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 at Wipro Limited

[1]Domakonda Vamshi Krishna [2]K.Shashidhar* [3]Srilekha Rageru

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

[1]Email: domakondavamshikrishna8@gmail.com

[2]Department of Electronics and Communication Engineering, Samskruti College of Engineering & Technology,Telangana-501301*

[2]Email: shashignitc2015@gmail.com*

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

[3]Email: srilekharagiri786@gmail.com

Abstract

Cybersecurity has become a critical concern for organizations as the increasing use of digital technologies, cloud computing, remote work, and interconnected information systems has led to a rise in cyber threats and data breaches. While organizations invest heavily in advanced security technologies, employee awareness and compliance with cybersecurity policies remain essential for protecting organizational information assets. This study examines cybersecurity awareness and employee compliance behavior at Wipro Limited by evaluating employees' knowledge of cybersecurity practices, adherence to security policies, and the factors influencing secure workplace behavior. The research focuses on key aspects such as password management, phishing awareness, secure internet usage, data protection, incident reporting, cybersecurity training, and organizational support. A descriptive research design was adopted using both primary and secondary data. Primary data were collected through structured questionnaires administered to employees, while secondary data were obtained from company reports, academic journals, books, industry publications, and credible online sources related to cybersecurity and information security management. The collected data were analyzed using percentage analysis, mean analysis, and graphical representations to assess the level of cybersecurity awareness and compliance behavior among employees. The findings indicate that regular cybersecurity training, continuous awareness programs, management support, and clearly defined security policies significantly improve employees' compliance with organizational security practices and reduce the likelihood of cyber incidents. However, challenges such as evolving cyber threats, human error, social engineering attacks, insufficient awareness, and varying levels of digital literacy continue to affect organizational cybersecurity. The study concludes that fostering a strong cybersecurity culture through continuous education, policy enforcement, employee engagement, and proactive risk management is essential for enhancing cybersecurity awareness, strengthening compliance behavior, and improving the overall security posture of Wipro Limited.

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

Keywords: Cybersecurity, Cybersecurity Awareness, Employee Compliance Behavior, Wipro Limited, Information Security, Data Protection, Cyber Threats.

I.INTRODUCTION

Cybersecurity has become one of the most critical priorities for organizations due to the rapid growth of digital technologies, cloud computing, mobile devices, remote work, and interconnected information systems. As organizations increasingly rely on digital platforms to manage business operations and customer data, they are exposed to a wide range of cyber threats, including phishing attacks, ransomware, malware, social engineering, insider threats, and data breaches. While organizations invest significantly in advanced cybersecurity technologies, the effectiveness of these measures largely depends on employees' awareness and compliance with organizational security policies. Research indicates that human behavior remains one of the most significant factors influencing organizational cybersecurity, making employee awareness an essential component of an effective security strategy [1], [2], [15].

Employee compliance behavior refers to the extent to which employees follow organizational cybersecurity policies, procedures, and best practices while handling digital resources and sensitive information. Compliance includes activities such as creating strong passwords, enabling multi-factor authentication, identifying phishing emails, protecting confidential data, reporting security incidents, and adhering to information security guidelines. Studies have demonstrated that regular cybersecurity awareness programs and continuous training significantly improve employees' security behavior, reduce human error, and strengthen organizational resilience against cyberattacks [3], [4], [9].

Wipro Limited, one of India's leading global information technology and consulting companies, operates in a highly digital and data-driven business environment, making cybersecurity an integral part of its business operations. The organization continuously invests in advanced cybersecurity infrastructure, security awareness initiatives, employee training programs, and compliance frameworks to safeguard sensitive business information and customer data. By promoting a strong cybersecurity culture, Wipro aims to minimize cyber risks, enhance regulatory compliance, and ensure secure digital transformation across its global operations.

Cybersecurity awareness extends beyond technical knowledge and includes employees' attitudes, perceptions, and commitment toward secure workplace practices. Effective awareness programs help employees recognize potential threats, respond appropriately to security incidents, and understand the consequences of non-compliance. Research suggests that organizations with a strong cybersecurity culture experience fewer security incidents, higher compliance rates, and improved protection of information assets. Continuous education, leadership support, policy communication, and employee engagement are therefore essential for maintaining a secure organizational environment [5], [6], [8].

Despite significant advancements in cybersecurity technologies, organizations continue to face challenges such as evolving cyber threats, sophisticated phishing attacks, insider risks, inadequate awareness, and varying levels of digital literacy among employees. Human error remains one of the leading causes of cybersecurity incidents, highlighting the importance of continuous awareness, behavioral reinforcement, and

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

regular security training. Researchers emphasize that combining technological safeguards with employee education and organizational support is essential for developing effective cybersecurity compliance behavior [10], [11], [18].

