Irish Interdisciplinary Journal of Science & Research (IIJSR)
Volume 9, Issue 3, Pages 46-59, July-September 2025

A Comprehensive Study on the Protection of Business Information in the Indian Digital Ecosystem

Nasreen Johi*

*5th Year B.A. LL.B. (Hons), SRM School of Law, SRM Institute of Science and Technology (SRMIST), SRM University, Chennai, Tamil Nadu, India. Corresponding Author Email: johiibrahim06@gmail.com**

DOI: https://doi.org/10.46759/IIJSR.2025.9306

Article Received: 01 June 2025 *Article Accepted: 12 August 2025* *Article Published: 21 August 2025*

ABSTRACT

In today's digital age, the protection of business information is of paramount importance. Organisations face numerous challenges in safeguarding their sensitive data from unauthorised access, data breaches, and other forms of cyber threats. The consequences of information loss or compromise can be severe, leading to financial losses, reputational damage, and legal liabilities. Therefore, it is imperative for organisations to adopt effective strategies and measures to ensure the confidentiality, integrity, and availability of their business information. In the rapidly evolving digital landscape of India, the protection of business information has emerged as a critical concern for organisations across various sectors. With the country's ambitious digital transformation initiatives and the growing reliance on technology, businesses face unique challenges and risks when it comes to safeguarding their valuable information. Thus, the study of the protection of business information in India is of utmost importance to ensure the security and integrity of sensitive data. The objectives of the research is To analyse the effectiveness of existing data protection strategies and policies, To analyse the impact of data breaches or security incidents on the reputation of business organisations and To propose recommendations and best practices for enhancing the protection of business information. The research method followed is empirical Research. A total of 201 samples were taken from the general public through convenient sampling. The primary source of information was taken from the general public in the form of a survey method. The secondary sources of information were from journal articles, books and reports of presidency non-governmental organisations. This paper concludes that as India continues its digital journey, prioritising the protection of business information is vital for sustainable growth and success.

Keywords: Information Security; Data Protection; Cybersecurity; Confidentiality; Business; Digital Security; Personal Data Protection; Information Governance; Cyber Laws; Risk Management; Data Breach; Digital Economy; Information Privacy; Cyber Resilience; Data Compliance.

1. Introduction

In today’s digital landscape, the protection of business information is of paramount importance. Organisations face numerous challenges in safeguarding their sensitive data from unauthorised access, data breaches, and other forms of cyber threats. The consequences of information loss or compromise can be severe, leading to financial losses, reputational damage, and legal liabilities. Therefore, it is imperative for organisations to adopt effective strategies and measures to ensure the confidentiality, integrity, and availability of their business information. In the rapidly evolving digital landscape of India, the protection of business information has emerged as a critical concern for organisations across various sectors. With the country's ambitious digital transformation initiatives and the growing reliance on technology, businesses face unique challenges and risks when it comes to safeguarding their valuable information. Thus, the study of the protection of business information in India is of utmost importance to ensure the security and integrity of sensitive data. One of the key factors driving the need for protection of business information in India is the exponential growth of the digital economy. With the proliferation of e-commerce, online banking, and digital payment systems, businesses are handling vast amounts of customer data, including personal and financial information. The loss or compromise of such data can have severe consequences for individuals and organisations alike. Therefore, it becomes imperative to study and implement robust security measures to protect this sensitive information from unauthorised access, data breaches, and cyber threats. Moreover, India has witnessed a significant rise in cybercrime incidents in recent years. With the increasing adoption of digital

technologies, cybercriminals have become more sophisticated in their methods, targeting both large enterprises and small businesses. The study of business information protection in India aims to address these emerging threats and vulnerabilities by developing comprehensive strategies, conducting risk assessments, and implementing cybersecurity frameworks.

Furthermore, India has implemented stringent data protection regulations to safeguard the privacy and security of personal information. The Personal Data Protection Bill, 2019, which is currently under consideration, aims to establish a robust data protection framework in line with international standards. The study of business information protection in India involves understanding and complying with these regulations to ensure legal and regulatory compliance, and to build trust with customers. Additionally, the study of business information protection in India also encompasses promoting awareness and education on cybersecurity best practices. Businesses need to invest in training programs and workshops to equip their employees with the necessary knowledge and skills to recognize and mitigate potential risks. By fostering a culture of cybersecurity awareness, organisations can create a strong line of defence against cyber threats. The government plays a crucial role in ensuring the protection of business information by implementing various initiatives and policies aimed at enhancing cybersecurity and data protection.

