sdmimd

Shri Dharmasthala Manjunatheshwara Institute for Management Development, Mysuru, India

7th International Conference on “Technology and Transformation in Marketing: Advancing Purpose, Performance, and Personalisation for Impact“, on 23rd January 2026.

Technology and Transformation in Marketing: Effective Feedback

G.S. Umadevi
Assistant Professor
Department of Commerce
St. Joseph’s First Grade College
Mysore
gadidasuumadevi@gmail.com

Chandrakala N
Assistant Professor
Department of Commerce
St. Josephs' First Grade College
Jayalakshmipuram, Mysore
chandrikan2291@gmail.com

Abstract

Technology has affected marketing to a great extent, leaving an imprint on market research, data collection, and the promotion of new products. However, significant issues have arisen regarding data protection and the trust customers repose in brands. It is critical to examine whether brands can retain consumer faith regarding services and data safety. This paper questions if there is an immediate cost to companies when data breaches occur and analyses the laws available to protect stakeholders.

***Keywords**: Marketing, Technology, Feedback, Data Breach, Cybersecurity*

Introduction

The rapid advancement of digital technologies has fundamentally transformed marketing by enabling businesses to gather and analyze vast quantities of consumer information for personalized engagement and strategic decision-making. While such capabilities have enhanced market reach and operational efficiency, they have also heightened concerns about data security, privacy, and the erosion of customer trust when personal information is compromised.

Data breaches, in particular, can severely undermine customer confidence and loyalty, making robust protection mechanisms essential in the digital marketing domain. In India, the enactment of the Digital Personal Data Protection Act, 2023, and the subsequent Digital Personal Data Protection Rules, 2025, has established a comprehensive legal framework. This framework mandates secure data handling, timely breach reporting, and adherence to principles such as consent, purpose limitation, and accountability to protect individuals’ personal data. Compliance with these laws, combined with stringent cybersecurity measures—such as encryption, access control, regular audits, and incident response planning—can mitigate the risks of data breaches and reinforce customer trust in digital marketing practices.

Objectives

The primary objectives of this study are:

1. To analyze the impact of data breaches on various stakeholders.
2. To identify effective methods for preventing and mitigating data breaches.
3. To study the existing legal measures for data breach protection in India.

Methodology

This research is based on secondary data collected from various sources, including academic journals, industry reports, and case studies regarding recent cybersecurity incidents.

Case Studies: Data Breaches in 2024

This paper examines three significant companies that experienced data breaches in 2024 to understand the nature and impact of such incidents.

boAt

In April 2024, the Indian consumer electronics company boAt experienced a significant data exposure incident that reportedly affected the personal information of over seven million users. The breach was attributed to a threat actor operating under the alias “Shopify Guy,” who allegedly offered the compromised dataset for sale at a minimal cost. This facilitated its rapid circulation across dark web forums and social media platforms. The exposed data, estimated to be approximately 2 GB in size, was disclosed on a widely known cybercrime platform.

boAt acknowledged the incident and initiated an internal investigation, publicly sharing the findings. However, the company did not conclusively determine whether the breach originated from internal systems or a third-party service provider. Such data exposures present serious risks, including unauthorized access to financial accounts, fraudulent transactions, and misuse of payment instruments. Although boAt did not immediately issue a formal breach notification, it later published advisory communications recommending preventive measures for users, such as updating passwords and enabling multi-factor authentication.

HDFC Life Insurance

Between November 19 and 21, 2024, HDFC Life Insurance was reportedly subjected to a cyber intrusion where threat actors alleged unauthorized access to confidential customer information. To substantiate their claims, the attackers released sample data that purportedly included policy identification numbers, customer names, residential addresses, contact details, and sensitive health-related information of policyholders. The perpetrators communicated extortion demands through email and WhatsApp and threatened to publicly disclose the compromised data if demands were not met.

