IOSR Journal of Business and Management (IOSR-JBM)
e-ISSN:2278-487X, p-ISSN: 2319-7668. Volume 27, Issue 10. Ser. 1 (October. 2025), PP 07-14
www.iosrjournals.org

An Analysis Of Cybersecurity Threats And Data Protection In The Digital Workplace

Author

Abstract
This study explores the current situation regarding cybersecurity awareness and practices in the Indian corporate community, specifically in the context of a growing number of cyber threats and the emergence of new regulatory requirements in digital formats in the form of the Digital Personal Data Protection (DPDP) Act of 2023.
A quantitative methodological framework was used to analyze survey data in the current study of fifty employees, where descriptive statistics, independent-samples t-tests, and Pearson correlation were applied.
The results have shown a strong knowing-doing gap: workers declare that their awareness of the most widespread cyber threats is high, but the awareness does not reflect into their active compliance with major security habits, and bad password practices can be identified as the major weakness. The most significant result of the study suggests that the gap is caused by ineffective corporate training since the quality of training scored the lowest on all measures of organizational support. The correlation analysis also proves that a positive relationship between the quality of training and adoption of secure behaviors is statistically significant.
The study finds out that a lack of knowledge among the employees is not the main cybersecurity threat, and rather organizational strategy is much inadequate in integrating practices that are secure. On this basis, this paper proposes a radical strategic change of a technology-oriented approach to defense posture to a human-oriented approach with a major focus on the redesign of training courses in order to produce a robust and security-conscious workforce.

Date of Submission: 22-09-2025 Date of Acceptance: 02-10-2025

I. Introduction

In the world of business today, the use of digital tools is crucial to our lives and success because of its fast pace. Nevertheless, the reliance has placed businesses at an unprecedented risk. The economic impact of cybercrime is of significant concern, and recent statistics present the data that losses amounted to more than $16 billion in 2024 and directly affect the company profitability and stability (Tiutiunyk et al., 2025). This is not a mere IT issue anymore; it is a business risk that is critical and all employees should be aware of it, starting in the front desk, to the executive suite.

Cyber threats have radically shifted in nature. Attackers are no longer simply an incidental bother; they are advanced attackers who may employ artificial intelligence (AI) to produce very believable phishing email and business scams that are hard to detect (Dhanararaj, 2025). These attacks attack the human aspect directly and make employees the most vulnerable aspect of a company. This has made the security of company and customer sensitive information a business priority. The privacy of the data is directly related to the security, the reputation, and the possibility of a business to remain in business (Ablon et al., 2017).

Problem Statement

The main problem of the Indian corporate community is the unprecedented increase in cyberattacks, which are increasing more rapidly than defensive solutions. According to recent reports, there was a rise of 115 percent in cyberattacks in India in Q2 2024 over the same timeframe in the previous year (Indusface, 2025), which is much higher than the global average. Not only are these attacks more frequent, but they are also more advanced, as they use advanced malware and AI to exploit vulnerabilities in corporate networks. The economic and reputational harm of such incidents is a serious hazard to business sustenance and national financial wellbeing.

Need

The study is critical as Indian corporations are exposed to a level of cyber threat never witnessed before yet the quality of defences is alarmingly under-evaluated. Technology is no longer the core weakness, but the human element, namely, the disconnect between what employees are aware of regarding cybersecurity and what they actually do in reality. The Digital Personal Data Protection (DPDP) Act, 2023, that now makes corporate directors personally liable in the event of data breaches, is no longer merely an IT matter, but an essential governance and compliance requirement. This research offers the data-driven urgency that is required to know

the actual situation of employee preparedness and to construct security measures to confront the most relevant area of failure: human behaviour.

Research Objectives

The principal aims of the research are:

- To determine and classify the most common cybersecurity threats to Indian business in the digital workplace.
- To determine the efficiency of the existing data protection strategies and best practises that Indian organisations implement.
- To examine the opportunities and challenges of the new Digital Personal Data Protection (DPDP) Act, 2023 to corporate compliance and security.
- To recommend a list of practical solutions to a robust cybersecurity system that would suit the needs of the Indian digital workplace.