In India, several notable government initiatives have been introduced to address the challenges and risks associated with the protection of business information. One of the prominent initiatives is the National Cyber Security Policy (NCSP) 2013, which outlines the government's strategy to protect the country's cyberspace. The NCSP focuses on developing a secure and resilient information infrastructure, creating an ecosystem for cybersecurity research and development, and promoting awareness and capacity building in the field of cybersecurity. It aims to establish a secure digital ecosystem to safeguard business information from cyber threats. Another significant government initiative is the establishment of the Indian Computer Emergency Response Team (CERT-In) in 2004. CERT-In serves as the national nodal agency for responding to cybersecurity incidents and managing vulnerabilities in the country's information infrastructure. It provides early warning and response mechanisms, incident response coordination, and cybersecurity training and awareness programs. CERT-In collaborates with various stakeholders, including businesses, to strengthen cybersecurity measures and protect critical business information. The government has also introduced data protection regulations to safeguard personal information. The proposed Personal Data Protection Bill, 2019, aims to provide a comprehensive framework for the protection of personal data and establish individuals' rights over their data. The bill introduces stricter regulations on data processing, consent requirements, data localization, and enforcement mechanisms. Once implemented, it will enhance the protection of personal and business information and provide individuals with greater control over their data. The Digital India program also emphasises the importance of cybersecurity and aims to create a digitally secure environment by integrating security measures across various digital initiatives. Furthermore, the government has collaborated with industry bodies and organisations to enhance cybersecurity measures. The Ministry of Electronics and Information Technology (MeitY) has partnered with industry associations and sector-specific organisations to develop sectoral Computer Emergency Response Teams (CERTs) to address cybersecurity challenges specific to different industries. These sectoral CERTs work closely with businesses to enhance their cybersecurity posture and protect their critical business information. The UK has well-established data protection laws aligned with the EU GDPR,

while India is in the process of enacting the Personal Data Protection Bill. The UK does not have explicit data localization requirements, whereas India mandates data localization for sensitive personal data. Both countries have cybersecurity initiatives, such as the UK's National Cyber Security Centre and India's CERT-In. The UK actively engages in international cooperation on cybersecurity, while India participates in various forums. As the legal frameworks and approaches differ, businesses in the UK and India face varying requirements and considerations when it comes to protecting their business information. The main aim of the research is to analyse the effectiveness of existing data protection strategies.

1.1. Study Objectives

1) To analyse the potential threat that poses the greatest risk to the security of business information.
2) To analyse the impact of data breaches or security incidents on the reputation of business organisations.
3) To propose recommendations and best practices for enhancing the protection of business information.
4) To analyse the effectiveness of existing data protection strategies and policies.
5) To evaluate the role of legal regulatory frameworks in safeguarding business information in India.
6) To examine the influence of employee awareness and organisational culture on information security practices.

2. Review of Literature

1. **Li, X., & Huang, J.** "Enhancing Business Information Security: Encryption and Access Control Measures." In their study Concluded that Robust encryption techniques and access control mechanisms are crucial for protecting business information from unauthorised access. Continuous monitoring and updates of security measures are necessary to address evolving threats.

2. **Wang, Y., & Chen, H**. In their study on "Mitigating Employee Negligence: Training Programs for Business Information Security." concluded that Employee negligence and social engineering attacks pose significant vulnerabilities in business information security. Comprehensive training programs and awareness campaigns are essential to educate employees about security risks and promote responsible information handling.

3. **Jones, L., & Smith, R.** In their analysis on "Passwords and Authentication: Strengthening Business Information Security." Concluded that Strong password policies and multi-factor authentication play a crucial role in safeguarding business information. Password management tools and regular password updates can mitigate the risk of unauthorised access.

4. **Garcia, A., & Martinez, P.** In their journal on "Organisational Culture and Information Security: Creating a Security-Conscious Environment." Concluded that Organisational culture influences information security practices. Leadership commitment, employee involvement, and clear communication are essential to foster a strong security culture within businesses.

5. **Johnson, M., & Thomas, S** in their research on "The Impact of Data Breaches on Business Organisations: Financial and Reputational Consequences." Concluded that Data breaches have significant financial and

reputational consequences for business organizations. Incident response plans, data backup strategies, and cyber insurance are crucial in mitigating the risks associated with breaches.

6. **Brown, K., & Wilson, D** in their analysis on "Legal and Regulatory Framework for Protecting Business Information: Compliance and Consequences." Concluded that Compliance with data protection laws, privacy regulations, and industry standards is crucial for businesses to avoid legal penalties and reputational damage.

