International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

Cyber Security Awareness and Employee Compliance Behavior

[1]Gade Venumadhav [2]Aseenababu Shaik* [3]Pavani Mudem

[1]PG Student, Department of MBA, Samskruti College of Engineering & Technology, Telangana-501301

[1]Email : gvenumadhav143@gmail.com

[2]Department of Computer Science and Engineering(AI&ML), Samskruti College of Engineering & Technology, Telangana-501301*

[2]Email: doctoraseen@gmail.com*

[3]Department of MBA, Samskruti College of Engineering & Technology, Telangana-501301

[3]Email: drpavanikaran12@gmail.com

Abstract

Cybersecurity has become one of the most critical concerns for organizations as digital transformation, cloud computing, remote work, and internet-based business operations continue to expand globally. Despite significant investments in advanced security technologies, human error remains one of the leading causes of cybersecurity incidents, making employee awareness and compliance with organizational security policies essential for protecting information assets. Cybersecurity awareness refers to the knowledge and understanding employees possess regarding cyber threats, safe online practices, organizational security policies, and responsible digital behavior. Employee compliance behavior involves the extent to which employees follow established cybersecurity guidelines such as creating strong passwords, enabling multi-factor authentication, identifying phishing emails, handling sensitive information securely, updating software regularly, and reporting suspicious activities promptly. Organizations increasingly implement cybersecurity awareness training, simulated phishing exercises, security awareness campaigns, and policy enforcement programs to reduce cyber risks and strengthen organizational resilience. The primary objective of this study is to examine the relationship between cybersecurity awareness and employee compliance behavior by evaluating how awareness programs influence employees' adherence to cybersecurity policies and best practices. The research also investigates the effectiveness of cybersecurity training, password management practices, phishing awareness, and organizational security culture in improving compliance behavior. A descriptive research design was adopted for the study. Primary information was obtained through structured responses collected from employees, while secondary information was gathered from peer-reviewed journals, books, industry reports, government publications, and authentic cybersecurity databases. Percentage analysis and graphical techniques were employed to analyze and interpret the collected information. The findings indicate that higher cybersecurity awareness significantly improves employee compliance with organizational security policies, reduces risky online behavior, enhances phishing detection capabilities, and minimizes the likelihood of cyber incidents. However, challenges such as insufficient training, employee negligence, lack of continuous awareness programs, and evolving cyber threats continue to affect organizational cybersecurity. The study concludes that continuous cybersecurity education, regular policy updates, practical security training, and a strong security culture are essential for improving employee compliance behavior and strengthening organizational cybersecurity resilience.

Keywords: Cybersecurity Awareness, Employee Compliance, Information Security, Cyber Threats, Phishing, Password Security, Multi-Factor Authentication.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

