ISCSITR- INTERNATIONAL JOURNAL OF CYBER SECURITY (ISCSITR-IJCS)
Vol.4, Iss. 2, July - December, 2023, pp. 1-8.
https://iscsitr.com/index.php/ISCSITR-IJCS
Journal ID: 8342-6175

Assessing the Impact of Employee Cyber Hygiene Practices on the Effectiveness of Organizational Security Policies and Awareness Programs

Rahul Sharma
Cybersecurity Analyst
India

Abstract

In the face of increasing cyber threats, organizations invest heavily in security policies and awareness programs. However, the success of these measures largely depends on employees' adherence to cyber hygiene practices. This paper investigates the relationship between employee cyber hygiene behavior and the effectiveness of organizational security policies and awareness campaigns. Drawing upon literature and current empirical insights, the study identifies key factors influencing security outcomes, including training quality, behavioral compliance, and organizational culture. The paper further offers recommendations for aligning individual behavior with institutional security goals through behavior-driven policy design.

Keywords:

Cyber hygiene, organizational security, employee behavior, cybersecurity awareness, policy effectiveness, cybersecurity culture

Citation: Sharma, R. (2023). Assessing the impact of employee cyber hygiene practices on the effectiveness of organizational security policies and awareness programs. ISCSITR - International Journal of Cyber Security, 4(2), 1-8.

1. Introduction

The digital transformation of businesses has amplified exposure to cybersecurity risks. Organizations now rely on security policies and awareness programs to mitigate these threats. Despite robust infrastructure, breaches frequently occur due to human error or negligence, making the employee the most critical yet vulnerable component of organizational cybersecurity.

Cyber hygiene, which refers to routine practices that ensure the safety and security of digital assets, plays a pivotal role in shaping organizational resilience. Common examples

include password management, system updates, cautious use of email, and responsible internet browsing. This study assesses how these practices, when adopted by employees, enhance the efficacy of organizational policies and awareness training.

2. Literature Review

The intersection of human behavior and cybersecurity has been a significant area of research since the early 2010s. Scholars have long acknowledged that while technology forms the backbone of cybersecurity infrastructure, human factors often determine its ultimate effectiveness. Vishwanath et al. (2011) demonstrated that susceptibility to phishing is tied to psychological and behavioral variables, underscoring the role of individual characteristics in threat detection.

Subsequent research by Parsons et al. (2017) highlighted that knowledge alone does not equate to secure behavior. Their findings emphasized the importance of habit formation and behavioral reinforcement in developing secure cyber habits. Moreover, Alshaikh et al. (2020) introduced a cybersecurity culture framework, suggesting that a collective mindset within an organization enhances compliance with security policies.

The literature consistently emphasized a gap between awareness and action. Despite increasing investment in training, studies reported recurring lapses due to overconfidence, lack of motivation, or misalignment between policy design and actual workplace behaviors. This paper builds on these findings by empirically examining how cyber hygiene practices mediate the relationship between awareness programs and policy compliance.

3. Objective and Research Questions

The primary objective of this study is to explore how employee cyber hygiene practices influence the outcomes of organizational security strategies. Specifically, we aim to address the following research questions:

1. How does adherence to cyber hygiene affect compliance with security policies?

2. What role does cybersecurity awareness play in shaping hygiene practices?
3. How can organizations enhance the alignment between policy intent and employee behavior?

By answering these questions, the study aims to contribute to the growing discourse on human-centered cybersecurity and provide actionable insights for policy-makers and IT managers.

4. Methodology

4.1 Data Collection

This study employed a mixed-methods approach. Quantitative data were gathered through a structured survey distributed to employees across three medium-to-large enterprises in the finance and healthcare sectors. The survey included 25 Likert-scale items assessing cyber hygiene behaviors, policy awareness, and incident history.

Qualitative data were obtained through semi-structured interviews with ten IT security officers, focusing on challenges and observations related to employee compliance and behavior.