7. **Zhang, Q., & Liu, C.** In their study on "Cloud Computing Security for Business Information: Challenges and Solutions." Concluded that Cloud computing security poses challenges for protecting business information. Implementing encryption, access controls, and secure communication protocols are important solutions for ensuring data confidentiality and integrity.

8. **Sharma, A., & Patel, R**. "Information Security Challenges in Indian Businesses: A Comprehensive Review." Concluded that Indian businesses face unique information security challenges due to factors such as regulatory landscape, cultural aspects, and increasing cyber threats. A holistic approach encompassing technology, policies, and employee awareness is necessary for effective protection of business information.

9. **Gupta, S., & Verma, N** in their review on "Cybersecurity Policies and Practices in Indian Organisations: A Literature Review." Concluded that The literature highlights the importance of robust cybersecurity policies and practices in Indian organisations for protecting sensitive business information. Implementation of standards, frameworks, and risk assessment methodologies is essential to mitigate cyber risks effectively.

10. **Reddy, M., & Kumar, S** in their study on "Data Privacy and Protection in Indian Business Environment: An Overview." Concluded that Indian businesses are grappling with data privacy and protection challenges due to regulatory frameworks and evolving customer expectations. Compliance with the Personal Data Protection Bill and adoption of privacy-enhancing technologies are crucial for safeguarding business information.

11. **Desai, P., & Joshi, V** conducted research on "Insider Threats to Business Information Security: A Review of Indian Case Studies." In which they Concluded that Insider threats pose significant risks to the security of business information in Indian organisations. Effective implementation of access controls, employee monitoring, and awareness programs are essential to mitigate insider risks.

12. **Chatterjee, R., & Singh, P.** In their study on "Cloud Security in Indian Business Organizations: Challenges and Countermeasures." Concluded that Indian businesses face challenges in ensuring the security of business information in cloud environments. Encryption, data segregation, and third-party audits are key countermeasures for enhancing cloud security and maintaining data integrity.

13. **Kapoor, M., & Singhania, R.** In their research on "Emerging Technologies for Business Information Security in India: A Literature Review." The study explores the potential of emerging technologies such as blockchain, artificial intelligence, and machine learning in enhancing business information security in the Indian context. Adoption of these technologies can improve data protection, authentication, and threat detection capabilities.

14. **Joshi, A., & Sharma, V.** In their study on "Role of Government Initiatives in Enhancing Business Information Security in India." Concluded that literature highlights the role of government initiatives, such as the National

Cyber Security Policy and Digital India program, in promoting and enforcing information security practices in Indian businesses. Collaboration between government agencies, industry stakeholders, and academia is crucial for a robust cybersecurity ecosystem.

15. **Raghavan, S., & Mehta, N.** "Mobile Security in Indian Business Organizations: A Review of Challenges and Solutions." Concluded that The review identifies the challenges associated with mobile security in Indian business organisations, including device vulnerabilities and data leakage risks. The implementation of mobile device management, secure app development, and user awareness programs can mitigate these challenges effectively.

16. **Mishra, R., & Gupta, A.** In their journal on "Supply Chain Security in Indian Businesses: An Overview and Best Practices." Concluded that The study provides an overview of supply chain security challenges faced by Indian businesses and emphasises the importance of implementing best practices. Collaboration, risk assessment, and continuous monitoring are key strategies to enhance supply chain information security.

17. **Patel, S., & Singh, A.** In their analysis on "Big Data Security and Privacy in Indian Business Organizations: A Literature Review." Concluded that The review explores the security and privacy challenges associated with big data in Indian business organisations. Solutions such as data anonymization, encryption, and privacy-preserving techniques are crucial to protect sensitive information while leveraging the benefits of big data analytics.

18. **Rajput, K., & Pandey, S.** in their study on "Role of Ethical Hacking in Strengthening Business Information Security in India." Concluded that Ethical hacking plays a vital role in identifying vulnerabilities and testing the effectiveness of security measures in Indian business organisations . Conducting regular penetration testing and engaging ethical hackers can help proactively identify and address security weaknesses.

19. **Singh, R. K.** In their study on "The Impact of Data Breaches on Business Organizations in India: A Literature Review" Concluded that The review highlights the severe consequences of data breaches on Indian business organisations, including financial losses, reputational damage, and regulatory implications. It emphasises the need for robust cybersecurity measures and proactive incident response strategies.

20. **Verma, S** In their study on "Understanding the Impact of Data Breaches on Business Organizations in India: A Comprehensive Review" Concluded that The study reveals that data breaches have far-reaching effects on Indian business organisations, affecting customer trust, brand reputation, and competitive advantage. It underscores the importance of implementing effective security measures and establishing breach response plans.