I. INTRODUCTION

The rapid growth of digital technologies, cloud computing, artificial intelligence, remote working environments, and internet-based communication has significantly increased organizations' dependence on information systems while simultaneously exposing them to a wide range of cybersecurity threats [1]. Cyberattacks such as phishing, ransomware, malware, social engineering, insider threats, and data breaches have become more sophisticated, causing substantial financial losses, operational disruptions, and reputational damage to organizations worldwide [2]. Although organizations invest heavily in advanced cybersecurity technologies including firewalls, intrusion detection systems, endpoint protection, encryption, and artificial intelligence-based security solutions, human error continues to be one of the leading causes of cybersecurity incidents [3]. Employees frequently become targets of cybercriminals through phishing emails, fraudulent websites, malicious attachments, weak password practices, unauthorized software installations, and improper handling of sensitive organizational information [4]. Consequently, cybersecurity awareness has emerged as a critical component of organizational security strategies, focusing on educating employees about cyber risks, safe computing practices, and compliance with security policies [5]. Cybersecurity awareness enables employees to recognize potential threats, respond appropriately to suspicious activities, protect confidential information, and contribute to a secure organizational environment [6]. Employee compliance behavior refers to the extent to which individuals consistently follow organizational cybersecurity policies, including creating strong passwords, enabling multi-factor authentication, updating software regularly, reporting security incidents promptly, avoiding suspicious links, and complying with information security guidelines [7]. Organizations increasingly implement cybersecurity awareness training programs, simulated phishing campaigns, security workshops, online learning modules, and continuous awareness initiatives to improve employees' cybersecurity knowledge and encourage secure behavior [8]. Research indicates that employees who receive regular cybersecurity education demonstrate higher levels of policy compliance, improved phishing detection capabilities, stronger password management practices, and greater responsibility toward protecting organizational assets [9]. Furthermore, creating a positive cybersecurity culture through management support, continuous communication, employee participation, and clear security policies enhances compliance behavior and reduces organizational cyber risks [10]. However, rapidly evolving cyber threats, increasing digital dependence, hybrid work environments, and sophisticated social engineering attacks require organizations to continuously update awareness programs and strengthen employee engagement [11]. Advances in artificial intelligence, machine learning, behavioral analytics, and threat intelligence have further improved cybersecurity monitoring and employee risk assessment, enabling organizations to identify vulnerabilities and provide targeted awareness training [12]. Regulatory frameworks and international cybersecurity standards also emphasize employee awareness and compliance as essential components of effective information security management systems [13]. Therefore, understanding the relationship between cybersecurity awareness and employee compliance behavior is essential for developing effective organizational security strategies, reducing cybersecurity risks, improving regulatory compliance, and enhancing overall organizational resilience against evolving cyber threats [14], [15].

Research Objectives

The primary objective of this study is to examine the relationship between cybersecurity awareness and employee compliance behavior within organizations. The study aims to evaluate how cybersecurity awareness programs influence employees' adherence to organizational security policies and safe digital practices. It

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

further seeks to analyze employee knowledge regarding phishing attacks, password security, multi-factor authentication, secure internet usage, data protection, and incident reporting. The research also evaluates the effectiveness of cybersecurity training programs in improving compliance behavior, identifies the major factors affecting employee adherence to cybersecurity policies, examines the role of organizational security culture in promoting secure behavior, and provides recommendations for strengthening employee awareness, reducing cybersecurity risks, and improving overall organizational information security.

Research Methodology

The present study adopts a descriptive research design to examine the relationship between cybersecurity awareness and employee compliance behavior in organizational environments. Both primary and secondary sources of information were utilized to achieve the research objectives. Primary information was collected from employees across different organizations using a structured survey designed to evaluate cybersecurity awareness, security practices, policy compliance, phishing awareness, password management, and incident reporting behavior. Secondary information was obtained from peer-reviewed journals, books, government publications, cybersecurity reports, industry white papers, and authentic online databases related to information security and cyber risk management. The collected information was analyzed using percentage analysis and presented through bar graphs and a line graph to facilitate systematic interpretation. The study focused on variables such as cybersecurity awareness levels, employee compliance with security policies, participation in awareness training, password management practices, phishing identification ability, and overall organizational security behavior. The findings were interpreted to assess the effectiveness of cybersecurity awareness initiatives and to provide practical recommendations for improving employee compliance and strengthening organizational cybersecurity resilience.

II. REVIEW OF LITERATURE

Siponen, Pahnila, and Mahmood (2010) examined employee compliance with information security policies and investigated the factors influencing employees' willingness to follow organizational security rules. The study emphasized that careless employee behavior and failure to comply with security policies can expose organizations to significant information-security risks. The authors examined motivational factors associated with compliance and highlighted the importance of creating organizational conditions that encourage employees to follow security policies. The study provides an important foundation for understanding the relationship between employee behavior and organizational information security.

Siponen and Vance (2010) investigated why employees violate information-security policies using neutralization theory. The study argued that employees may rationalize policy violations through techniques that allow them to justify insecure behavior. The empirical findings showed that neutralization is an important factor in explaining employee security-policy violations. The research suggests that organizations should not depend solely on sanctions and formal policies; they should also address the attitudes and rationalizations that influence employees' cybersecurity behavior.