Research Questions

The following questions will be considered in this research:

- Which are the main attack surfaces and typical categories of cyber attacks to Indian business in remote and hybrid work environments?
- How well does the current data protection policies and employee awareness strategies help reduce these risks?
- What is the effect of the Digital Personal Data Protection (DPDP) Act, 2023 on the corporate data protection policy and what are the main issues of its implementation?
- Which strategic and operational suggestions can enhance cybersecurity resilience in organisations based in India?

Independent Variables

1. **Organizational Support:** Testing if a higher level of perceived organizational support leads to better employee behavior.
2. **Gender:** This is a demographic independent variable. Used to see if being male or female predicted a difference in awareness or practices.

Dependent Variables

1. **Cybersecurity Awareness:** This is a primary dependent variable.Measuring how aware employees are of the different factors in cybersecurity.
2. **Adherence to Best Practices:** Measuring what practices employees undertake in the field of cybersecurity and data protection.

Hypotheses

Hypothesis 1: The Impact of Training on Security Practices

- **H0 (Null Hypothesis):** There is no statistically significant relationship between the perceived quality of cybersecurity training and employees' adherence to technical best practices.
- **Ha (Alternative Hypothesis):** A higher perceived quality of cybersecurity training is positively correlated with greater adherence to technical best practices.

Hypothesis 2: The Impact of Policies on Awareness

- **H0 (Null Hypothesis):** There is no statistically significant relationship between the clarity of organizational policies and employees' awareness of common cybersecurity threats.
- **Ha (Alternative Hypothesis):** Greater clarity of organizational policies is positively correlated with a higher level of employee awareness of common cybersecurity threats.

Hypothesis 3: Gender Differences in Cybersecurity Practices

- **H0 (Null Hypothesis):** There is no statistically significant difference between male and female employees in their self-reported adherence to cybersecurity best practices.
- **Ha (Alternative Hypothesis):** There is a statistically significant difference between male and female employees in their self-reported adherence to cybersecurity best practices.

II. Literature Reviews

1. The Evolving Legal Landscape of Cybersecurity in India

Agarwal, S., & Antima, D. (2025). In this paper, a legal examination of the development of the cybersecurity laws in India will be provided. It brings to attention the fact that the transition between the reactive IT Act of 2000 to the proactive Digital Personal Data Protection (DPDP) Act of 2023 imposes on businesses new

and preventative responsibilities. This will be essential in comprehending the role of a corporation as a legal and compliance entity.

2. Cybersecurity Governance and Corporate Accountability in India

Chaudhry, R., & Singh, J. (2025). The given review article is targeted to the business executives and claims that cybersecurity is a government matter, rather than an IT one. It describes the introduction of legal and financial responsibility of corporate directors in the DPDP Act, which allows a data breach to become a personal liability. This highlights the necessity of cybersecurity being a part of the general business strategy of companies.

3. Cybersecurity Resilience in the Digital India Framework

Devi, M. S., & Saravanan, S. (2025). This paper is a general, policy-based view of the governmental initiative of Digital India. The main conclusion of it is that the pressure to adopt technology has been faster than security preparedness. It refers to a multi-stakeholder solution, i.e. government and private sectors, to overcome the extreme lack of awareness and lack of talented cybersecurity specialists in India.

4. The Role of Cybersecurity in Protecting Intellectual Property

Okpabi, J., & Uka, J. A. (2024). This review is very applicable in the technology and manufacturing industries in the companies. It dwells on the fact that cybersecurity is an important instrument in protecting the most valuable asset of a company intellectual property (IP). It examines that IP theft is one of the major causes of most advanced cyberattacks and emphasises the risks of external and insider threats.

5. The Impact of Remote Work on Corporate Cybersecurity

Bhattacharya, P., & Verma, S. (2025). This is a systematic review paper that directly covers the issues of the digital workplace. It gives a detailed discussion about the weaknesses introduced by the massive use of remote work. The review contends that the conventional model of the perimeter defence is no longer useful and proposes the concept of a zero-trust security model to safeguard the company data of a distributed workforce.