3. Methodology

The research method followed is descriptive research. A total of 201 samples have been taken out of which is taken through convenient sampling. The sample frame taken by the research through the general public based on a questionnaire. The primary source of information was taken from the general public in the form of a survey method. The secondary sources of information were from journal articles, books and reports of presidency non-governmental organisations. The independent variables taken here are age, gender, education, occupation. The dependent variables are Encrypting is the best possible defence against a security breach, best way to protect sensitive business information, Any organisation that wants to work effectively need to ensure the safety of their

information by implementing a data protection plan etc., The statistical tool used here in this research is graphical representation (SPSS).

4. Analysis

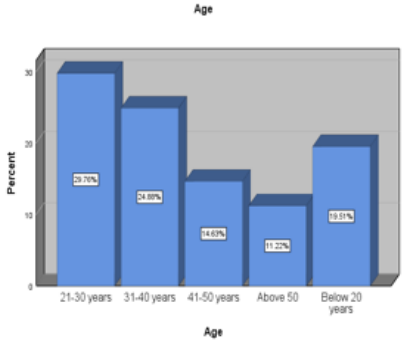

Figure 1. Bar graph represents the sample respondents on the basis of Age

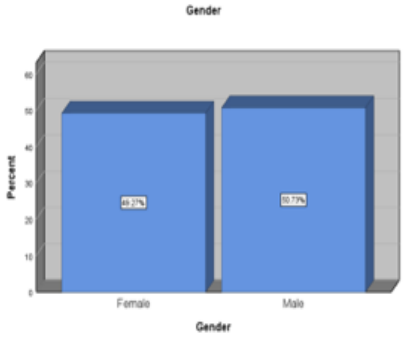

Figure 2. Bar graph represents the sample respondents on the basis of Gender

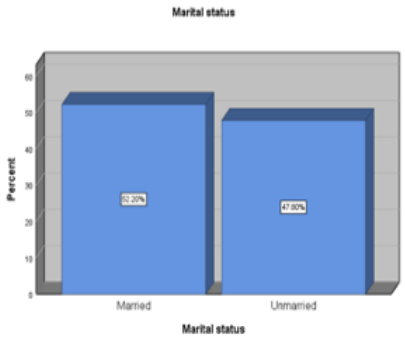

Figure 3. Bar graph represents the sample respondents on the basis of Marital status

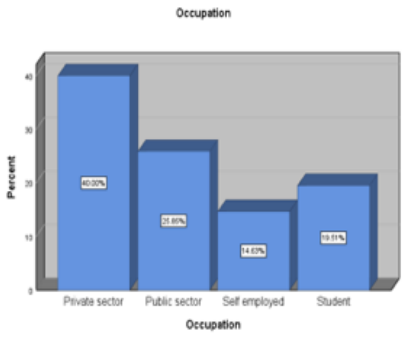

Figure 4. Bar graph represents the sample respondents on the basis of occupation

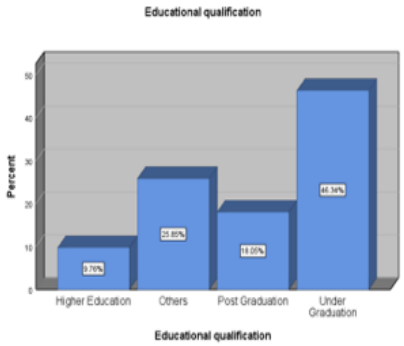

Figure 5. Bar graph represents the sample respondents on the basis of Educational qualification

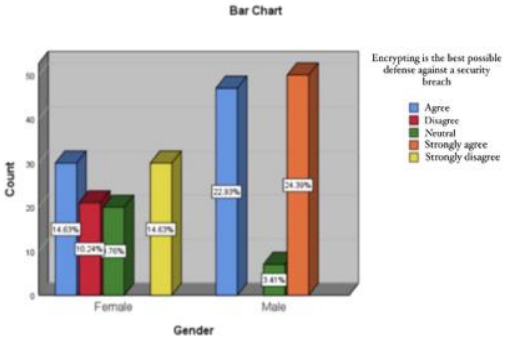

Figure 6. Agreeability on Encrypting is the best possible defence against a security breach with reference to gender of the sample respondents