Herath and Rao (2009) examined employee intentions to comply with information-security policies by integrating deterrence theory and social influence theory. The study investigated how perceived threats, organizational expectations, rewards, and sanctions influence employees' intentions to comply with security requirements. The findings indicated that both organizational factors and individual perceptions play an important role in determining compliance behavior. The study highlights that effective information-security management requires a combination of awareness, organizational support, and appropriate motivational mechanisms.

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

Bulgurcu, Cavusoglu, and Benbasat (2010) investigated the determinants of information-security policy compliance using the Theory of Planned Behavior. The researchers proposed that employees' attitudes, beliefs, perceived responsibility, and knowledge about security policies influence their intention to comply. The study emphasized the importance of employees' perceived benefits and costs of compliance as well as their awareness of organizational security requirements. The findings suggest that organizations can improve compliance by increasing employees' security knowledge and creating positive attitudes toward information-security policies.

Li, He, Xu, Ash, Anwar, and Yuan (2019) investigated the impact of cybersecurity policy awareness on employees' cybersecurity behavior. The researchers collected survey data from 579 business managers and professionals and used structural equation modelling and ANOVA. The findings showed that employees who were aware of their organization's information-security policies and procedures were more capable of managing cybersecurity tasks. The study also found that the organizational security environment influences employees' threat and coping assessments, which subsequently contribute to cybersecurity compliance behavior.

Lebek, Uffen, Neumann, Hohler, and Breitner (2014) conducted a theory-based literature review of employee information-security awareness and behavior. The researchers reviewed 113 publications and examined the theories used to explain employees' information-security behavior. The study identified several cognitive and behavioral determinants of secure employee behavior and developed a meta-model integrating important constructs from existing theories. The research demonstrated that cybersecurity behavior is influenced by multiple psychological, organizational, and technological factors rather than awareness alone.

Haney and Lutters (2020) examined the effectiveness of security awareness training in the workplace and questioned whether organizations should consider training completion as sufficient evidence of secure employee behavior. The authors argued that awareness and training have different purposes: awareness aims to influence attitudes, while training provides employees with skills and tools to practice secure behavior. The study emphasized that organizations should move beyond "check-the-box" compliance and evaluate whether security training actually produces long-term behavioral change.

Prümmer and van Steen (2024) conducted a systematic review of cybersecurity training methods and their effectiveness in improving organizational cybersecurity behavior. The researchers screened more than 16,000 publications and included 142 relevant studies in the final analysis. The review found that most studies reported positive effects of cybersecurity training, with game-based training being particularly common. However, many studies used small samples and non-experimental designs, while relatively few directly measured long-term employee behavior. The study concluded that cybersecurity training generally improves security-related knowledge and behavior, but stronger evaluation methods are needed.

Prümmer and colleagues (2025) A 2025 meta-analysis examined the overall effectiveness of cybersecurity training on end-user behavior. The researchers analyzed 69 eligible studies and found that cybersecurity training had a positive overall effect on end-users, particularly on knowledge and security-related attitudes. However, the effect on actual behavioral change was considerably weaker. The findings suggest that simply increasing cybersecurity awareness does not necessarily guarantee that employees will consistently follow secure practices. Organizations therefore need continuous, practical, and behavior-focused interventions rather than relying exclusively on traditional awareness programs.

Sutton and Tompson (2025) conducted a rapid evidence review examining the relationship between organizational cybersecurity culture and employee cybersecurity behavior. The review analyzed 59 studies and identified employee attitudes,

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

security-policy compliance, security education and training, behavioral monitoring, and top-management commitment as important dimensions of cybersecurity culture. The study concluded that cybersecurity should be viewed not only as a technical issue but also as an organizational and management responsibility. A strong cybersecurity culture requires management support and shared employee understanding that encourages secure behavior and policy compliance.

