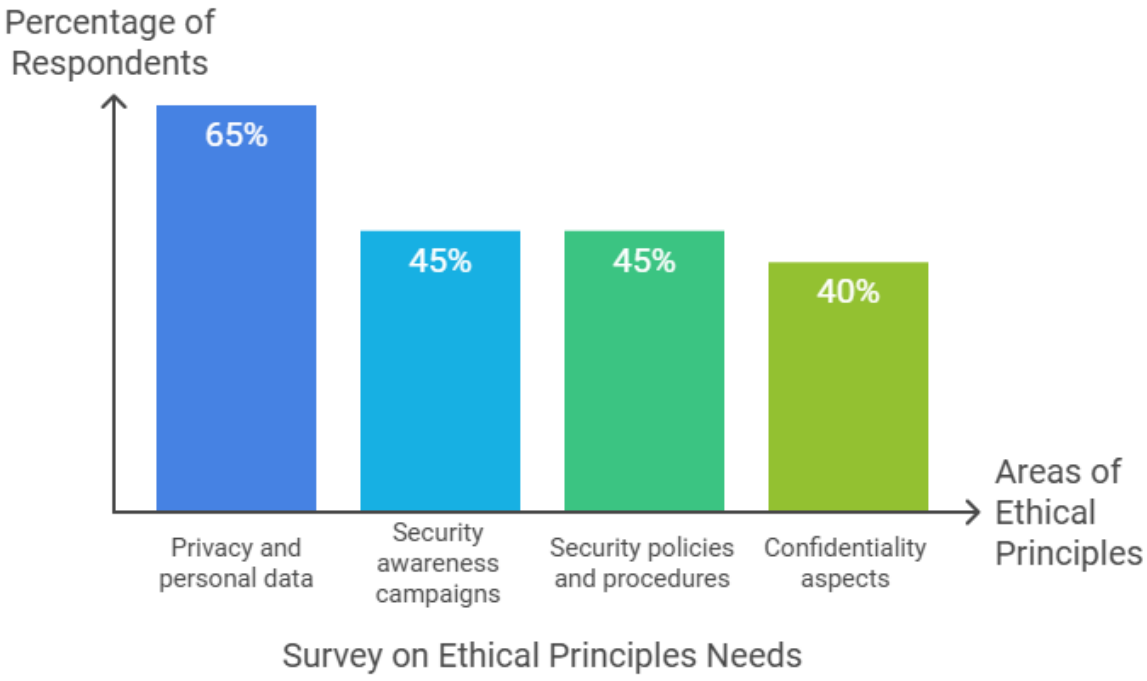


This distribution indicates a broad perception that ethical principles are largely absent across the cybersecurity domain.

When asked about areas where ethical principles are most needed, the top responses were:

1. Privacy and personal data (65%)

2. Security awareness campaigns (45%)
3. Security policies and procedures (45%)
4. Confidentiality aspects (40%)



The area considered least in need was security risk management (31%).

Regarding the question, “What would you like to see in security behavior change and ethics?”, the most common responses were:

- Senior management involvement in behavior change and ethics (23%)
- End-user involvement (22%)

Concerns cited by participants included:

- End-users prioritizing other concerns (27%)
- Senior management prioritizing other concerns (26%)
  The least-cited concern was the immaturity of the cybersecurity field (8%), while only 2% of participants reported no concerns.

Principles and Their Importance

Participants were introduced to the six ethical principles for CBC interventions:

1. Autonomy: Individuals are free to accept or reject the intervention.
2. Beneficence and Nonmaleficence: Interventions should benefit individuals and avoid harm.
3. Justice: Individuals are supported based on their culture, digital literacy, and skillset.
4. Transparency: The intentions behind interventions are clear to users.
5. Privacy: Individuals have control over personal data and cannot be easily identified.

When asked which principles are useful or needed, Autonomy was rated the least useful, with 52% of participants stating it was not needed. In contrast, disagreement for the other principles was minimal:

- Beneficence and Nonmaleficence: 6% disagreement.
- Justice: 6% disagreement.
- Privacy: 2% disagreement.
- Transparency: No disagreement.

Participants ranked the principles by importance:

1. Transparency (most important; M = 2.36, SD = 1.13).
2. Beneficence and Nonmaleficence (M = 2.61, SD = 1.32).
3. Privacy (M = 2.70, SD = 1.34).
4. Justice.

