Data breaches in India and Europe. A Comparative study

Author – Subhashree.K, Co- Author – Venkatraman.N
5th year, B.Com L.L.B. (hons)
Subhashree.K
B.Com., L.L.B. (hons), SASTRA Deemed to be University, Thanjavur, India

Abstract

This paper deals with data breaches in network security against advanced hacking techniques. So. In today's world hacking has become a major threat to economy. Thus the problem of protecting information and data flows has existed from the very first day of information exchange. Various approaches have been devised to protect and transfer such information securely. However, as technology and communications advance and information management systems become more and more powerful and distributed, the problem has been taken on new and more complex dimensions and has become a major challenge. The widespread use of wired and wireless communication networks, internet, web applications and computing has increased the gravity of the problem. Organizations are totally dependent on reliable, secure and fault tolerant systems, communications, applications and information basis. Unfortunately, serious security and privacy breaches still occur every day, creating an absolute necessity to provide secure and safe information security systems through the use of firewalls, encryption, authentication and other hardware and software solutions. This paper aims to address these issues and also the legal framework of how this is related to cyber law and A multiple case study approach is applied to this study, using secondary data from the case studies of British airways (2018) and air India breach (2021)

KEYWORDS : DATA BREACH, NETWORK SECURITY, INDIA,EU, COMPARITIVE STUDY

Introduction

Incidents involving the acquisition, disclosure, or unauthorised access of confidential data are known as data breaches. Financial information, login credentials, names, addresses, social security numbers, and other personally identifiable information are examples of personal data that falls under the category of sensitive information. There are many different contexts in which data breaches can happen, including companies, governmental organizations, academic institutions, healthcare facilities, and even individual devices or internet platforms. The impacted parties, organizations, and the general public's confidence in the security of digital systems may all suffer significantly as a result. Any crime involving a computer or network is included under the umbrella term of cybercrime. Identity theft, fraud, hacking, and data breaches are examples of cybercrimes. Because it is a rich source of financial and personal data, the healthcare business is a prominent target for hackers. More and more individuals are using digital media to manage their daily lives thanks to the internet, mobile phones, and a plethora of other new information technology. Additionally, even those who do not use technology frequently are monitored, tracked, and electronically surveyed, providing information on their attitudes, habits, and other aspects of their lives.

Numerous provisions of the EU's GDPR are included in the proposed law, currently known as the Personal Data Protection Act, which went into effect. These include constraints to guarantee that only information required for offering a service to the individual in question is gathered, limitations on the reasons for which corporations may use data, and requirements for notification and prior consent for the use of individual data. It also covers the necessity for data localization and the designation of data protection officers inside businesses. The Act offers India a thorough, cross-sectoral framework for data protection and privacy.

A lot of such activities necessitate disclosing personal information, including emailing, social networking, banking, shopping, and e-government. Online data that people or businesses retain might include sensitive personal data including bank and credit card account details, email or mailing addresses, passwords, and login credentials. More information is kept on servers as more activities move online. The protection of data security and privacy is complicated by this circumstance. Organizations must improve their security and privacy programs in order to prevent future occurrences and to ensure responsibility, in order to survive a data breach and mitigate its bad repercussions. Our study employs a multiple case study methodology based on two recent data breaches, in both India and Europe, to determine what viable practices could aid firms in recovering from data breaches.

Methodology

Through an analysis of well-known case studies, the research methodology compares data breaches in two different regions: Europe and India. The selection criteria for these cases consist of their severity, representativeness, and accessibility to extensive data. To obtain comprehensive information on the selected data breach instances, a thorough examination of official reports, cybersecurity databases, and reliable news sources would be the first step in the data collection process. The comparative analysis will concentrate on each nation's regulatory framework, reaction methods, types of compromised data, and attack routes. We'll use qualitative analysis to find trends, distinctions, and possible linkages. Through an analysis of well-known case studies, the research methodology compares data breaches in two different regions: Europe and India. The selection criteria for these cases consist of their severity, representativeness, and accessibility to extensive data. To obtain comprehensive information on the selected data breach instances, a thorough examination of official reports, cybersecurity databases, and reliable news sources would be the first step in the data collection process. The comparative analysis will concentrate on each nation's regulatory framework, reaction methods, types of compromised data, and attack routes. We'll use qualitative analysis to find trends, distinctions, and possible linkages.