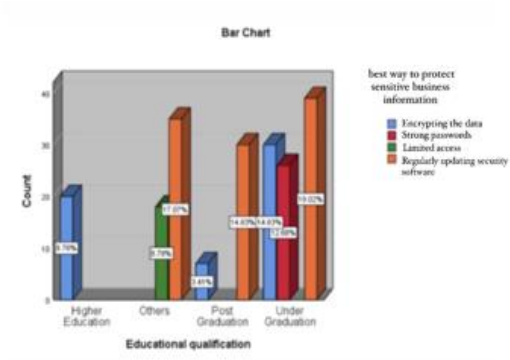

Figure 7. Opinion on the best way to protect sensitive business information with reference to educational qualification of the sample respondents

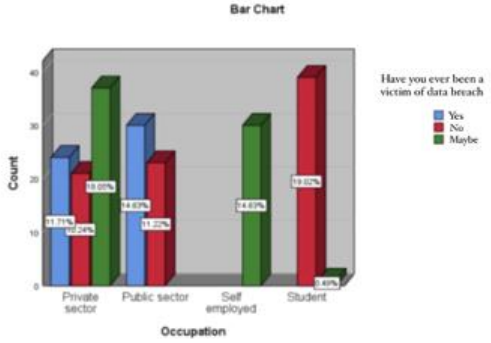

Figure 8. Deals with have you ever been a victim of data breach with reference to occupation of the sample respondents

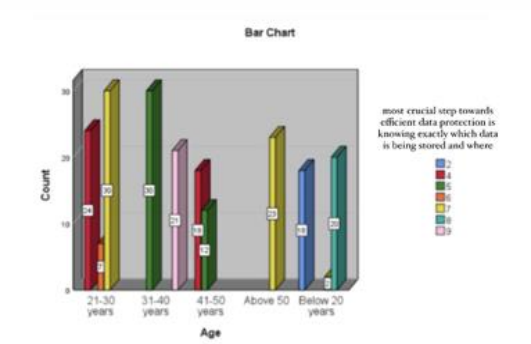

Figure 9. Deals with opinion on One of the most crucial steps towards efficient data protection is knowing exactly which data is being stored and where with reference to age of the sample respondents

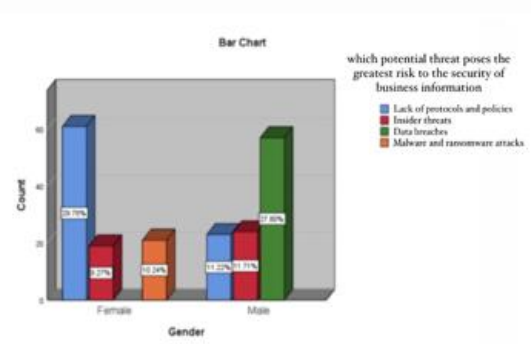

Figure 10. Deals with opinion on which potential threat poses the greatest risk to the security of business information with reference to gender of the sample respondents

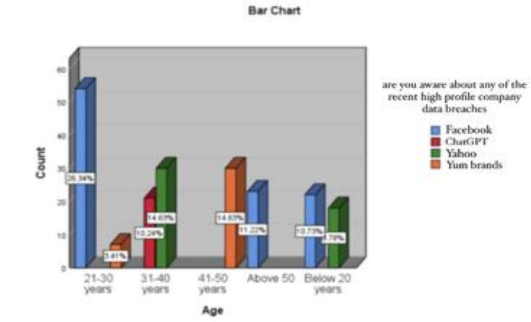

Figure 11. Deals with awareness on any of the recent high profile company data breaches with reference to age of the sample respondents

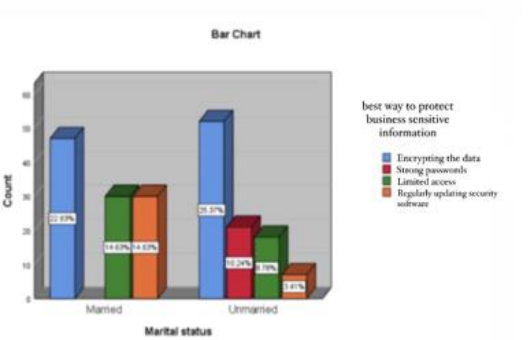

Figure 12. Deals with opinion on the best way to protect sensitive business information with reference to marital status of the sample respondents

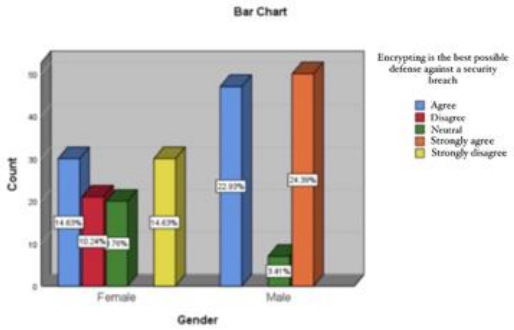

Figure 13. Deals with Agreeability on Encrypting is the best possible defence against a security breach with reference to gender of the sample respondents