6. Cybersecurity: A Review of Recent Advances, Threats, and Future Directions

Patel, N., & Shah, M. (2025). This review offers valuable insights for professionals aiming to stay current in the field. It provides a comprehensive overview of the current cybersecurity landscape and forecasts future trends. Particularly insightful is the discussion on artificial intelligence (AI), which highlights its dual role: as a tool for attackers to develop sophisticated threats and as a powerful new defense mechanism.

7. The Business Case for Cybersecurity Investment: A Review of Strategic Drivers

Jha, P. K., & Gupta, A. (2024). This review targets business professionals, asserting that cybersecurity is a strategic investment rather than merely an expense. It presents evidence that a strong security stance directly leads to an improved brand image, increased customer trust, and a competitive advantage. The review highlights that the long-term costs of data breaches significantly exceed the initial expenditures on preventative security measures.

8. Digital Transformation and Cybersecurity Challenges

Kourouma, G., & Dhaou, S. (2025). Human factor is the one largest vulnerability of the digital workplace that is given attention in this review. It is a synthesis of studies that indicate that over billions of dollars on technology, an uneducated worker who clicks on a harmful link is one of the most dominant causes of the information breach. It puts a solid argument in place of establishing a culture of security awareness, who says that human behaviour is a more important defence mechanism than any firewall.

9. A Systematic Review of Cybersecurity Awareness Programs

Sharma, V., & Singh, R. (2024). The paper is very useful and gives a methodological analysis of various training programmes. It discusses the most effective training strategies to influence employee behaviour that can prevent such menaces as phishing and social engineering. The review finds that resilient training in the form of ongoing involvement and realistic training like phishing simulation is required to create a truly resilient human defence layer.

10. The Need for Proactive Cybersecurity in India's Growing Digital Economy

Agarwal, R., & Jain, S. (2025). The present review claims the need of fundamental transformation of the security philosophy: reactive to proactive in a company. It throws light on the fact that India has a fast-growing digital economy, which has become a favourable target of attack with financial interests. The paper ends by

concluding that waiting until there is a breach is no longer an effective strategy and organisations need to invest in predictive analytics, threat intelligence, as well as preventative mechanisms to remain ahead of the threats.

III. Research Methodology

This paper uses a quantitative research design as a means to examine cybersecurity awareness, practises, and organisational support perceptions in the context of the Indian corporate community. The study design was designed in a way that enables gathering and analysing numerical data so that the relationships between the key variables could be statistically analysed. The rationale behind the use of this approach is to present empirical data to answer the research questions on the effectiveness of current cybersecurity postures.

Research Instrument

Data was primarily gathered using a self-administered, structured online questionnaire "Cybersecurity Awareness and Practices Questionnaire." This survey comprised two main sections.

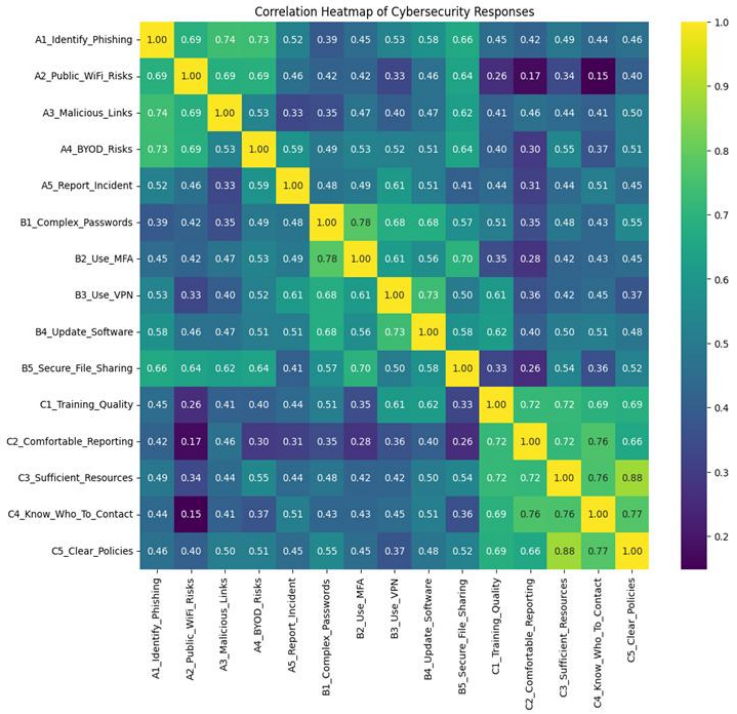
1. **Demographic questions:** This section collected basic data on the respondents' age and gender to allow for demographic analysis.
2. **Likert Scale Questions:** The core of the questionnaire comprised into three thematic sections:
   - **Section A: Awareness of Common Threats**
   - **Section B: Adherence to Technical Best Practices**
   - **Section C: Organizational Support and Security Culture**
3. All items were measured on a **5-point Likert scale**, ranging from 1 ("Strongly Disagree") to 5 ("Strongly Agree"). This scale was chosen to quantify the attitudes and self-reported behaviors of the participants in a standardized manner.