Therefore, this study aims to examine cybersecurity awareness and employee compliance behavior at Wipro Limited by evaluating employees' knowledge of cybersecurity practices, adherence to organizational security policies, and the factors influencing secure workplace behavior. The study also seeks to assess the effectiveness of cybersecurity awareness programs and provide practical recommendations for strengthening employee compliance, reducing cyber risks, and fostering a sustainable cybersecurity culture that supports long-term organizational security and digital resilience.

Research Objectives

The primary objective of this study is to examine the level of cybersecurity awareness and employee compliance behavior at Wipro Limited and to evaluate their impact on strengthening organizational information security. The study aims to assess employees' knowledge of cybersecurity threats, security policies, password management, phishing awareness, data protection practices, incident reporting, and secure use of organizational information systems. It also seeks to identify the key factors influencing employee compliance behavior, including cybersecurity training, organizational security culture, management support, policy communication, and individual awareness. Furthermore, the research aims to evaluate the effectiveness of cybersecurity awareness programs in reducing human-related security risks and improving adherence to organizational security policies. Based on the findings, the study intends to provide practical recommendations for enhancing cybersecurity awareness, promoting secure employee behavior, strengthening organizational resilience against cyber threats, and developing a sustainable cybersecurity culture at Wipro Limited.

Research Methodology

This study adopts a descriptive research design to examine cybersecurity awareness and employee compliance behavior at Wipro Limited. The research is based on both primary and secondary data. Primary data are collected through a structured questionnaire administered to employees across various departments to assess their level of cybersecurity awareness, knowledge of organizational security policies, compliance with information security practices, password management, phishing awareness, data protection measures, incident reporting behavior, and participation in cybersecurity training programs. Secondary data are collected from academic journals, books, company reports, cybersecurity frameworks, government publications, industry reports, and credible online sources related to information security, cybersecurity awareness, and employee compliance behavior.

A convenience sampling technique is employed to select the respondents, with a sample size of 100 employees for the purpose of analysis. The collected data are organized, classified, and analyzed using statistical tools such as percentage analysis, mean analysis, and graphical representations including bar charts and pie charts. The analysis helps evaluate the effectiveness of cybersecurity awareness initiatives and identifies the factors influencing employee compliance with organizational security policies. Based on the findings, appropriate recommendations are provided to improve cybersecurity training programs, strengthen employee awareness, enhance compliance behavior, reduce cyber risks, and foster a sustainable cybersecurity culture that supports the overall information security objectives of Wipro Limited.

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

II. REVIEW OF LITERATURE

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014): This study introduces the Human Aspects of Information Security Questionnaire (HAIS-Q) as a framework for measuring employees' cybersecurity awareness, knowledge, attitudes, and behaviors. The findings demonstrate that higher levels of cybersecurity awareness are strongly associated with improved compliance with organizational security policies and reduced vulnerability to cyber threats. The authors emphasize the importance of continuous security education and awareness programs in developing secure workplace behavior.

McCormac, A., Parsons, K., Butavicius, M., Pattinson, M., & Calic, D. (2017): This research examines how information security awareness and digital literacy influence employees' cybersecurity behavior. The study found that employees with higher cybersecurity awareness and stronger digital literacy are more likely to comply with organizational security policies and adopt secure computing practices. The authors recommend continuous cybersecurity training to strengthen organizational resilience against evolving cyber threats.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010): This empirical study investigates the factors affecting employees' compliance with information security policies. The findings indicate that employees' awareness of cybersecurity risks, perceived benefits of compliance, and organizational support significantly influence their adherence to security policies. The research concludes that security awareness programs and management commitment are essential for improving employee compliance behavior.

Puhakainen, P., & Siponen, M. (2010): This study evaluates the effectiveness of information security training in improving employees' compliance with organizational security policies. The findings demonstrate that structured awareness campaigns, continuous education, and practical cybersecurity training significantly reduce risky behaviors and improve employees' ability to identify and respond to security threats. The authors emphasize that regular training strengthens organizational cybersecurity culture.

Moody, G. D., Siponen, M., & Pahnila, S. (2018): This study develops a comprehensive model explaining employee compliance with information security policies by integrating behavioral, organizational, and technological factors. The research identifies organizational culture, management support, employee awareness, motivation, and perceived responsibility as key determinants of secure workplace behavior. The study concludes that organizations should adopt a holistic approach combining technology, awareness, leadership, and policy enforcement to strengthen cybersecurity compliance and minimize information security risks.