Autonomy (least important).

Interestingly, 51% of participants disagreed, and 29% somewhat disagreed, with the statement, “Users should be free to accept or reject security practices,” further confirming the lower importance of Autonomy.

Participant Suggestions

In response to the question, “Is there any other ethical principle or consideration you would like to propose or mention?”, several notable suggestions emerged, including:

- Improved training at all levels, emphasizing accessibility and tailoring to end-user needs, particularly in areas with limited digital literacy and resources.
- Alignment of corporate missions with personal goals.
- Inclusion of aspects related to biometrics and artificial intelligence.

These insights underscore the need for ethical frameworks that are inclusive, practical, and adaptable to diverse user needs.

Conclusion

This research explored the efficacy of behavioral biometrics as an innovative approach to enhancing cybersecurity. By focusing on the unique patterns of user behavior, such as typing speed, mouse movements, and gait, behavioral biometrics offers an added layer of security that is both seamless and effective in detecting unauthorized access and potential threats. Our findings suggest that behavioral biometrics can significantly improve security systems, particularly in environments where traditional methods such as passwords and PINs are vulnerable to compromise.

However, while the technology shows promise, challenges remain in its widespread implementation, particularly in ensuring accuracy, mitigating false positives, and addressing privacy concerns. Behavioral biometrics also require continuous adaptation and learning to keep pace with evolving threats.

Furthermore, integrating behavioral biometrics with existing security frameworks can offer a more robust and multi-layered defense strategy, enhancing both user authentication and overall cybersecurity. For the full potential of behavioral biometrics to be realized, future research should focus on refining the technology, addressing ethical concerns, and evaluating its real-world applicability across different sectors.

In conclusion, behavioral biometrics represents a significant advancement in cybersecurity, offering a novel way to secure systems and protect users. Its potential to improve authentication processes, alongside traditional security measures, could play a crucial role in defending against increasingly sophisticated cyber threats.

1. References

2. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40–46.
3. Ajzen, I. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs.
4. Alnifie, K. M., & Kim, C. (2023). Appraising the manifestation of optimism bias and its impact on human perception of cybersecurity: A meta-analysis. *Journal of Information Security*, *14*(2), 93–110.
5. Ariely, D. (2008). *Predictably irrational: The hidden forces that shape our decisions*. New York.
6. Aristotle, J. O., Urmson, J. L., & Ackrill, J. (1983). *Nicomachean ethics*. In W. D. Ross, J. O. Urmson, & J. L. Ackrill (Eds.), Oxford University Press (pp. 123–149).

7. Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety, and ethics. *Digital Twin Technology for Smart Cities*, 123–149.
8. Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cybersecurity awareness campaigns: Why do they fail to change behavior? In *International Conference on Cyber Security for Sustainable Society*.
9. BCS. (2024). *Code of conduct*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ (Accessed: 12 June 2024).
10. Beauchamp, T. L., & Childress, J. F. (1989). *Principles of biomedical ethics*. Oxford.
11. Bednar, K., & Spiekermann-Hoff, S. (2020). The power to design: Exploring utilitarianism, deontology, and virtue ethics in three technology case studies. In *ETHICOMP 2020* (p. 396).
12. Bentham, J. (1876). *An introduction to the principles of morals and legislation*. Clarendon Press.
13. Brännmark, J. (2017). Respect for persons in bioethics: Towards a human rights-based account. *Human Rights Review, 18*(2), 171–187.
14. Briggs, P., Jeske, D., & Coventry, L. (2017). Behavior change interventions for cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behavior Change Research and Theory* (pp. 115–136). Elsevier.
15. Camerer, C. (2003). *Behavioral game theory: Experiments in strategic interaction*. New York.
16. Camerer, C. F. (2004). Prospect theory in the wild: Evidence from the field. In C. F. Camerer, G. Loewenstein, & M. Rabin (Eds.), *Advances in behavioral economics* (pp. 148–161). Princeton & Oxford.
17. Canca, C. (2020). Operationalizing AI ethics principles. *Communications of the ACM, 63*(12), 18–21.
18. Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *CHI 2019*.
19. Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security, 97*, 101963.
20. Cisco. (2017). *Annual cybersecurity report*.
21. Coventry, L., Briggs, P., Jeske, D., & van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cybersecurity environment. In A. Marcus (Ed.), *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience* (pp. 229–239).
22. Craggs, B., & Rashid, A. (2017). Smart cyber-physical systems: Beyond usable security to security ergonomics by design. In *Proceedings of the 3rd International Workshop on Software Engineering for Smart Cyber-Physical Systems* (pp. 22–25). IEEE Press.
23. Craggs, B. (2019). A just culture is fundamental: Extending security ergonomics by design. In *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)* (pp. 46–49).
24. CREST. (2024). *Code of ethics*. Available at: https://www.crest-approved.org/about-us/code-of-ethics/ (Accessed: 12 June 2024).