Sampling and Data Collection

This study used a non-probability convenience sampling method. A questionnaire was administered electronically to employees in different firms of the Indian corporate world. Although 60 responses were obtained, the analysis was carried out with the first 50 complete responses (N=50) to ensure consistency of the data. The sample was composed of 68 percent males and 32 percent females, with the majority of the respondents being in the age groups of 18-24 and 25-34.

Data Analysis

A Pearson correlation analysis was conducted to examine the correlations between the various aspects of cybersecurity posture that the respondents reported. The results of the analysis revealed that various positive correlation coefficients are statistically significant and indicate that there is a high level of interconnectedness between awareness, practises, and the perceived organizational security culture.



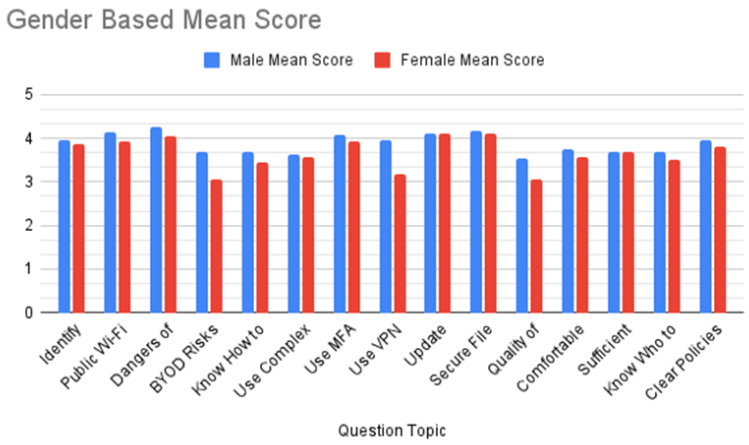
Pearson correlation test showed that there are multiple significant relationships in the data. Updating software (B4) and Multi-Factor Authentication (B2) have the highest positive correlation ($r=0.73$, $p< 0.001$). This implies that the two technical best practices are closely associated with each other and an employee that engages in one is highly likely to engage in the other.

Moreover, the analysis presents statistical data that organisational support is connected to the behaviour of employees. Indicatively, the quality of training (C1) has a moderate and significant relationship with the use of complex passwords (B1) and the VPN (B3). This affirms the finding that improved training has a relationship with improved security practices.

Lastly, the correlation between the clarity of organisational policies (C5) and the awareness of certain threats such as the risk of using public Wi-Fi (A2) is strong, with the $r=0.69$,$p<0.001$. This implies that clear policies are one of the major considerations in sensitising employees on the possible danger.

The correlation analysis illustrates that a good cybersecurity posture is a comprehensive system. It seems that organisational policies and high-quality training are the primary forces that not only raise employee awareness but are connected to the regular implementation of technical best practices.

An independent sample t-test was employed to determine possible differences in cybersecurity awareness and practises between the genders regarding each of the 15 questions in the survey. It was conducted to compare the mean scores of the male (N=34) and female (N=16) respondents.



The findings reveal that cybersecurity posture, cybersecurity awareness, and cybersecurity practices are fairly homogenous, regardless of gender in this sample. The remainder of the 15 questions showed no significant difference in the mean scores of males and females (all $p>0.05$). This indicates that gender does not play a major role in various sections of cybersecurity awareness or behaviour, including phishing detection, password management, and organisational support senses.

