International Journal of Innovative Research in Management Studies (IJIRMS)
Volume 8, Issue 3, March 2026. pp.57-61.

IMPACT OF DATA BREACHES ON CONSUMER TRUST AND BRAND REPUTATION

Manoj S S[1], Dr. Dhakshayini K N[2]

[1]*Research Scholar, University of Mysore & SJB College of Management Studies, Bengaluru.*
Email ID: manu39kgf@gmail.com

[2]*Research Guide, University of Mysore & SJB College of Management Studies, Bengaluru*

Abstract—*In the developed technology, its big concern to protect consumer personal data. A data breach happens when people without permission get into company's networks, or databases to access personal data/information. The stolen information can be things like personal details, money records, etc. The advancement in the technology makes a person to hack the data easily which are kept confidentially with the company. This makes a big concern to the company to retain the consumers after data breach and to react to the problem. This study aims to know about the consumers prospective about the companies trust and brand reputation when a data breach is occurred. The study also recommends some remedies which can help to overcome the data breaches. A mixed approach is used to collect the data and SPSS is used to analyze the data. The data is collected from 30 respondents and Likert scale is also used collect the data. The brand loyalty plays an important role in any company; consumer trust reduces after the crisis of data breach. A sustainable investment should be made by the company to protect the consumer personal information from crisis of data breach.*

Keywords: *Data Breach, Consumer Trust, Brand.*

Introduction

A data breach is a security incident in which unauthorized individuals access, disclose, or steal sensitive or confidential information. A data breach happens when people without permission get into computer systems, networks, or databases to access private information. The stolen information can be things like personal details, money records, inventions, or any other kinds of protected data that should not be in the wrong hands. The effects of a data breach can be really bad, such as losing money, damaging a company's reputation, facing legal problems, and causing harm to the people affected. This can happen to anyone, from regular individuals to small businesses and even big companies around the world. There are multiple technical reasons why data breaches happen. These include employees accidentally or on purpose sharing information, losing or having stolen devices that aren't encrypted, hackers breaking into a system by finding weaknesses in software, and social engineering attacks like phishing, where employees are tricked into giving away information.

The following are the types of data breach:

- Physical Breaches: It is a case where there is the illegal acquisition of the physical form of the devices or documents that hold sensitive information. It is necessary that organizations ensure that their physical environments are strictly secured to prevent such violations.
- Phishing: Phishing attacks are coordinated, in most cases, by the use of spam emails or messages that fool people by manipulating them to reveal confidential information such as passwords or credit card details or logins.
- Malware Attacks: An attacker can use malicious software to steal data or malfunction the system. This type includes other types of malwares, including viruses, spyware, and other malicious code.
- SQL Injection: SQL injection is an attack where attackers insert malicious SQL code into a database query, allowing them to access, modify, or delete database contents.
- Insider Threats: This is the threat where individual inside the organization misuse his access to cause a data breach.

The Digital Personal Data Protection Act, 2023 has been implemented in order to create a comprehensive system of protecting digital personal data. The Act is also following the SARAL model which is characterized as Simple, Accessible, Rational, and Actionable. In this act, a personal data breach is defined to be the unauthorized processing of personal data or the accidental disclosure, acquisition, sharing, usage, modification, destruction or loss of access to personal data, which compromises the confidentiality, integrity or availability of the data. The Act also compels data fiduciaries to put in place reasonable security measures in order to prevent such violations.

The Digital Personal Data Protection Rules, 2025, are an addition to the Act as they provide the operational guidelines. The latter Rules stipulate that data fiduciaries must notify the Data Protection Board and affected data principals about the breach as soon as it has occurred and provide detailed information about the incident and the corrective actions that have been taken. Together, the Act and its Rules will build a functional, innovation-oriented data protection ecosystem that is more user-friendly and friendly to compliance to promote the trust of the people in the growing digital environment of the country.

Review of Literature

Iyer, M., Banerjee, A. (2025). Data breaches lead to immediate declines in consumer trust, particularly when sensitive information is involved. The consequences extend beyond immediate financial losses, leading to identity theft, psychological distress, undermining consumer confidence, reducing platform usage, and causing long-term reputational damage. Rebuilding lost trust is challenging and expensive. Measures like credit monitoring, refunds, or identity protection services signals a commitment to user welfare and can help mitigate trust damage.

Yadav, D. T. C., Kala, K., Kolachina, R. I. R., Kanneganti, M. C., & Pasupuleti, S. S. (2024). Consumers concern about their data privacy increase, their trust in brands and digital marketing practices tends to decrease. Transparency in data practices and regulatory compliance (GDPR, CCPA) were identified as critical factors influencing consumer trust. Brands that are open and clear about how they collect, use, and share consumer data are more likely to gain trust. Key privacy issues identified include over-collection, lack of transparency, unauthorized sharing, and data breaches.