III. DATA ANALYSIS & INTERPRETATION

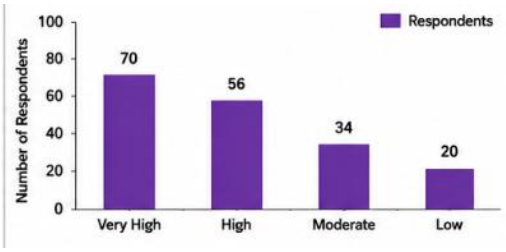

Fig 1:Employee Cybersecurity Awareness Level

Figure 1 The graph indicates that 38.9% of respondents have a very high level of cybersecurity awareness, while 31.1% reported a high level of awareness. About 18.9% demonstrated moderate awareness, and 11.1% had low awareness.

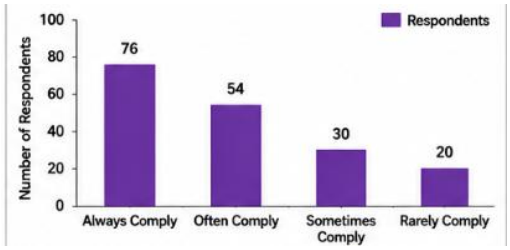

Fig 2:Compliance with Organizational Cybersecurity Policies

Figure 2 The graph shows that 42.2% of employees always comply with organizational cybersecurity policies, while 30.0% often follow the prescribed security guidelines.

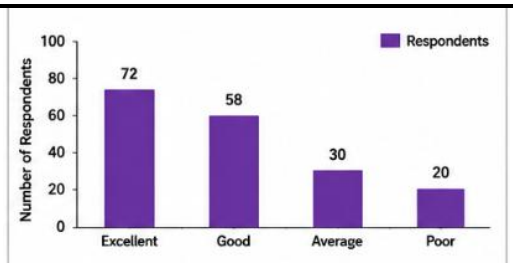

Fig 3: Password Security Practices

Figure 3 The graph reveals that 72.2% of respondents maintain good or excellent password security practices, such as using strong passwords, changing passwords regularly, and enabling multi-factor authentication.

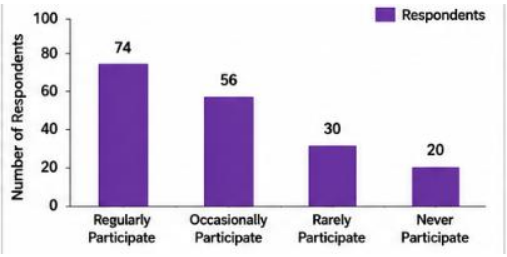

Fig 4: Participation in Cybersecurity Awareness Training

Figure 4 The graph indicates that 41.1% of employees regularly participate in cybersecurity awareness training, while 31.1% attend training occasionally.

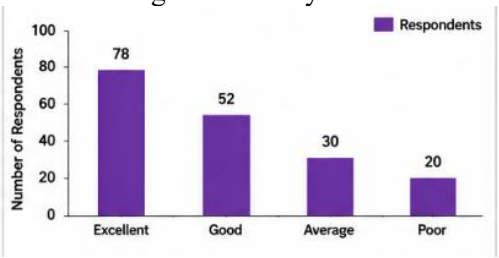

Fig 5: Ability to Identify Phishing Emails

Figure 5 The graph shows that 43.3% of respondents possess excellent phishing identification skills, while **28.9%** demonstrate good ability.

Fig 6: Overall Cybersecurity Awareness and Employee Compliance

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

Figure 6 The line graph presents the overall relationship between cybersecurity awareness and employee compliance behavior.

IV. FINDINGS

The study reveals that cybersecurity awareness has a significant positive influence on employee compliance behavior within organizations. The majority of employees demonstrated a high level of cybersecurity awareness and understood the importance of following organizational security policies. Employees who regularly participated in cybersecurity awareness training exhibited better compliance with security guidelines, stronger password management practices, and greater ability to identify phishing emails and other cyber threats. The findings also indicate that continuous awareness programs improve employees' knowledge of cyber risks, encourage timely reporting of suspicious activities, and reduce unsafe digital practices. Organizations that promote a strong cybersecurity culture through regular training, policy communication, and management support experience higher employee compliance and lower cybersecurity risks. However, a small percentage of employees still display low awareness and inconsistent compliance due to limited training, negligence, lack of motivation, or insufficient understanding of evolving cyber threats. Overall, the findings confirm that effective cybersecurity awareness initiatives strengthen employee compliance behavior, improve organizational security, and reduce the likelihood of successful cyberattacks.