The use of a company Virtual Private Network (VPN) on unsecured networks was the only area that was found to differ statistically significantly (B3). Male respondents reported higher frequency of using VPN ($M=3.97$) than female respondents ($M=3.19$). The difference was found to be statistically significant ($p=0.02$).

IV. Findings

The data analysis of this study provides an insightful overview of contemporary workplace in the digital realm. Although employees are much more confident in their skills to detect the most widespread security risks such as phishing emails and malicious links, their compliance with the most important personal security measures is significantly lower. This was the greatest behavioural weakness that was observed, in the form of not consistently using unique and complex passwords. Such a gap indicates a severe gap in which risk awareness fails to translate into risk mitigation practices.

The study confirms strongly that organisational support systems can influence employee behaviour. A Pearson correlation analysis revealed that the quality of cybersecurity training has a positive and significant correlation with the improvement of the quality of security practises, including the use of strong passwords and VPNs. Equally important, employee awareness about a certain threat, such as the dangers of using public Wi-Fi, is mainly caused by the presence of clear and well-defined corporate policies. The idea behind these relationships is that a proper cybersecurity posture is a comprehensive system in which corporate culture can directly affect individual behavior.

Nevertheless, corporate training was found to be the weakest link in this system as well. Although employees admit that the availability of clear policies is known, the training aimed to execute these policies is seen as a poor-quality, unrelated, and unengaging one. This ineffective approach to education seems to be one of the root causes of the observed risky behaviour.

Lastly, the researchers examined the difference between genders and discovered that there is no significant difference between the cybersecurity awareness and practices between men and women. The results were statistically equal on 14 out of 15 survey questions. The difference in the use of a company VPN was the only statistically significant difference with males reporting greater use of the VPN compared to their female counterparts.

V. Discussion

A key finding from this research is the large "knowing-doing gap" between employees, who demonstrate high confidence in spotting threats such as phishing, but report poorer personal habits such as using a password manager. This empirically serves to confirm that the human factor is the most significant vulnerability in the digital workplace as presented by Kourouma & Dhaou (2025). Although it can cost an organisation a lot of money in technological defences, this paper demonstrates that irregular employee behaviour is a major vulnerability that is reiterated in the fact that an untrained employee who clicks a link is one of the main reasons for breaches.

More so, the data reveals the perceived poor quality of corporate training as the weakest link of the organisational defence system. This directly aligns with the systematic review conducted by Sharma & Singh (2024) which concluded that effective training must be continuous and engaging in order for it to truly change behaviour. The training effectiveness scores in this study are low indicating that most organisations in India continue to employ a check-the-box method of training that, as the data reveal, does not impart safe practices.

The correlation study offers effective statistical data to support the suggestions presented by Chaudhry and Singh (2025) that cybersecurity is essentially a governance, rather than an IT, problem. The results indicate that the quality of training is correlated with improved security practices, including the use of complex passwords and VPN, in a positive way. Similarly, the high correlation between the clarity of organizational policies and the awareness of employees towards certain threats ($r=0.69$), shows that the existence of a well defined structure of governance is one of the critical factors for the creation of a secure culture.

These results support the view that cybersecurity must be considered a strategic investment, which in turn is consistent with the approach proposed by Jha & Gupta (2024). Employee practice failure which has been attributed directly to the failure of training provides a clear business rationale to invest in high quality continuous education programmes. The results suggest that organizations that make cybersecurity a core strategy and hold leadership accountable for security as mandated under the DPDP Act have a more likely chance of fostering a resilient security posture.

Subsequently, the t-test results showed that there is mostly no significant difference in cybersecurity awareness and practices between genders, with the results being statistically significant in only 14 out of 15 areas. The only exception was that of VPN since male respondents indicated a higher usage rate. This single difference can also be explained by extraneous factors that were not considered in this research, including the varying job descriptions or the need to travel to work. However, the overall conclusion is that gender is not a significant predictor of general cybersecurity behavior in the sample, which would suggest that awareness and training initiatives should be applied universally, rather than based on gender.