What is known as Data breach

Any unauthorized acquisition, disclosure, alteration, or access to private, sensitive information that is owned by an organization is referred to as a data breach. Given the increasing reliance on digital technologies and the volume of personal and corporate data being processed, data breaches have become major concerns in the contexts of Europe and India. The incidents range from poorly configured system security to the irresponsible disposal of outdated computers or data storage media, to coordinated hacking attacks by malevolent individuals or groups (black hats), organized crime, political activists, or national governments. Information about actions that a government official finds embarrassing and tries to conceal could be exposed through leaks, endangering national security. Data breaches may expose intellectual property, trade secrets, or personally identifiable information (PII). Sensitive documents, files, and other unstructured data may also be vulnerable to data breaches.

In India, Unauthorized access to databases, networks, or other systems can compromise sensitive information, including financial records, intellectual property, or personal data. We call these kinds of things "data breaches." Cybercriminals use a range of tactics, including phishing, malware attacks, and system vulnerabilities, to take advantage of weaknesses in security protocols. In India, data breaches can have detrimental effects on one's reputation, finances, and possibly even legal action. The Personal Data Protection Act (PDPB) is altering the regulatory environment. It was passed with the intention of establishing comprehensive data protection guidelines and enforcing stricter penalties for noncompliance.

In Europe, The General Data Protection Regulation (GDPR), a strong framework created to safeguard people's right to privacy and guarantee that businesses handle data responsibly, governs data breaches in Europe. According to GDPR, an organization is required to report an incident of unauthorized access or accidental loss of personal data as soon as possible. GDPR imposes strict guidelines on data protection, which include putting security measures in place, designating Data Protection Officers (DPOs), and notifying affected parties and supervisory authorities in the event of a breach. Strong cybersecurity measures are crucial since noncompliance with GDPR may result in hefty fines.

Types of data Breaches (Geetha & Robin, 2021)

Data breaches are frequently planned using a range of complex techniques that take advantage of holes in networks and systems. It is imperative for organizations to comprehend these strategies in order to execute efficacious cybersecurity protocols. These are five typical methods that lead to data breaches.

Phishing Attacks:
Description: Phishing is still a common technique used by cybercriminals to trick people into disclosing sensitive information like login passwords or bank account information. Phishing emails, messages, or websites are deceptive.

Modus Operandi: Attackers create believable messages that seem authentic, frequently imitating respectable companies or associates. Information that recipients unintentionally give is used to gain unauthorized access.

Malware Infections:
Description: Malicious software, also known as malware, is used to infiltrate networks and pilfer confidential information. Ransomware, Trojan horses, and other malicious software fall under this category.
Modus Operandi: By means of compromised software, email attachments, or infected websites, cybercriminals propagate malware. Malware can spy on users, steal information, and lock files for ransom once it has gained access to a machine.

Insider Threats:
Description: Insider threats are people who work for a company, such as contractors or employees, and who may purposefully or inadvertently jeopardize data security.
Modus Operandi: Insiders with malicious intent may use their access privileges to steal or divulge confidential information. Human error can lead to accidental breaches, such as incorrectly configured settings or inadvertent data exposure.

Third-Party Vulnerabilities:
Description: For a variety of tasks, many businesses depend on outside suppliers or service providers. On the other hand, it is possible to obtain sensitive data without authorization by taking advantage of flaws in these outside sources.
Modus Operandi: Cybercriminals look for holes in third-party vendors' security protocols, which they then take advantage of to breach the network or systems of the company.

Advanced Persistent Threats (APTs):
Description: APTs are long-term, focused cyberattacks that are planned and carried out by highly skilled and well-funded threat actors, frequently with particular goals in mind, like stealing intellectual property or conducting espionage.

