From Exposure to Response: Understanding and Managing Data Breaches

Raja Irfan Ahmad

***Abstract:** As the amount of data available to individuals, businesses, and governments on the internet increases, this may lead to data misuse. As the data available on the internet is in a huge volume, making any strategy that may be real-time or we think is effective regarding stopping or minimising data breaches is impractical. For individuals and organisations alike, the primary issue in the digital era is data breaches, which can affect any data available online. This review paper examines patterns in data breaches and their effects across sectors worldwide, as well as mitigation methods. This review paper aims to advance understanding of data breaches by considering case studies and the existing literature, and by outlining essential techniques/measure to enhance data security.*

***Keywords:** Data Breach, Mitigation, Machine Learning, SPSS, Data Security, Personally Identifiable Information, Cybercriminals,*

Nomenclature:

CCPA: California Consumer Privacy Act
GDPR: General Data Protection Regulation
PII: Personally Identifiable Information
IDOR: Insecure Direct Object Reference
CERT: Computer Emergency Response Team
AIIMS: All India Institute of Medical Sciences
OSINT: Open-Source Intelligence
ICMR: Indian Council of Medical Research
AWS: Amazon Web Services
DoS: Denial-of-Service
AWS: Amazon Web Services
BEC: Business Email Compromise
PRC: Privacy Rights Clearinghouse
AI: Artificial Intelligence
ML: Machine Learning
CSIRT: Computer Security Incident Response Team
CIRT: Cyber Incident Response Team

I. INTRODUCTION

A. Definition of Data Breaches

A data breach is an incident in which confidential, private, protected, or sensitive information is revealed to someone who is not authorized to view it. This information can include personal information, financial records, and proprietary business information. This can occur through an unintentional mishap or through deliberate efforts to obtain information from an individual or organisation.

For instance, a worker might inadvertently disclose sensitive data, or they could intentionally take company information and share it with—or sell it to—a third party. Additionally, a hacker might infiltrate a corporate database that holds sensitive information to steal it.

Regardless of the initial cause of a data breach, the acquired information enables cybercriminals to profit by either selling it or incorporating it into broader attacks. A data breach generally involves the loss or theft of sensitive information, including bank account information, credit card numbers, personal health records, and login details for email and social media accounts.

An information breach can have severe consequences for businesses, affecting them not only through monetary losses but also through reputational harm to customers, clients, and employees. Additionally, organisations may face penalties and legal repercussions due to the increasing strictness of data and privacy laws, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [2].

A data breach may occur due to an external attacker targeting one or more organisations for specific types of information, or it may originate from individuals within the organisation. Cybercriminals often target specific organisations with tailored cyberattacks.

Data breaches can occur as a result of intentional attacks, accidental mistakes or oversights by staff members, or weaknesses and vulnerabilities in an organization's systems.

B. Importance of the Topic

Cybercriminals typically target valuable data, including corporate information and personally identifiable information (PII), which they can exploit for profit or to harm individuals or organisations. As these attackers grow more advanced, their tactics become carefully orchestrated to uncover vulnerabilities and target individuals who are more likely to fall victim to an assault.

Upon gaining access to data, the repercussions can be tremendously harmful. A data breach may result not only in organisations losing sensitive information, such as financial data or trade secrets, but also in incurring penalties, financial losses, and reputational harm, often with lasting effects. An attack on a governmental entity could expose confidential and highly sensitive data, including details about military operations, national infrastructure, and political affairs, thereby putting both the government and its citizens at risk from foreign entities.

When individuals experience a breach, their personal data may be compromised, including banking information, health records, or Social Security numbers. With access to this information, a cybercriminal could commit identity theft, infiltrate their social media accounts, damage their credit

Manuscript received on 05 January 2026 | First Revised Manuscript received on 02 February 2026 | Second Revised Manuscript received on 10 February 2026 | Manuscript Accepted on 15 February 2026 | Manuscript published on 28 February 2026.

*Correspondence Author(s)
Raja Irfan Ahmad*, Multidisciplinary Research Unit (MRU), Sher-I-Kashmir Institute of Medical Science, Soura, Srinagar, J&K, India. Email ID: rirfan900@gmail.com, ORCID ID: 0000-0003-0579-3188

score, misuse their financial resources, and even generate new identities for subsequent attacks.