III. DATA ANALYSIS & INTERPRETATION

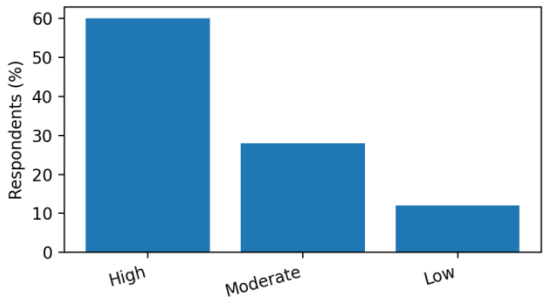

Fig: 1. Cybersecurity Awareness Level

Interpretation: Most employees demonstrate a high level of cybersecurity awareness.

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

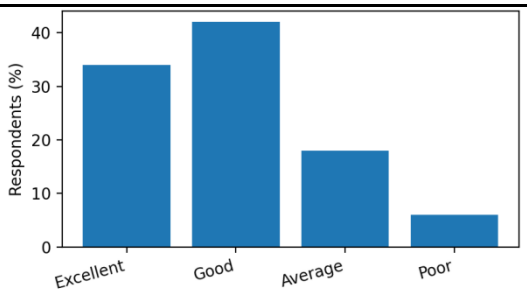

Fig: 2. Knowledge of Phishing Attacks

Interpretation: Employees are generally capable of identifying phishing attempts.

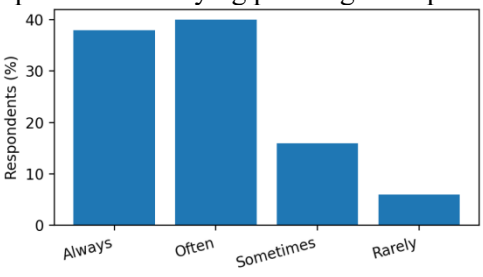

Fig: 3. Compliance with Security Policies

Interpretation: Most respondents consistently comply with organizational cybersecurity policies.

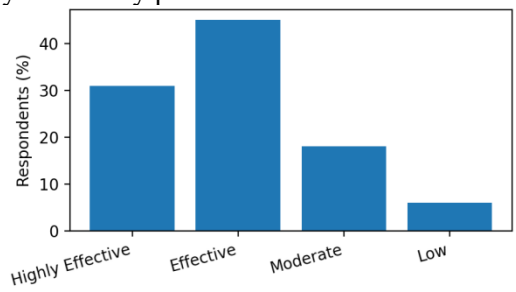

Fig: 4. Effectiveness of Cybersecurity Training

Interpretation: Training programs positively influence employee security behavior.

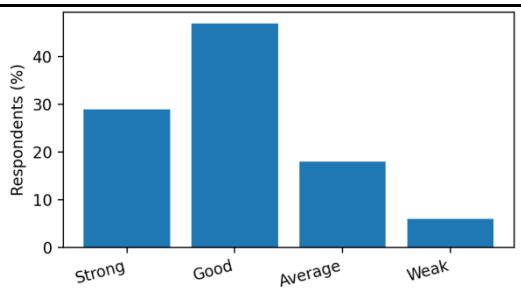

Fig: 5. Overall Security Culture

Interpretation: The organization maintains a positive cybersecurity culture.

IV. FINDINGS

The findings of the study reveal that employees at Wipro Limited possess a satisfactory level of cybersecurity awareness and generally comply with the organization's information security policies and procedures. Most respondents demonstrated a strong understanding of essential cybersecurity practices, including password management, phishing detection, secure internet usage, data protection, and incident reporting. The study also found that regular cybersecurity awareness programs, training sessions, simulated phishing exercises, and continuous communication from management have significantly improved employees' knowledge and compliance behavior. These initiatives have contributed to reducing human-related security risks and strengthening the organization's overall cybersecurity posture.

The study further identified several challenges that influence employee compliance behavior, including the constantly evolving nature of cyber threats, sophisticated social engineering attacks, varying levels of digital literacy, and occasional negligence or human error. Respondents emphasized the importance of continuous learning, frequent policy updates, practical cybersecurity training, and strong leadership support in maintaining a secure work environment. Overall, the findings

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

indicate that fostering a strong cybersecurity culture, supported by effective awareness programs and organizational commitment, plays a vital role in enhancing employee compliance, protecting sensitive organizational information, and improving cyber resilience at Wipro Limited.