In response, HDFC Life formally reported the matter to the South Region Cyber Police, leading to the registration of a case under the provisions of the Bharatiya Nyaya Sanhita and the Information Technology Act. This breach poses serious risks to affected customers, including identity theft and the erosion of personal privacy due to the disclosure of medical information. Following the incident, HDFC Life engaged external cybersecurity specialists to assess the breach and strengthen its security posture.

Bharat Sanchar Nigam Limited (BSNL)

The data breach involving BSNL was initially reported by the Indian cybersecurity firm Athenian Tech.

The incident was attributed to a threat actor using the alias “kiberphant0m,” who claimed responsibility for leaking a substantial volume of sensitive telecommunications data affecting millions of subscribers. The compromised information reportedly included International Mobile Subscriber Identity (IMSI) numbers, SIM-related records, Home

Location Register (HLR) data, and screenshots of BSNL’s SOLARIS server infrastructure.

The actor claimed that approximately 278 GB of confidential information had been exposed and offered the data for sale for USD 5,000. Leaked call detail records revealed subscriber mobile numbers, call dates, durations, and associated charges. The nature of the exposed information poses significant security risks, such as SIM cloning and communication interception. This incident highlights the escalating cybersecurity vulnerabilities within India's telecommunications sector and the critical need for robust security controls.

Data Breach Prevention

In the Indian cybersecurity landscape, effective defense against data breaches requires alignment with both technical safeguards and regulatory frameworks such as the Digital Personal Data Protection (DPDP) Act, 2023, and CERT-In guidelines.

Organizations must enforce strong identity and access management practices, including multi-factor authentication (MFA) and role-based authorization, to prevent unauthorized data exposure. Regular security audits, timely patch management, and vulnerability assessments are critical in addressing system weaknesses commonly exploited in large-scale breaches.

Furthermore, encrypting personal and sensitive data during storage and transmission reduces the severity of breaches by limiting data misuse.

Continuous monitoring, threat intelligence sharing, and well-defined incident response mechanisms enable early detection and rapid containment of cyber incidents. Additionally, strengthening employee cybersecurity awareness helps mitigate risks arising from phishing, credential theft, and third-party vulnerabilities, which have been significant contributors to recent data breaches in India.

Evolving Legal Measures to Prevent Data Breaches (Up to 2025)

India's approach to regulating data protection continues to evolve, emphasizing compliance, accountability, and digital trust. Foundational legal instruments include the Information Technology Act, 2000, and the IT Rules of 2011, which impose obligations on organizations to deploy reasonable security practices.

A key milestone is the Digital Personal Data Protection (DPDP) Act, 2023, which introduced consent-driven data processing, mandatory breach reporting, penalties for non-compliance, and the establishment of a Data Protection Board. By 2025, the implementation roadmap for the DPDP Act has brought new operational obligations, including data fiduciary classification and cross-border data rules. Further regulatory strengthening has occurred through CERT-In directives mandating tighter cybersecurity reporting timelines. Collectively, these measures illustrate India's transition toward a comprehensive data protection architecture aligning with global standards.

Conclusion

Data breaches pose a growing threat to organizations and individuals, particularly in data- intensive sectors such as insurance and telecommunications. These incidents can lead to a loss of customer trust, legal consequences, and reputational damage. To reduce these risks, companies must apply strong encryption to protect customer data and regularly perform cybersecurity audits, vulnerability assessments, and penetration testing.

Preventing such incidents requires a multi-layered cybersecurity approach that includes robust access controls, employee awareness training, and continuous monitoring of network activity. Equally important is adherence to India's legal and regulatory framework, including the Information Technology Act, 2000, and the Digital Personal Data Protection Act, 2023. Effective implementation of these laws, coupled with timely incident reporting and regulatory oversight, can significantly reduce the impact of data breaches and enhance public trust in digital systems.

References

https://economictimes.indiatimes.com/industry/cons-products/electronics/boat-data- breach-name-address-contact-number-email-id-of-75-lakh-boat-customers-reportedly- leaked-

online/articleshow/109127405.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst .https://www.dlapiperdataprotection.com/?t=law&c=IN