Modus Operandi: APTs usually consist of several phases, such as the initial infiltration, presence establishment, and long-term data exfiltration. Attackers frequently use cutting-edge strategies to evade discovery.

What is Cybercrime?
Cybercrime is the attempt to commit unlawful acts via a computer or the internet. They may wish to play tricks to make things go wrong or steal sensitive data, such as passwords or photos of you and your family. Let's say you have a favorite online game that you enjoy playing. It is possible for a cybercriminal to enter your game covertly, pose as you, and steal any and all of your collected treasures or points. It's like when someone tries to use your toys for play without permission!

Developing effective cybersecurity strategies in India and Europe requires an understanding of the nature of cybercrime and the legislative responses to it. The Personal Data Protection Bill (PDPB) was passed by India in response to a changing regulatory environment.

Cybercrime in India:
India has seen a rise in cybercrime incidents due to its economy, which is rapidly becoming more digital. These offenses include identity theft, financial fraud, data breaches, and online harassment. Several notable challenges included the absence of comprehensive data protection laws, disparities in awareness, and the lack of strong cybersecurity measures.
To address these issues, the Personal Data Protection Bill (PDPB) of 2023 is a historic legislative initiative. In line with international standards, the PDPB aims to create a thorough framework for the protection of personal data. The law gives people control over their personal data and places duties on organizations that handle it.

Types of Cybercrimes in India:
Financial Fraud:
Description: Cybercriminals use a variety of tactics, like phishing and online scams, to trick people out of their money.
Impact: Financial fraud directly endangers people and companies by causing losses and compromising bank information..

Identity Theft:
Description: Identity theft is a common way for criminals to obtain financial advantage or carry out other illegal activities.
Impact: Identity theft victims may experience financial losses, reputational harm, and legal repercussions**..**

Data Breaches:
Description: unauthorized access to sensitive data that exposes private and sensitive information, frequently as a result of malware or hacking.
Impact: Data breaches can have serious repercussions, such as compromised privacy, monetary losses, and reputational harm to an organization.

Cyberbullying and Online Harassment:
Description: Online harassment or bullying, frequently via messaging apps or social media sites.
Impact: Cyberbullying can lead to extreme cases of physical harm or suicide, as well as emotional distress and mental health problems.

Ransomware Attacks:
Description: Files belonging to a victim are encrypted by malicious software, which then demands a ransom to unlock.
Impact: Ransomware attacks have the potential to destroy companies, erase data, and have financial repercussions if the ransom is paid.

Cybercrime in Europe:
Despite having a strong technological infrastructure, Europe is not immune to the global cybercrime surge. The General Data Protection Regulation (GDPR), which went into effect in 2018, has had a big impact on how European nations handle cybersecurity and data protection. GDPR lays out strict guidelines for processing personal data, placing a strong emphasis on accountability, transparency, and individual rights.

Types of Cybercrimes in Europe:
GDPR Violations:
Description: Non-compliance with GDPR's regulations pertaining to data protection, such as insufficient security protocols, unapproved data processing, and tardiness in reporting data breaches.
Impact: GDPR infractions can cost businesses dearly in fines, legal repercussions, and harm to their reputation**.**

Phishing and Social Engineering:
Description: attempts to use phony emails or messages to trick people or employees into divulging sensitive information.
Impact: Financial fraud, data breaches, and unauthorized access to systems can all result from phishing.

State-Sponsored Cyber Espionage:
Description: Nation-states engaging in covert cyber operations to obtain unauthorized access to private data for military, political, or economic objectives.
Impact: Cyber espionage supported by the state can have serious repercussions, including jeopardizing economic and national security.

Financial Cybercrimes:
Description: sophisticated financial crimes, such as crimes involving cryptocurrencies, payment card fraud, and online banking fraud.
Impact: Financial cybercrimes have the potential to cause both individuals and financial institutions to suffer large financial losses..

Distributed Denial of Service (DDoS) Attacks:
Description: flooding a targeted system or network with so much traffic that it becomes inoperable either permanently or temporarily.
Impact: DDoS attacks have the potential to interfere with online services, costing businesses money and harming their reputations..