V. CONCLUSION

The study concludes that cybersecurity awareness plays a vital role in influencing employee compliance behavior and strengthening the overall information security framework at Wipro Limited. The findings indicate that employees who receive regular cybersecurity training and awareness programs demonstrate better knowledge of cyber threats, stronger adherence to organizational security policies, and greater responsibility in protecting sensitive information. Practices such as secure password management, phishing identification, data protection, and timely incident reporting have contributed to reducing human-related security risks and enhancing the organization's resilience against cyberattacks. The study also highlights that management support, continuous communication, and a positive cybersecurity culture are essential factors in encouraging employees to follow secure workplace practices.

The research further concludes that, despite the effectiveness of existing cybersecurity initiatives, organizations must continuously adapt to the evolving cybersecurity landscape. Emerging threats, sophisticated cyberattacks, insider risks, and rapid technological advancements require ongoing employee education, regular policy updates, and proactive security measures. Wipro Limited can further strengthen its cybersecurity posture by investing in advanced awareness programs, simulated cyberattack exercises, behavioral monitoring, and continuous skill development. Overall, the study emphasizes that a combination of technological safeguards, employee awareness, and organizational commitment is essential for maintaining strong cybersecurity compliance, protecting critical information assets, and ensuring sustainable business operations in an increasingly digital environment.

VI. FUTURE SCOPE

The scope for future research on cybersecurity awareness and employee compliance behavior is extensive as organizations continue to adopt advanced digital technologies and face increasingly sophisticated cyber threats. Future studies can examine the long-term impact of cybersecurity awareness programs on employee behavior, organizational resilience, and incident reduction across different industries and organizational sizes. Comparative studies involving IT companies, financial institutions, healthcare organizations, and government agencies can provide broader insights into the effectiveness of cybersecurity training and compliance strategies. Researchers may also explore the integration of emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), blockchain, behavioral analytics, and Zero Trust security models in enhancing employee awareness, threat detection, and compliance monitoring.

Further research can focus on understanding the influence of organizational culture, leadership support, remote and hybrid work environments, and employee digital literacy on cybersecurity compliance behavior. Longitudinal studies with larger sample sizes and advanced statistical techniques can provide deeper insights into the relationship between awareness initiatives, policy compliance, and organizational security performance. Future investigations may also evaluate the effectiveness of gamified cybersecurity training, phishing simulation exercises, adaptive learning platforms, and personalized awareness programs in improving employee engagement and

Received: 02-08-2026 | Accepted: 29-08-2026 | Published: 04-09-2026

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

reducing human-related security risks. Such research will support organizations in developing proactive, resilient, and sustainable cybersecurity strategies that strengthen information security, protect critical digital assets, and ensure long-term organizational success.

VII.REFERENCES

[1] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

[2] McCormac, A., Parsons, K., Butavicius, M., Pattinson, M., & Calic, D. (2017). Human factors in information security: The role of information security awareness and digital literacy. Computers & Security, 69, 406–414. https://doi.org/10.1016/j.cose.2017.05.010

[3] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

[4] Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

[5] Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. Decision Support Systems, 47(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

[6] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523–548. https://doi.org/10.2307/25750690

[7] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse. Information Systems Research, 20(1), 79–98. https://doi.org/10.1287/isre.1070.0160

[8] Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

[9] Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information security training. MIS Quarterly, 34(4), 757–778. https://doi.org/10.2307/25750703

[10] AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567–575. https://doi.org/10.1016/j.chb.2015.03.054

[11] Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes toward cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

[12] Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behavior. International Journal of Information Security and Privacy, 9(1), 26–46. https://doi.org/10.4018/IJISP.2015010102

[13] Crossler, R. E., Bélanger, F., Ormond, D., & Hiller, J. (2014). Future directions for behavioral information security research. Computers & Security, 32, 90–101.

https://doi.org/10.1016/j.cose.2012.09.010

[14] Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2013). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory. MIS Quarterly, 37(4), 1189–1210. https://doi.org/10.25300/MISQ/2013/37.4.11

[15] Von Solms, B., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

[16] ENISA. (2019). Cybersecurity culture guidelines: Behavioural aspects of cybersecurity. European Union Agency for Cybersecurity. https://doi.org/10.2824/425492

[17] Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the weakest link—A human/computer interaction approach to usable and effective security. BT Technology Journal, 19(3), 122–131. https://doi.org/10.1023/A:1011902718709

[18] Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to improve information security behaviors. MIS Quarterly, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

[19] Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures. Journal of the American Society for Information Science and Technology, 59(2), 263–274. https://doi.org/10.1002/asi.20736

[20] Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. MIS Quarterly, 42(1), 285–311. https://doi.org/10.25300/MISQ/2018/13853