Some of the most significant data breaches in history have had enduring repercussions for the affected organisations. Notable examples of data compromises include:

i. Yahoo

In 2016, the major internet company Yahoo announced that it had experienced two data breaches in 2013 and 2014. The incidents, which compromised up to 1.5 billion accounts, were reportedly carried out by hackers believed to be state-sponsored who obtained personal details such as email addresses, names, and unencrypted security questions and answers.

ii. Equifax

A data breach at Equifax, a financial services company, occurred between May and June 2017, impacting over 153 million individuals in Canada, the U.K., and the U.S. This breach revealed sensitive customer information, including birth dates, driver's license numbers, names, and Social Security numbers, along with approximately 200,000 credit card details. The incident was triggered by a vulnerability in third-party software that had been fixed but was not implemented on Equifax's systems [14][15][16].

iii. X (Previously Known as Twitter)

In 2018, Twitter encouraged its 330 million users to change their passwords after a bug exposed them. This incident was attributable to an error in Twitter's password-hashing process. The social media platform stated that it had identified and resolved the bug, but it remains a notable instance of potential vulnerability exploitation [9].

In May 2020, Twitter experienced a potential breach that may have affected businesses using its advertising and analytics services. Due to a caching issue, Twitter acknowledged that it was "possible" for some users' email addresses, phone numbers, and the last four digits of their credit card numbers to have been accessed.

iv. First American Financial Corporation

In May 2019, First American Financial, an insurance company, experienced an incident that exposed more than 885 million sensitive documents. This breach resulted in the online availability of files containing bank account numbers and statements, mortgage records, photographs of driver's licenses, Social Security numbers, tax documents, and wire transfer receipts dating back to 2003.

The breach is thought to have stemmed from an insecure direct object reference (IDOR), a flaw in website design that allowed a link meant for a specific user to become publicly accessible, enabling anyone to view the documents.

v. Facebook

In September 2019, a server containing phone numbers associated with over 419 million Facebook users' account IDs became exposed. Because the server lacked password protection, anyone could access the database. Three months later, hackers exposed a database that included approximately 300 million Facebook users' names, phone numbers, and user IDs, leaving it unsecured on the dark web for about two weeks.

vi. Solar Winds

In 2020, threat actors from Russia carried out a supply chain attack by compromising the software provider SolarWinds. The hackers exploited SolarWinds' Orion network monitoring platform to deploy malware to the organization's customers secretly.

Russian intelligence operatives accessed sensitive information from various US government agencies, including the Treasury, Justice, and State Departments, which rely on SolarWinds' services.

vii. Colonial Pipeline

In 2021, ransomware attackers targeted Colonial Pipeline's systems, resulting in a temporary shutdown of the pipeline that supplies 45% of the fuel for the US East Coast.

The hackers infiltrated the network by using an employee's password obtained on the dark web. The Colonial Pipeline Company paid a ransom of USD 4.4 million in cryptocurrency, although federal law enforcement recovered approximately USD 2.3 million of that sum.

viii. 23 and Me

In the autumn of 2023, hackers compromised the data of 6.9 million users of 23andMe. This breach was significant for two main reasons. First, because 23andMe focuses on genetic testing, the attackers accessed unique, highly personal information, including DNA data and family trees.

Secondly, the breach occurred through a method known as "credential stuffing." In this type of attack, hackers use credentials obtained from previous data breaches to access users' accounts across multiple platforms. These attacks are effective because many individuals tend to reuse the same usernames and passwords across multiple sites.

C. Data Breaches in India 2022-2023

Cyberattack on All India Institute of Medical Sciences (AIIMS), New Delhi

In December 2022, in response to a question posed by Communist Party of India (Marxist) MP John Brittas, the Union government revealed that the All-India Institute of Medical Sciences (AIIMS), New Delhi, had suffered a cyberattack that encrypted approximately 1.3 terabytes of data across five servers.

Rajeev Chandrasekhar, the Minister of Electronics and Information Technology, indicated that the incident was classified as a "cybersecurity incident" stemming from unauthorised access to AIIMS' network caused by poor network segmentation.

The Indian Computer Emergency Response Team (CERT-In) evaluated the situation and suggested necessary actions to remedy the breach.

Meanwhile, in the Lok Sabha, the Minister of State for Health and Family Welfare, Bharati Pravin Pawar, disclosed that the attackers did not specify a ransom amount but left a message on the server confirming the cyberattack.