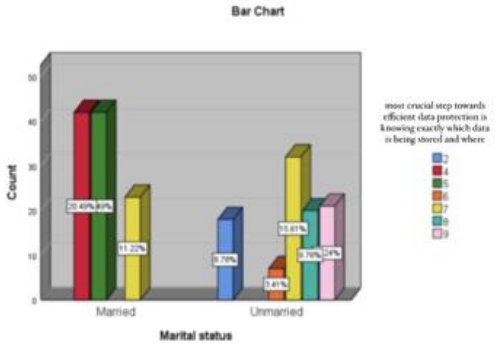

Figure 14. Deals with opinion on One of the most crucial steps towards efficient data protection is knowing exactly which data is being stored and where with reference to marital status of the sample respondents

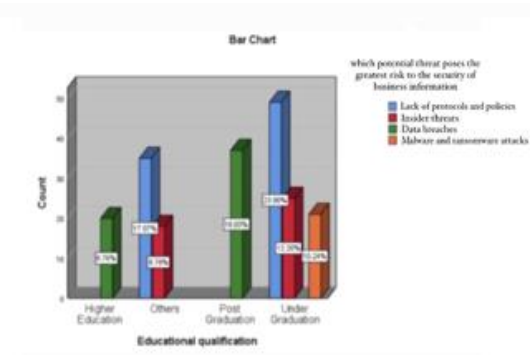

Figure 15. Deals with opinion on which potential threat poses the greatest risk to the security of business information with reference to educational qualification of the sample respondents

5. Results

Figure 1- Bar graph represents the sample respondents on the basis of Age, 29% of the respondents belonged to the age group of 21-30 years and 24% of the respondents belonged to age group 31-40 years. **Figure 2**-Bar graph represents the sample respondents on the basis of Gender, 49% of the respondents were female and 51% were male respondents. **Figure 3**-Bar graph represents the sample respondents on the basis of Marital status, 52% of the respondents were married and 48% of the respondents were Unmarried. **Figure 4**- Bar graph represents the sample respondents on the basis of occupation, majority of the sample respondents belonged to the private sector by 40% and 20% were belonging to the public sector and the remaining 34% were self-employed or students. **Figure 5**- Bar

graph represents the sample respondents on the basis of Educational qualification, 46% of the respondents were undergraduates and the remaining 54% was postgraduates and others. **Figure 6-** 24% of the male respondents strongly agreed to it and 14% of the female respondents and another 23% of the male respondents agreed to it. **Figure 7**- 19% of the respondents belonging to undergraduate's, 14% of the respondents belonging to postgraduate's 17% others think it is regularly updating security software. **Figure 8**-11% of the respondents belonging to the private sector and 14% of the respondents belonging to the public sector answered yes. **Figure 9**-30% of the respondents belonging to the age group of 21-30 yrs and 23% of the respondents belonging to above 59 years opted for 7. **Figure 10-** 29% of the female respondents and 11% of the male respondents answered lack of protocols and policies. **Figure 11-** 26% of the respondents belonging to the age group of 21-30 yrs and 11% of the respondents belonging to above 50 years answered Facebook as they were aware of it. **Figure 12-** 23% of the married respondents and 25% of the Unmarried respondents answered encrypting the data. **Figure 13-** 23.5% of the male respondents strongly agreed to it and 14% of the female respondents and another 23% of the male respondents agreed to it. **Figure 14-** 11% of the married respondents and 15% of the Unmarried respondents opted for 7. **Figure 15-** 23% of the undergraduate respondents and 17% of others think its lack of protocols and policies, 18% of postgraduates and 9% of higher education think its data breaches.

6. Discussion

Figure 1- Most of the respondents were between the age category of 21-40 years. **Figure 2-** Male respondents were higher in number by 2%. **Figure 3-** Married respondents were higher in number by 5%. **Figure 4-** Most of the respondents belonged to the Private or public sector. **Figure 5-** Most of the respondents belonged to undergraduates. **Figure 6-** 24% of the male respondents strongly agreed to it this could be because it helps to protect sensitive information from unauthorised access.

Figure 7- 19% of the respondents belonging to undergraduate's , 14% of the respondents belonging to postgraduate's 17% others think it is regularly updating security software this could be because a regular check and update can protect others sensitive information. **Figure 8**-11% of the respondents belonging to the private sector and 14% of the respondents belonging to the public sector answered yes this could be because nowadays there is increasing in number of e-frauds and ethical hackers. **Figure 9**- 30% of the respondents belonging to the age group of 21-30 yrs and 23% of the respondents belonging to above 59 years opted for 7 this could be because when every data which are highly sensitive is secured separately it is easy to secure it.