Malicious Activity Data:

Cybersecurity experts use malicious activity data, which is a broad category of information, to identify, evaluate, and address possible threats. Numerous sources, such as network logs, system alerts, antivirus programs, intrusion detection systems, and threat intelligence feeds, can provide this information. It offers information about the tricks, methods, and practices (TTPs) that online fraudsters use.

Types of Malicious Activity Data:

Network Traffic Patterns:

Description: Finding odd or suspicious activity, such as an abrupt spike in data transfers or connections to known malicious servers, can be aided by analyzing patterns in network traffic.

Example: Unusual increases in a particular user's or device's data traffic could be a sign of a possible network breach.

Anomaly Detection:

Description: Potential security risks can be found by keeping an eye out for irregularities in user behavior, system performance, or application usage. Examples include peculiar login times or unexpected data access patterns.

Example: An anomaly detection system may identify a specific user's unusual access locations or erratic login times..

System Logs:

Description: System logs keep track of network and computer activity. These logs can be examined to look for indications of suspicious activity, system problems, or unwanted access.

Example: An abrupt rise in unsuccessful login attempts in log files could indicate that user accounts are being brute-forced attacked.

Endpoint Security Data:

Description: Data is gathered from individual devices, or endpoints, in order to identify and stop malware, illegal access, or anomalous activity on particular devices.

Example: EDR data may reveal a sharp rise in file modifications or the running of questionable processes on a particular device.

Firewall and Intrusion Detection/Prevention System (IDS/IPS) Logs:

Description: Information gleaned from firewall and IDS/IPS system data sheds light on attempts to compromise network security. It may contain details on connections that are permitted or prohibited as well as possible dangers.

Example: recording of the steps done, adjustments made, and knowledge gained while responding to a malware outbreak.

Anti-Virus and Anti-Malware Logs:

Description: Information about threats found, their kinds, and the steps taken to neutralize them can be found in the logs produced by antivirus and anti-malware programs.

Example: an antivirus alert stating that a known malware signature was found during a regular scan.

Types of Identifiable Information:

Malware Signatures:

Malicious activity data aids in the detection and blocking of these threats by recognizing the distinctive signatures or patterns of known malware.

IP Addresses and Domains:

Network traffic analysis can help block or monitor sources by identifying suspicious IP addresses or domains linked to malicious activity.

User Behavior Anomalies:

Unusual user behaviors, such as repeated unsuccessful login attempts, logins from strange locations, or irregular data access patterns, can be detected by malicious activity data.

System and Application Errors:
Errors in system or application behavior that are recorded in logs can be an indicator of possible security problems and help patch holes before they are used against you.

Command and Control (C2) Servers:
Finding communication between known C2 servers that hackers use can reveal attempts to take over compromised systems..

File and System Modifications:
Unauthorized modifications can be detected by keeping an eye on file and system change logs. These changes may be a sign of an attempted hack or security breach.

Login Attempts and Credentials:
Data on malicious activity can show trends in questionable login attempts, such as the use of hacked credentials or brute force attacks.

Comparative study

Air India breach case study 2021

The national airline of India, Air India, suffered a serious data breach in 2021 that impacted about 4.5 million passengers. Sensitive personal data, such as names, dates of birth, contact details, passport information, credit card information, and frequent flyer data, were exposed in the breach. The people who were impacted by the fraudulent transactions using the stolen data suffered greatly.

Background
Since its founding in 1947, Air India has represented India as its flag carrier. It has encountered several difficulties over the years, such as monetary difficulties, operational problems, and intense competition from private airlines. The airline underwent privatization in 2021, with the Tata Group obtaining a majority stake.

The Data Breach
Although the data breach happened between August 2011 and February 2021, it wasn't identified until that month. A cyberattack on SITA, a Swiss technology company that offers reservation and passenger processing systems to airlines globally, was the reason for the breach. Air India did not make the incident public until May 2021, despite receiving notification from SITA about the breach in February 2021.