Ferdyan Putri, Z. Q., & Efawati, Y. (2025). The study aimed to investigate how customer data security affects consumer trust in Gojek's digital services. Analysis revealed that approximately 38.3% of consumer trust in Gojek services is influenced by customer data security factors. The remaining 61.7% of consumer trust levels are influenced by other factors not tested in this study, such as service quality and user experience. To maintain consumer trust, it is important to develop a holistic approach by considering other aspects such as service quality, response speed, and feature innovation.

Strzelecki, A., & Rizun, M. (2022). The study found that consumers' trust towards the Morele.net online store significantly decreased after the personal data breach incident. Consumers have become significantly more aware of the importance of personal data security following the breach, leading to a change in their attitudes towards sharing personal information online. The study highlights that the incident has resulted in a strong decrease in consumer trust towards Morele.net, indicating a need for the store to implement improvements to regain this trust.

Kaushal J. (2025). The study identifies fraudulent practices in India's coaching industry, including fake advertisements, fabricated rankings, bot-generated reviews, and coerced testimonials. There is a predominance of negative feedback concerning the services offered by coaching institutes. Psychological biases such as the bandwagon effect, halo effect, and fear of missing out (FOMO) are exploited to mislead consumers and exaggerate success claims.

Varma, M., Kumar, V., Sangvikar, B., & Pawar, A. (2020). The primary objective of the research paper is to explore the factors influencing customer buying intention through electronic commerce in India. Privacy, trust, security, and organization's reputation significantly affect online purchase intention. It is emphasized through the study that the higher the value of goods needs, the higher the level of trust. Trust is the most significant factor, the study indicates that there is lack of trust in online commerce.

Research Methodology

A mixed method of research i.e., both quantitative and qualitative data is used to analysis the data. The research involves collection of data from individual through structured questionnaires, circulated through online forms and responses are obtained. SPSS (Statistical Package for the Social Sciences) software is used to analysis and interpret the data.

Objectives

- To analyze the relation between data breach severity and the decline in consumer trust.
- To understand how consumers react to the brand which is data breach.

- To identify the key drivers of "brand recovery" post-breach.

Analysis

It was noted that large set of population i.e., 43.3% have responded that only sometimes they will read the privacy policies before sharing their personal data with the company. By this response we will say that the consumers will read the policies only when they perceive a higher risk, such as when dealing with financial data or an unfamiliar brand. Interestingly 26.7% of respondents claim that they always read the policies. And nearly 30% of the population will rarely/never read the policies, by which we can conclude that this category blindly trusts the brand.

By comparing age with the comfortable they are with the digital technology: It was seen that half of the respondent are youngsters who are highly comfortable to use the digital technology. When it comes to mid-range age group (around 50) they have rated themselves as 5 and below. There is gap that aged people may fail to understand the digital technology.

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
I feel my personal information is safe when shopping online.	30	1	5	2.83	1.262
A single data breach would make me stop using a brand permanently.	30	1	5	3.20	1.324
I trust large corporations more than small businesses to handle my data.	30	1	5	2.97	1.402
I am more likely to trust a company if they are transparent about a breach immediately.	30	1	5	3.53	1.042
Valid N (listwise)	30				

1. I feel my personal information is safe when shopping online: Most of the respondents don't feel safe about their personal data while shopping online. This because the Mean is below the midpoint ($\bar{x}$=2.83), this indicates a sloping to disagreement. This shows low baseline trust and security.
2. A single data breach would make me stop using a brand permanently: The mean of 3.20 reveals a threat for companies because it shows there is a moderate respond that a single data breach may result in leaving the brand. Nevertheless, with Standard deviation 1.324 indicates that some are forgiving and continuing with brand and others are strict. This shows there is a high volatility in brand loyalty.
3. I trust large corporations more than small businesses to handle my data: A Mean of 2.97 points out that the respondents do not see whether the company is big or small, it only depends on the security handling techniques followed by the company.
4. I am more likely to trust a company if they are transparent about a breach immediately: The mean score of 3.53 suggest consumers value honesty. Even if a breach occurs, being "transparent immediately" is the most effective way to retain or rebuild trust. Even the Standard deviation 1.042 lowest here, suggest that most of the respondents agree on the same point. This suggest Transparency is the best policy.

The most of the respondents (i.e., 43.3%) sees the data breach as the failure of the firm's technical capabilities. This says that data security is seen as the core competency for a company and a failure in data security is lack of professional diligence. 36.7% of respondents view the brand as "dishonest or secretive" following a data breach.

50% of the respondents has identified that "The company delaying the announcement of the breach" as the most damaging factor to their trust. This suggest that consumers value honesty and timely communication over the technical perfection of the brand. 40% feels that the breach is the main reason to loss the trust on the brand because they feel that the company do not keep up with the promise of security to the consumer data. Consumers expect a brand to take full responsibility for its ecosystem; shifting blame to partners or vendors is seen as equally damaging as the security failure itself.

If the most loved brand suffers from a data breach, then most of the respondents will not refer/recommend the brand to others. This may be big loss to the company as the new consumers may be reduced and even the existing consumers may leave the brand.