Figure 10- 29% of the female respondents and 11% of the male respondents answered lack of protocols and policies. **Figure 11-** 26% of the respondents belonging to the age group of 21-30 yrs and 11% of the respondents belonging to above 50 years answered Facebook as they were aware of it this is because Facebook had nearly 8 data breaches since its launch in 2004 including the Cambridge analytic scandal. **Figure 12-** 23% of the married respondents and 25% of the Unmarried respondents answered encrypting the data this could be because a regular check and update can protect others sensitive information. **Figure 13-** 23.5% of the male respondents strongly agreed to it and 14% of the female respondents and another 23% of the male respondents agreed to it this could be because it helps to protect sensitive information from unauthorised access. **Figure 14-** 11% of the married

respondents and 15% of the Unmarried respondents opted for 7 this could be because when every data which are highly sensitive is secured separately it is easy to secure it. **Figure 15-** 23% of the undergraduate respondents and 17% of others think its lack of protocols and policies, 18% of postgraduates and 9% of higher education think its data breaches.

7. Limitations

One of the major limitations of the study in the sample frame. There is a major constraint in the sample frame as it is limited. We collected our responses through a survey in bus stands and the general public and was conducted by sending online forms to the people. The Convenient sampling method is followed to carry out the survey. All our respondents are literates. Thus, it proves to be difficult to extrapolate it to a larger population.

8. Findings of the Research

In today's digital landscape, businesses face numerous threats to the security of their valuable information. However, one potential threat that poses the greatest risk is the rise of sophisticated social engineering attacks. Social engineering techniques involve manipulating individuals into revealing sensitive information or granting unauthorised access. Whether through phishing emails, impersonation, or pretexting, attackers exploit human vulnerabilities rather than technical weaknesses. These attacks can target employees at all levels, seeking to exploit their trust, curiosity, or lack of awareness. By gaining access to business systems or confidential data, cybercriminals can cause significant financial and reputational damage. Mitigating this threat requires a combination of robust cybersecurity protocols, regular employee training, and vigilant awareness to ensure the protection of business information in the face of evolving social engineering tactics.

9. Suggestions

1. Implement Strong Access Controls: Use strong passwords, two-factor authentication, and role-based access controls to ensure that only authorised individuals have access to sensitive business information.

2. Regularly Update and Patch Systems: Keep software, applications, and operating systems up to date with the latest security patches to address vulnerabilities that can be exploited by hackers.

3. Encrypt Sensitive Data: Implement encryption for sensitive data both at rest and in transit. Encryption helps protect data even if it falls into unauthorized hands or is intercepted during transmission.

4. Conduct Regular Security Audits and Assessments: Perform regular security audits and risk assessments to identify vulnerabilities, assess the effectiveness of security controls, and make necessary improvements to protect business information.

5. Provide Employee Training and Awareness: Educate employees on cybersecurity best practices, phishing awareness, and the proper handling of sensitive information. Promote a culture of security awareness within the organisation.

6. Backup and Disaster Recovery: Regularly backup critical business data and establish a robust disaster recovery plan to ensure that business information can be restored in case of a data loss incident or breach.

7. Implement a Security Incident Response Plan: Develop and implement a well-defined incident response plan to effectively handle and respond to security incidents, minimising the impact on business operations and the loss of sensitive information.

10. Conclusion

In conclusion, the protection of business information is crucial for organisations to safeguard their valuable assets and maintain the trust of customers and stakeholders. Data breaches or security incidents can have a significant impact on the reputation of business organisations. These incidents can erode customer trust, result in financial losses, and damage brand reputation. Swift and transparent response, proactive security measures, and effective communication are crucial in mitigating the reputational damage caused by such incidents. By implementing strong access controls, regular system updates, encryption, and conducting security audits, businesses can enhance their cybersecurity posture. Employee training, backup and disaster recovery plans, and a well-defined incident response plan are also essential components of an effective information protection strategy. By adopting these measures and staying updated on the latest cybersecurity trends and threats, organisations can mitigate risks and protect their business information in an increasingly digital and interconnected world. The government of India has introduced several initiatives and policies to address the protection of business information. From formulating cybersecurity policies and establishing CERT-In to proposing data protection regulations, the government is actively working towards creating a secure digital ecosystem. Collaborative efforts between the government, industry, and individuals are essential to ensure effective protection of business information and mitigate cybersecurity risks in the country. Hence, the study of the protection of business information in India is crucial for organisations to navigate the complexities of the digital landscape and safeguard their sensitive data. By addressing the unique challenges posed by the digital economy, complying with data protection regulations, and promoting cybersecurity awareness, businesses can enhance their resilience against cyber threats and build trust with their stakeholders. As India continues its digital journey, prioritising the protection of business information is vital for sustainable growth and success.