SITA and Air India Data Breach

SITA is a technology company with its headquarters located in Switzerland that focuses on communications related to air travel and information technology. Since its founding, it has expanded to offer a variety of airline operating services, such as reservation systems and passenger processing, from its original membership of just 11 airlines. In an attempt to become a member of the Star Alliance, Air India signed a contract with SITA in 2017 to modernize its IT infrastructure. Air India was able to use a number of SITA services, including automated boarding control, baggage reconciliation, online booking, online booking engine, check-in capabilities, and frequent flyer programs, thanks to this partnership.

Impact of the Breach
Both the airline and its passengers were significantly impacted by the Air India data breach. In addition to causing financial losses and harming Air India's reputation, the breach prompted affected customers to file lawsuits. Due to its apparent incapacity to secure customer data and its tardy disclosure of the breach, the airline's credibility was damaged.

Lessons Learned
The Air India data breach was a sobering reminder of the value of data security and the necessity for businesses to put strong safeguards in place to protect client information. The event brought to light a number of areas in which Air India's data security procedures may have been strengthened, such as:

- Securing sensitive data with more robust security controls and encryption.

- Regularly carrying out penetration tests and security audits to find and fix vulnerabilities.

- Educating staff members on cybersecurity best practices and threats on a regular basis.

- Possessing an efficient incident response strategy in place to react to data breaches as soon as possible and lessen their effects.

Conclusion

One significant event that had far-reaching effects was the Air India data breach. The airline appointed a data protection officer to supervise its data privacy program and made improvements to its data security procedures. But the incident should serve as a lesson to all businesses that handle private client information. To safeguard their information assets and the privacy of their clients, businesses need to put a high priority on data security and take preventative action.

British airways case

Over 400,000 customers of British Airways (BA) were impacted by a significant data breach that occurred in 2018. Sensitive personal data, including names, addresses, passport information, and credit card numbers, were revealed by the hack. In addition to having a major effect on BA's operations and reputation, the incident served as a sobering reminder of how crucial data security is.

Background

One of the biggest airlines in the world, British Airways has a rich history of providing global customer service. The airline launched a digital transformation program as part of its modernization program in 2018. In order to improve its online booking and check-in procedures, BA has been investing in new technologies as part of this initiative.

The Data Breach

The period of the data breach was August 21, 2018, to September 5, 2018. Cybercriminals diverted consumer payments to a fraudulent website by taking advantage of a flaw in BA's booking system. The attackers were able to obtain the personal data of more than 400,000 clients as a consequence.

When BA learned about the breach in September 2018, the airline moved quickly to contain the damage and halt the attack. Nevertheless, the impacted customers' data had already been compromised.

Impact of the Breach

The airline was significantly impacted by the BA data breach. Customers who were harmed by the company's actions threatened to sue it. Financial losses were also incurred by BA as a result of the breach since it had to pay out compensation to impacted customers and put new security in place.

Apart from the harm to finances and reputation, the hack also affected BA's day-to-day operations. The incident caused disruptions to the airline's booking and check-in procedures, and it took several months for BA to fully recover.

Lessons Learned

1. The airline industry received a serious wake-up call from the BA data breach. The incident brought to light the significance of data security and the growing threat posed by cyberattacks. The breach taught BA several important lessons, including:
2. The necessity of robust cybersecurity measures
3. The significance of frequent penetration tests and security audits
4. The requirement for cybersecurity awareness training for staff members
5. The significance of having a response strategy in place for data breaches
6. To improve its cybersecurity posture and address these lessons, BA has taken action. The airline has made investments in new security technologies, put new security policies and procedures into place, and given staff members more security awareness training.

Conclusion

Although it was a significant setback for the airline, the BA data breach also acted as a catalyst for change. BA is now better prepared to protect the data of its customers because it has learned important lessons from the incident. The hack serves as a warning about the value of data security and the increasing danger of cyberattacks. Businesses need to take precautions to safeguard their data and the information of their clients as they depend more and more on technology.