The responses say that if a breach is occurred then 50% of the respondents have choice that they will delete their account/ stop using the service. And demand for their financial compensation. And 33.3% responded that they will change the password but continue using the service. This set of respondents represents that whatever happen they trust the brand and they are the main asset to the company.

Conclusion

The biggest data breach in India occurred in the early 2018 with the Aadhar. Unique Identification Authority of India (UIDAI) was managing the data base where 1.1 billion persons data was leaked. This data breach exposed name, address, biometric, bank account details. And this data was sold online openly for ₹500. Investigation showed that this breach occurred due to poor API and poor access control. To prevent data, they enforced strict access controls and endpoint security protocols, ensuring secure API management and regular audits.

1. It is statistically probable that as age increases in this specific sample, comfort levels begin to fluctuate or decrease, resulting in the "moderate" scores seen in the middle of the scale and young people will have be more comfortable with the new technology as well.
2. 43.3% of the population says that they sometimes only read the privacy policy and 26.7% says that they always read the policy because they may not trust the brand or the technology they deal with.
3. 23.3% have been notified that their personal data was involved in a data breach.
4. Nearly half of the population believe that the Company/Organization are the primarily responsible for protection of the consumer data.
5. The research data indicates that consumers never tend to consider data breaches as inevitable external offences. Rather, 43.3% of the sample associate’s security failures with technical incompetence, and 36.7% perceives them as a violation of the ethical transparency. It means that brand equity and consumer trust are central to modern brands, and cybersecurity is no longer a focal point of IT concerns.
6. The management of the crisis is more impact on brand then the crisis itself. If the company delay the notification of breach, then it leads to trust damaging factor. The timely responses to the consumers will increase the trust on the company. Blaming third party is unacceptable, the company should that the full responsibility of the breach and fix it.
7. The company should take multiple security steps to secure their consumer data and protect it from breach because the study found that if breach is accorded then most of the consumers may leave the brand and stop using their services and they even demand for compensation for their financial loss borne by the consumer.

The key drivers from brand recovery after breach are:

- Disclose immediately and clearly what has happen in the public.
- Regularly update about the things and what data has been breached.
- Improve cybersecurity protocols.
- Rebuild thrust through regular engagement with the consumers, shareholders.

The following are the activities which can be followed by organization to prevent from data breach:

- Mandatory Multi-Factor Authentication for all users.
- Use “Principle of Least Privilege” where only limited access is granted to the lower level of employee.
- Never trust any person, always verify persons who handle the data.
- Data loss prevention (DLP) tool should be used for sensitive data.
- Encrypt all data.
- Application Programming Interfaces (APIs) should be used from unauthorized access, misuse, and cyber threats.

The following are the prevention activities which can be used by consumer from data breach:

- Use a strong password for your account.

- Secure your mail account.
- Do not save your card details in any website.
- Avoid using public USB Port.
- Avoid using public Wi-Fi networks.
- Do not open any message link.
- Report any financial frauds as soon as you get to know.

References

[1] Iyer, M., Banerjee, A. (2025). Impact of Data Breaches on Consumer Trust in Digital Platforms. Journal of Cyber Risk and Digital Trust. 1(3), 69–75.
https://admin.mantechpublications.com/index.php/JCRDT/article/view/2760/1294

[2] Yadav, D. T. C., Kala, K., Kolachina, R. I. R., Kanneganti, M. C., & Pasupuleti, S. S. (2024). Data Privacy Concerns and their Impact on Consumer Trust in Digital Marketing. Interantional Journal of Scientific Research in Engineering and Management, 08(11), 1–7. https://doi.org/10.55041/ijsrem38555

[3] Ferdyan Putri, Z. Q., & Efawati, Y. (2025). Exploring the Impact of Customer Data Security on Consumer Trust in Gojek's Digital Services. International Journal Administration, Business & Organization, 6(1), 136–145. https://doi.org/10.61242/ijabo.25.332

[4] Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. Sustainability (Switzerland), 14(10). https://doi.org/10.3390/su14105866

[5] Kaushal J. (2025). Digital Deception and Consumer Trust in India's Coaching Industry Unveiling Fake Reviews, Psychological Biases, and Regulatory Gaps. 0–14. https://doi.org/10.20944/preprints202509.0127.v1

[6] Varma, M., Kumar, V., Sangvikar, B., & Pawar, A. (2020). Impact of social media, security risks and reputation of e-retailer on consumer buying intentions through trust in online buying: a structural equation modeling approach. 7(1), 119–127. http://www.jcreview.com/?mno=302645201

Websites

https://www.forbes.com/advisor/business/what-is-data-breach/

https://relevantcompliance.com/types-of-data-breaches/

https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc20251117695301.pdf

https://igap.in/wp-content/uploads/2024/12/IGAP_DPDP-Report-Part-I_Dec2024.pdf

https://www.corbado.com/blog/data-breaches-India

Annexure

https://docs.google.com/forms/d/e/1FAIpQLScK0WYWy2eU7Bu2dYX8xuqcxfHNYcJ1tORZrd8sMhSygS7xsw/viewform?usp=header

*****