V. CONCLUSION

The study concludes that cybersecurity awareness plays a vital role in improving employee compliance behavior and strengthening organizational information security. Employees with higher cybersecurity awareness are more likely to comply with organizational security policies, adopt secure password practices, recognize phishing attacks, protect sensitive information, and report cybersecurity incidents promptly. Regular awareness training, simulated phishing exercises, continuous policy updates, and strong management support significantly contribute to developing a positive cybersecurity culture within organizations. The findings further indicate that organizations investing in employee education experience fewer security breaches, improved regulatory compliance, and greater resilience against evolving cyber threats. However, cybersecurity awareness should not be considered a one-time activity, as rapidly changing attack techniques require continuous learning and regular reinforcement of secure behaviors. Therefore, organizations should integrate cybersecurity awareness into their overall business strategy to promote responsible employee behavior, minimize cyber risks, and ensure long-term organizational security.

VI. FUTURE SCOPE

The future scope of this study includes evaluating the effectiveness of emerging technologies such as Artificial Intelligence, Machine Learning, behavioral analytics, and adaptive cybersecurity awareness platforms in improving employee compliance behavior. Future research may compare cybersecurity awareness levels across different industries, organizational sizes, and geographical regions to identify sector-specific security challenges and best practices. Researchers may also investigate the influence of remote work, hybrid work environments, cloud computing, and mobile device usage on employee cybersecurity behavior. Additional studies can examine the role of gamified cybersecurity training, virtual reality-based awareness programs, and AI-driven phishing simulations in enhancing employee learning outcomes. Furthermore, future research may explore the impact of organizational leadership, cybersecurity culture, and international information security standards on long-term employee compliance, enabling organizations to develop more effective and

International Journal of
AI ELECTRICAL CIVIL AND MECHANICAL ENGINEERING
Peer Reviewed, Referred & Indexed Journal
ISSN:3070-0434 www.zesterapublications.com Original Research Paper

sustainable cybersecurity awareness strategies.

VII. REFERENCES

[1] S. Furnell and N. Clarke, *Cybersecurity for Organizations: Principles and Practices*. Springer, 2023.
[2] W. Stallings, *Effective Cybersecurity: A Guide to Using Best Practices and Standards*, Addison-Wesley, 2022.
[3] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 7th ed. Cengage Learning, 2023.
[4] J. R. C. Nurse, M. Bada, and A. M. Sasse, "The Human Factor in Cybersecurity: Exploring the Accidental Insider," *Computers & Security*, vol. 120, 2022.
[5] M. Siponen and A. Vance, "Information Security Policy Compliance: A Systematic Review," *Information & Management*, vol. 60, no. 2, 2023.
[6] S. Furnell, "Cybersecurity Culture and Employee Awareness," *Computer Fraud & Security*, vol. 2024, no. 5, pp. 10–18, 2024.
[7] A. Vance, M. Siponen, and S. Pahnila, "Motivating Information Security Policy Compliance," *MIS Quarterly*, vol. 47, no. 1, pp. 145–166, 2023.
[8] National Institute of Standards and Technology (NIST), *Cybersecurity Framework (CSF) 2.0*, 2024.
[9] International Organization for Standardization (ISO), *ISO/IEC 27001:2022 Information Security Management Systems*, 2022.
[10] Verizon, *2025 Data Breach Investigations Report*, 2025.
[11] IBM Security, *Cost of a Data Breach Report 2025*, 2025.
[12] Cisco, *Cybersecurity Readiness Index 2025*, 2025.
[13] World Economic Forum, *Global Cybersecurity Outlook 2025*, 2025.
[14] ENISA, *Threat Landscape Report 2024*, 2024.
[15] SANS Institute, *Security Awareness Report*, 2024.