VI. Recommendations

The results of this study require a significant strategic change from a reactive, technology-focused security approach to a proactive, human-focused approach. This starts with corporate leadership and governance boards, which must prioritize cybersecurity as a fundamental business strategy, acknowledging their direct responsibility for data protection in accordance with the DPDP Act, 2023. The most essential and urgent step is a total revamp of corporate training. The existing unproductive, compliance-focused model needs to be substituted with an ongoing educational structure that relies on interactive, role-specific material and hands-on activities such as phishing simulations. This targeted investment in a security-conscious culture is the best method to change the human factor from the most vulnerable aspect into the primary line of defense.

To facilitate this cultural and strategic change, IT and Information Security teams need to establish and uphold strong technical controls that address the significant behavioral gaps revealed in this analysis. Due to the widespread poor password practices, organizations should require Multi-Factor Authentication (MFA) for all essential systems without exceptions. Additionally, to tackle the fundamental issue of inadequate password habits, organizations should implement and mandate the usage of a high-quality password manager. These technical enhancements will successfully close the "knowing-doing gap" by alleviating the cognitive load on employees and implementing a stricter security standard, establishing a robust, multi-tiered defense that safeguards the organization against internal and external threats.

VII. Research Limitations

Although this research provides valuable data about the way Indian firms defend the information of their staff, it is limited. Such limits are to be remembered when considering the results, and assist in future research.

To begin with, the research utilized a survey response. Individuals might have claimed that they adhere to best security regulations as compared to the real adherence because they wish to appear good. This may imply that the difference between what is known and done by people might even be greater than the figures indicate.

Second, the researchers selected the participants who could be approached easily and not a random sample. They only got 50 people. This is sufficient to arrive at some statistics but this also implies that the findings might not be applicable to all the Indian workers, particularly because the group comprised predominantly of young employees. There is a great number of age groups and jobs in the entire Indian corporate sphere.

Lastly, the study presented numbers to indicate what the issues are like bad training and weak passwords but it failed to provide the reason as to why the issues exist. We are yet to understand why training may be evil and why individuals fail to use strong passwords. The various attitudes, cultures, or even particular barriers at work that influence the behavior of people cannot be comprehended by numbers alone.

VIII. Conclusion

This study notes that the greatest challenge in effective cybersecurity among Indian firms is not the fact that employees are unfamiliar with the threats, but the fact that the firms have not translated the knowledge into daily safe practices. The statistics reveal the obvious presence of the so-called knowing-doing gap: individuals are aware of the danger yet continue to engage in risk behaviors, particularly, using weak passwords. It has been evidenced as a result of poor corporate support where minimal training quality is the primary cause of the gap, instead of poor individual performance. It is demonstrated in the paper that there are good rules but methods of ensuring people adhere to them in real life are not effective. Thus, this piece confirms that firms should stop with the strategy consisting of exclusively employing technology but instead move towards the people-focused strategy. Cybersecurity can be enhanced the most by continuing to invest in relevant, motivating, and effective training that can transform individuals into the weakest link to the strong defense.

References

[1]. Ablon, O., Breytenbach, W., & Singh, R. (2017). The Rise Of Cybersecurity And Its Impact On Data Protection. Researchgate. Https://Www.Researchgate.Net/Publication/317968117_The_Rise_Of_Cybersecurity_And_Its_Impact_On_Data_Protection

[2]. Dhanaraj, B. V. (2025). The Role Of Artificial Intelligence In Enhancing Cyber Threats: A Review. Journal Of Cybersecurity. Https://Ijsra.Net/Sites/Default/Files/IJSRA-2024-2161.Pdf

[3]. Tiutiunyk, R., Shulga, I., & Chernov, A. (2025). The Escalating Financial Cost Of Cybercrime: A Global Perspective. Journal Of Economic Cybernetics. Https://Www.Researchgate.Net/Publication/389078572_Impact_Of_Cyber_Security_Measures_On_Risk_Mitigation_With_The_Mediating_Role_Of_Data_Protection

[4]. Dhanaraj, B. V. (2025). The Role Of Artificial Intelligence In Enhancing Cyber Threats: A Review. Journal Of Cybersecurity. Https://Ijsra.Net/Sites/Default/Files/IJSRA-2024-2161.Pdf