Limitations and Future Research

Our work has limitations even though it makes use of secondary data for analyses that are comparable to those of earlier studies. First of all, since secondary sources were used to gather the data, it is possible that certain unreported details about each case were present and were not examined. Our second drawback was the quantity of case studies we employed. Two case studies, each with a different conclusion, were used. There could have been more case studies, but the significance of these two particular data breaches played a role in our decision to select them. Additionally, by selecting these two data breaches, it was possible to examine the trends between the cases and determine which ones had different outcomes.

In the event of a data breach, companies risk losing the trust of their customers, which could lead to them breaking off their business relationship with the organizations as well as switching to rival brands. Additionally, customer loyalty could be compromised. Organizations should come up with a compensation and recovery plan right away to make sure that customers don't feel alone and to win back their trust and keep them from switching brands.

Furthermore, businesses should intensify their efforts to strengthen their relationships with consumers by being more open about the circumstances surrounding the data breaches and the measures being taken to prevent them from happening in the future.

References

Guha and Indurkar (2020) described the typical areas where attacks have occurred and the increased likelihood of a data breach, as well as the categories of hackers and the types of attacks they use for various forms of cybercrime like financial fraud, cyberbullying,

phishing, and remote access along with preventive measures.

https://ijersonline.org/HTMLPaper.aspx?Journal=Research%20Journal%20of%20Engineering%20and%20Technology;PID=2020-11-2-16

Surviving Data Breaches: A Multiple Case Study Analysis Nithya Shankar and Zareef Mohammed

https://www.erudit.org/en/journals/jcim/2020-v23-n1-jcim05502/1071508ar.pdf?embed&ds_name=PDF

Bali (2007) used case studies to illustrate how data that is outsourced is more likely to be stolen and is less secure.

https://heinonline.org/HOL/Page?handle=hein.journals/tclj21&div=6&g_sent=1&casa_token=zbDRgQwzTl0AAAAA:1siB0NxsaCl7cQclM-Qi4p7vSDqFLzaupzhSMYfbOtwkUe850DzgWAoqKYnHVPKEJnt_sBj86w

Fathima and Ahmed (2013) analyzed the challenges encountered by corporations in protecting the data of their clients, workers, and other stakeholders and recommended adopting data prevention strategies

https://d1wqtxts1xzle7.cloudfront.net/81448039/paper1-libre.pdf?1646038380=&response-content-disposition=inline%3B+filename%3DMaking_Data_Breach_Prevention_a_Matter_o.pdf&Expires=1700076596&Signature=YJDrwBJK1CU-oMxijEcMYwyseLmim787-NjaLRkLZ2LhXjl0iRJLbpEiU3aBTrEUehSZLE1An0OV9C74qpv0ZCjDcccJ~xBm8N52kbgu3FQSioDdL2k1hFwdp3aWEZa0zgql71zUOYbGszffaJW~F1oVl~zyGX~~kAFw~r0KKgWtzF2Yf316XxQ03VJ2b4IOOfBZFqUFj23aP2l0hpT9GcCBgxpwMV7wy89n0cuGwCM3vBqHwKz4Xn2Z~KdYRXbsgMmqtAEouq38~2PAsI5mHZhGOLVujl4n-G1jS7~pV6qk0af9rTcxtabMmKKiXAhiJ8etkMjPnBeZ1dJ25Ogtpg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

AN ANALYSIS OF THE INCREASING CASES OF DATA BREACHES IN INDIA by SMRITHI SUKESH, DOREEN HEPHZIBAH MIRIAM D, C. R. RENE ROBIN

https://www.researchgate.net/publication/371769609_An_analysis_of_the_increasing_cases_of_data_breaches_in_india

EU GDPR and Indian Data Protection Bill: A comparative study Authored by: Poulomi Sen

https://deliverypdf.ssrn.com/delivery.php?ID=136001008002096091091083024004126026030075090031022078086027070076126108098095004120059099053118019039062124008004067104065122108080094021003088082081090124072064070032082080079094072119031106086090125107087108029079022093010087102031031001001068070114&EXT=pdf&INDEX=TRUE