11. Future Scope & Suggestions

1) Conduct sector-specific security assessments across different industries.
2) Explore AI-based predictive analytics for detecting potential data breaches.
3) Develop a standardized cybersecurity training curriculum for Indian SMEs.
4) Conduct longitudinal studies to evaluate the effectiveness of new Indian data protection laws.
5) Create a collaborative national database of business-related cyber incidents for better trend analysis.

Declarations

Source of Funding

This study received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing Interests Statement

The author has declared that no competing financial, professional, or personal interests exist.

Consent for publication

The author has consented to the publication of this research work.

Authors' contributions

Author's independent contribution.

Availability of data and materials

Supplementary information is available from the author upon reasonable request.

Institutional Review Board Statement

Not applicable for this study.

Informed Consent

All participants in this study voluntarily gave their informed consent prior to their involvement in the study.

Acknowledgments

The author acknowledges all involved parties in this study.

References

[1] Zubair, M., Ayub, M., Naseem, M., & Khan, A. (2024). Access control for trusted data sharing. EURASIP J. Inf. Secur., 2024(1): 1–15. https://doi.org/10.1186/s13635-024-00178-z.

[2] Razi, Q., Singh, A., & Kumar, V. (2025). A comprehensive survey of privacy-enabling technologies. Comput. Secur., 130(1): 102987. https://doi.org/10.1016/j.cose.2024.102987.

[3] Punia, A., Singh, R., Girdhar, A., & Sharma, P. (2024). A systematic review on blockchain-based access control mechanisms. J. Cloud Comput., 13(1): 12–32. https://doi.org/10.1186/s13677-024-00697-7.

[4] Wang, Y., & Chen, H. (2020). Influence of cybersecurity training programs on employee behavior in corporate environments. Am. J. Comput. Eng., 7(2): 14–26. https://doi.org/10.47672/ajce.1906.

[5] Joint Task Force (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev 5). Natl. Inst. Stand. Technol. https://doi.org/10.6028/nist.sp.800-53r5.

[6] Gkioulos, V., Apostolopoulos, T., & Tzovaras, D. (2023). A systematic review of current cybersecurity training methods. Comput. Secur., 131: 103372. https://doi.org/10.1016/j.cose.2023.103372.

[7] Zafar, M., Naseer, A., & Zhou, L. (2025). A systematic review of multi-factor authentication in digital payment systems. J. Netw. Comput. Appl., 222: 103921. https://doi.org/10.1016/j.jnca.2025.103921.

[8] Kashyap, A.K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. Law Saf., 89(2): 207–216. https://doi.org/10.32631/pb.2023.2.19.

[9] Pool, J., & Hulsbosch, M. (2024). A systematic analysis of failures in protecting personal data. Comput. Secur., 133: 103847. https://doi.org/10.1016/j.cose.2024.103847.

[10] Jada, I., Ahmed, A., & Ball, E.F. (2024). The impact of artificial intelligence on organizational cyber resilience. Comput. Secur., 134: 103950. https://doi.org/10.1016/j.cose.2024.103950.

[11] Kuipers, S.L., & van Woensel, T. (2022). Data breaches and effective crisis communication. Crisis Manag. Stud., Leiden University. https://scholarlypublications.universiteitleiden.nl/access/item:3213796/download.

[12] Golightly, L., Singh, R., & Malik, S. (2023). Securing distributed systems: A survey on access control. J. Secur. Privacy, 55: 387–432. https://doi.org/10.1016/j.cose.2023.103385.

[13] Babbar, G. (2020). Framework and methodological solutions for cyber security in Industry 4.0. SSRN Electron. J. https://doi.org/10.2139/ssrn.3601513.

[14] Pursuit Editorial (2023). Data protection and data privacy. Pursuit, 9th Edition. https://cag.gov.in/uploads/icisa_resources/pursuit-9th-edition-0676a48f6b8c7a4-87699484.pdf.

[15] Chia, P., & Fink, J. (2022). Critical success factors for security education, training and awareness (SETA). Inf. Comput. Secur., 30(4): 552–569. https://doi.org/10.1108/ics-08-2022-0133.