25. Cuthbertson, J., & Penney, G. (2023). Ethical decision making in disaster and emergency management: A systematic review of the literature. *Prehospital and Disaster Medicine*, 1–6.
26. de Bruin, M., & Mersinas, K. (2024). Individual and contextual variables of cybersecurity behavior: An empirical analysis of national culture, industry, organization, and individual variables of (in)secure human behavior. *arXiv preprint*. https://arxiv.org/pdf/2405.16215.
27. Dekker, S. (2018). *Just culture: Restoring trust and accountability in your organization*. CRC Press.
28. Dhingra, N., Gorn, Z., Kener, A., & Dana, J. (2012). The default pull: An experimental demonstration of subtle default effects on preferences. *Judgment and Decision Making*, *7*(1), 69–76.

29. Bowers, K. D. (2009). *High Availability and Integrity Layer (HAIL): A High Availability and Integrity Management for Cloud Services*. International Journal of Cloud Computing and Services Science, 2(2), 45-56.

30. Gerges, M., Elgalb, A., & Freek, A. (2024). Concealed Object Detection and Localization in Millimetre Wave Passengers' Scans. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(4), 372-382.
31. Ahmed, E., & Abdelrahman, F. (2024). Harnessing Machine Learning for Real-Time Cybersecurity: A Scalable Approach Using Big Data Frameworks. *Emerging Engineering and Mathematics*, 01-09.

32. Alesiani, F., & Poli, D. (2018). *Cloud Computing Security Issues and Challenges: A Survey*. International Journal of Computer Science and Information Security, 16(5), 67-74.

33. Ahmed, E. (2024). Accelerating Drug Discovery Pipelines with Big Data and Distributed Computing: Applications in Precision Medicine. *Emerging Medicine and Public Health*, 1-7.

34. Zolotan, M., & Ross, A. (2016). *Intrusion Detection Systems in Cloud Computing: A Survey*. International Journal of Computer Applications, 143(10), 1-5. https://doi.org/10.5120/ijca2016907015

35. Guo, W., & Wang, Y. (2017). *Intrusion Detection for Cloud Computing Using Machine Learning*. Proceedings of the 2nd International Conference on Cloud Computing and Security, 203-210. https://doi.org/10.1109/CCS.2017.8239681

36. Zhang, Y., & Zhang, J. (2019). *A Comparative Study of Machine Learning Algorithms for Intrusion Detection in Cloud Computing Environments*. Journal of Cloud Computing: Advances, Systems, and Applications, 8(1), 22-35. https://doi.org/10.1186/s13677-019-0154-3

37. Nakamura, M., & Fujii, H. (2020). *Security Challenges and Solutions in Multi-Cloud Computing: A Case Study Using Machine Learning*. IEEE Transactions on Cloud Computing, 8(2), 430-440. https://doi.org/10.1109/TCC.2020.2973563

38. Rani, S., & Sharma, M. (2021). *Cloud Intrusion Detection Systems: A Review of Machine Learning Approaches*. International Journal of Cloud Computing and Services Science, 9(4), 68-76. https://doi.org/10.14419/ijccs.9.4.38525

39. Ahmed, E., & Maher, G. (2024). Optimizing Supply Chain Logistics with Big Data and AI: Applications for Reducing Food Waste. *Journal of Current Science and Research Review*, *2*(02), 29-39.

40. Gerges, M., & Elgalb, A. (2024). Comprehensive Comparative Analysis of Mobile Apps Development Approaches. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *6*(1), 430-437.