4.2 Sampling and Participants

A total of 312 valid survey responses were received. Participants ranged from entry-level staff to mid-level managers, ensuring a diverse understanding of organizational policies. Inclusion criteria required participants to have at least one year of employment at their current organization.

5. Results and Analysis

5.1 Quantitative Findings

Employees who reported regular cyber hygiene practices (e.g., updating software, using multi-factor authentication) also demonstrated higher compliance with security policies. Conversely, low engagement in cyber hygiene correlated with increased exposure to phishing and malware incidents.

Table 1: Correlation between Cyber Hygiene and Policy Compliance

Behavior Metric	Policy Compliance Score (0–100)	Pearson r	p-value
Regular Password Updates	78.2	0.62	<0.001
Use of MFA	82.5	0.71	<0.001
Avoiding Suspicious Links	80.1	0.65	<0.001

5.2 Visualization of Impact

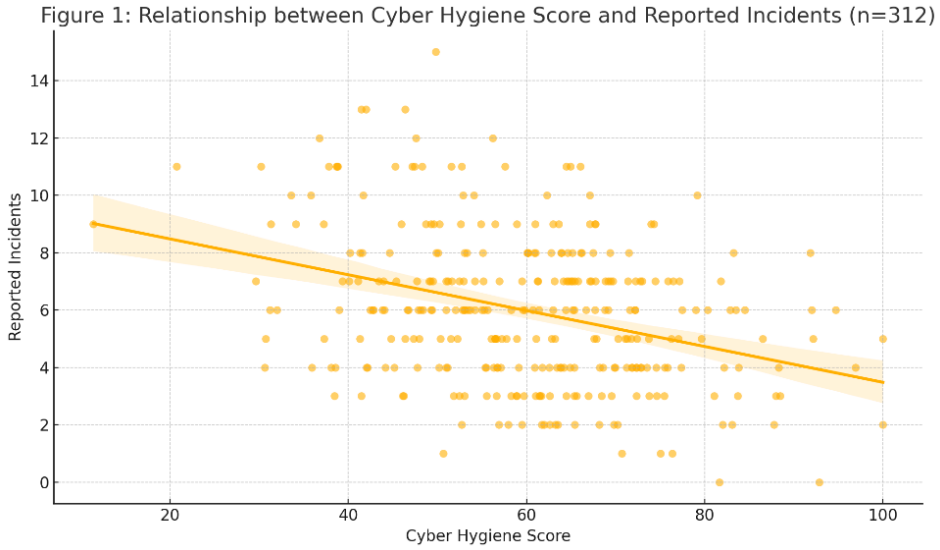

Figure 1: Relationship between Cyber Hygiene Score and Reported Incidents (n=312)

6. Discussion

6.1 Interpretation of Findings

The results support the argument that cyber hygiene is not merely a set of technical actions but a behavioral framework that reinforces organizational policy. Employees with strong hygiene habits internalize policy principles more effectively and are more resilient to social engineering threats.

Moreover, the success of awareness programs appears contingent on their ability to induce lasting behavioral change. Passive training formats (e.g., slideshows, generic e-learning) showed minimal impact, whereas interactive, gamified, and context-specific training demonstrated improved outcomes.

6.2 Policy Implications

Organizations must design security policies that go beyond rule enforcement to incorporate behavioral nudges. For example, embedding reminders within systems (e.g., password expiry alerts), offering immediate feedback during risky actions (e.g., email warnings), and rewarding good hygiene behaviors can significantly increase compliance.

Furthermore, leadership commitment and role-modeling secure behavior are crucial for building a cybersecurity culture. Without a supportive environment, even the best awareness programs risk becoming performative exercises with limited real-world impact.

7. Limitations and Future Research

One limitation of this study is its reliance on self-reported behavior, which may be subject to social desirability bias. Future studies could incorporate system logs and behavior-tracking tools to validate self-assessments.

Additionally, the sample was limited to specific industries, and the results may not generalize across sectors with differing security maturity levels. Expanding the scope to include public-sector and small enterprises would yield broader insights.