[5]. Indusface. (2025). Indian Application Security Threat Report 2024. Https://Www.Indusface.Com/Website/Resources/Reports/Indian-Application-Security-Report-2024

[6]. Researchgate. (2025). The State Of Cybersecurity In India: Challenges And Future Directions. Researchgate. Https://Www.Researchgate.Net/Publication/381502476_The_State_Of_Cybersecurity_In_India_Challenges_And_Future_Directions

[7]. Skillogic. (2024). Cybersecurity In The Era Of Remote Work: A Study On Indian Companies. Https://Skillogic.Com/Blog/Cyber-Security-In-The-Era-Of-Remote-Work

[8]. Agarwal, S., & Antima, D. (2025). Legal Dimensions Of Data Privacy And Cybersecurity In India's Digital Economy. IJCRT.Org. Https://Www.Ijcrt.Org/Papers/IJCRT2509061.Pdf

[9]. Chaudhry, R., & Singh, J. (2025). Cybersecurity Risks And Corporate Accountability In India: Director Responsibility, Legal Reforms, And The Role Of Regulatory Bodies In Data Protection. Researchgate. Https://Www.Researchgate.Net/Publication/391819934_CYBERSECURITY_RISKS_AND_CORPORATE_ACCOUNTABILITY_IN_INDIA_DIRECTOR_RESPONSIBILITY_LEGAL_REFORMS_AND_THE_ROLE_OF_REGULATORY_BODIES_IN_DATA_PROTECTION

[10]. Devi, M. S., & Saravanan, S. (2025). Cybersecurity Resilience In The Digital India Framework: Challenges And Strategies. Researchgate. Https://Www.Researchgate.Net/Publication/391901034_CYBERSECURITY_RESILIENCE_IN_THE_DIGITAL_INDIA_FRAMEWORK_CHALLENGES_AND_STRATEGIES

[11]. Okpabi, J., & Uka, J. A. (2024). The Role Of Cybersecurity In Protecting Intellectual Property. Researchgate. Https://Www.Researchgate.Net/Publication/383204010_The_Role_Of_Cybersecurity_In_Protecting_Intellectual_Property

[12]. Bhattacharya, P., & Verma, S. (2025). An Overview Of Remote Work And Its Impact On Cybersecurity. Https://Www.Researchgate.Net/Publication/391456722_An_Overview_Of_Remote_Work_And_Its_Impact_On_Cybersecurity

[13]. Patel, N., & Shah, M. (2025). Cybersecurity: A Review Of Recent Advances, Threats, And Future Directions. JETIR Research Journal. Https://Www.Jetir.Org/Papers/JETIRGB06057.Pdf

[14]. Jha, P. K., & Gupta, A. (2024). A Comprehensive Review Of The Strategic Importance Of Cybersecurity Investment In The Indian Corporate Sector. Researchgate. Https://Www.Researchgate.Net/Publication/382103456_A_Comprehensive_Review_Of_The_Strategic_Importance_Of_Cybersecurity_Investment_In_The_Indian_Corporate_Sector

[15]. Kourouma, G., & Dhaou, S. (2025). Editorial: Digital Transformation And Cybersecurity Challenges. Frontiers In Computing.

Https://Www.Researchgate.Net/Publication/392026583_Editorial-_Digital_Transformation_And_Cybersecurity_Challenges
[16]. Sharma, V., & Singh, R. (2024). A Systematic Review Of Cybersecurity Awareness Programs For Corporate Employees In India. International Journal Of Modern Engineering Research. Https://Www.Ijmer.Com/Papers/Vol14_Issue7/A_Systematic_Review_Of_Cybersecurity_Awareness_Programs_For_Corporate_Employees_In_India.Pdf
[17]. Agarwal, R., & Jain, S. (2025). The Need For Proactive Cybersecurity In India's Growing Digital Economy. International Journal Of Research In Engineering And Technology. Https://Www.Ijret.Org/Research-Paper/The-Need-For-Proactive-Cybersecurity-In-Indias-Growing-Digital-Economy