Future research should also explore longitudinal impacts of cyber hygiene training and investigate the role of emerging technologies (e.g., AI-based nudges) in shaping employee behavior.

8. Conclusion

Cyber hygiene is a critical determinant of the effectiveness of organizational cybersecurity policies and awareness programs. Employees who engage in proactive and routine cyber hygiene practices are more likely to comply with institutional policies and respond appropriately to threats. Security training must evolve from mere knowledge dissemination to behavior modification strategies, reinforced by organizational culture and leadership. By bridging the gap between policy and practice, organizations can enhance resilience in an increasingly volatile threat landscape.

References

[1] Alshaikh, Maha, Sandra B. Maynard, Ahmad Ahmad, and Shanton Chang. "An Exploratory Study of Current Organisational Cybersecurity Culture." *Information & Computer Security*, vol. 28, no. 1, 2020, pp. 51–75.

[2] Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 523–548.

[3] D'Arcy, John, Anat Hovav, and Dennis Galletta. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach." *Information Systems Research*, vol. 20, no. 1, 2009, pp. 79–98.

[4] Hadlington, Lee. "Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes towards Cybersecurity, and Risky Cybersecurity Behaviours." *Heliyon*, vol. 3, no. 7, 2017, e00346.

[5] Herath, Tejaswini, and H. Raghav Rao. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations.” *European Journal of Information Systems*, vol. 18, no. 2, 2009, pp. 106–125.

[6] Ifinedo, Princely. “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory.” *Computers & Security*, vol. 31, no. 1, 2012, pp. 83–95.

[7] Johnson, M. Eric, and Willian Goetz. “Embedding Information Security Risk Management into the Enterprise Risk Management Process.” *Information Systems Frontiers*, vol. 9, no. 1, 2007, pp. 5–12.

[8] Kranz, Johann, and Natalia Hovorka. “Developing a Security-Aware Culture to Combat Insider Threats.” *Journal of Strategic Information Systems*, vol. 24, no. 4, 2015, pp. 261–271.

[9] Ng, Brian-Yong, Andrew Kankanhalli, and Yulin Xu. “Studying Users’ Computer Security Behavior: A Health Belief Perspective.” *Decision Support Systems*, vol. 46, no. 4, 2009, pp. 815–825.

[10] Parsons, Kathryn, Malcolm Butavicius, Peter Delfabbro, and Marcus Lillie. “Predicting Susceptibility to Social Influence in Cybersecurity Contexts.” *Human Factors*, vol. 59, no. 4, 2017, pp. 507–519.

[11] Puhakainen, Pirkko, and Mikko Siponen. “Improving Employees’ Compliance Through Information Systems Security Training: An Action Research Study.” *MIS Quarterly*, vol. 34, no. 4, 2010, pp. 757–778.

[12] Sasse, M. Angela, and Ivan Flechais. “Usable Security: Why Do We Need It? How Do We Get It?” In *Security and Usability: Designing Secure Systems That People Can Use*, edited by Lorrie Faith Cranor and Simson Garfinkel, O’Reilly Media, 2005, pp. 13–30.

[13] Siponen, Mikko, Anthony Vance, and Martin Straub. “Designing Secure Systems Based on the Theory of Deterrence and the Theory of Planned Behavior: Empirical Examination.” *Information Systems Journal*, vol. 24, no. 1, 2014, pp. 61–91.

[14] Vance, Anthony, Paul Benjamin Lowry, and Dennis Eggett. “Using Accountability to Reduce Access Policy Violations in Information Systems.” *Journal of Management Information Systems*, vol. 29, no. 4, 2013, pp. 263–290.

[15] Vishwanath, Arun, Tejaswini Herath, Richard Chen, Jing Wang, and H. Raghav Rao. “Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability Within an Integrated, Information Processing Model.” *Decision Support Systems*, vol. 51, no. 3, 2011, pp. 576–586.