The e-Hospital data was efficiently restored from an unaffected backup server, and most application features were recovered after a two-week restoration period.

II. MOCHHATUA DATA BREACH

According to a hacker on a forum, MoChhatua, an Indian l ocal governance software, experienced a data breach in May 2023.

According to the threat actor, the breach revealed private use r data, including passwords, emails, and identities.

The regional department of women and child development in Odisha created the app to anage and digitize the delivery of ration supplies to recipients.

The Odisha state government was contacted by the Cyber Express team for confirmation, but they did not provide an o fficial comment.

Threat intelligence firm Falcon Feeds posted an update on Twitter that included a download link for the stolen data as well as a screenshot of the hacker's post with the exposed da ta.

A. Zivame, Data Breach

Zivame, an online marketplace for women's clothing in India, experienced a serious data breach that resulted in the online sale of thousands of its female customers' personal information.

About 1.5 million Zivame users' names, email addresses, phone numbers, and physical addresses were among the data compromised.

A person claiming to have the data was willing to sell it for $500 in cryptocurrency, according to an investigation by India Today's Open-Source Intelligence (OSINT) team. The team used a Telegram handle to contact the vendor, posing as a prospective buyer, to verify the authenticity of the data.

As evidence, the supplier provided a sample dataset containing the private information of more than 1,500 individuals. The vendor insisted on payment only in bitcoin, a standard practice in such illegal transactions, and emphasised that the data was not publicly accessible.

B. Cyberabad Police Data Leak

The Cyberabad Police issued notices to more than eleven firms, including a social media company, an IT services firm, an online insurance company, and banks, in connection with the large-scale data breach that affected 669 million people and entities across India in April this year.

Bhardwaj is accused of theft, illegal retention, and the unauthorised disclosure of personal and proprietary information belonging to individuals and businesses.

The Information Age crime included the theft of customer and student data from several EdTech firms, business customer data, and GST records.

The Cyberabad police launched a comprehensive investigation into the database hacking and data leak to identify security vulnerabilities and prevent similar incidents in the future.

Delegates from the companies concerned are answering questions regarding their database management systems, procedures, policies, and access rights.

C. Swachh Platform Hacked

In September 2022, data belonging to nearly 16 million users were compromised after the swachhcity.org website, which is linked to the Swachh Bharat Mission and the Ministry of Housing and Urban Affairs, was hacked.

The hackers, who claimed to be LeakBase, targeted users' email addresses, hashed passwords, phone numbers, OTPs, IP addresses, user tokens, and even their browser fingerprints.

LeakBase compromised this account for financial gain. The database they stole was posted for sale on the dark web.

Given the nature of the compromised data, this breach poses a significant threat. Exploitation of the stolen data is highly likely, and phishing emails purporting to be breach notices, along with social engineering tactics, pose additional challenges.

This type of information retrieval can also result in ransomware attacks, unauthorised data collection, and the sale of leads on cybercrime forums.

D. Rentomojo Cyber Attack

A data breach at Rentomojo, an online rental marketplace in India, occurred in April 2023, exposing users' private data.

Rentomojo's database was compromised on April 20, 2023, resulting in unauthorised access and endangering user data. When Reddit users reported receiving emails from a hacker organisation purporting to have access to financial data and personally identifiable information (PII), Rentomojo's assurance that no financial information was compromised raised concerns.

This data breach in India has serious repercussions because it exposes users' personal information, thereby increasing their susceptibility to financial fraud and identity theft.

Rentomojo responded promptly, alerting the authorities, enlisting the assistance of legal and cybersecurity professionals, and strengthening its security measures [19].

The need for robust cloud security procedures was emphasised by CEO and co-founder Geetansh Bamania, who indicated that the hackers obtained PII by exploiting cloud misconfigurations [3].

E. Sun Pharma Cyber Attack

One of India's leading pharmaceutical companies, Sun Pharmaceutical Industries, experienced a serious security breach that affected its operations.

Sun Pharma informed the stock markets about the occurrence, but it withheld information about the impact and the identity of the culpable party.

Following similar breaches at Dr Reddy's Laboratories, Lupin, and the All-India Institute of Medical Sciences, this event was the third high-profile cyberattack on a major Indian pharmaceutical company in recent years.

Sun Pharma acknowledged that some file systems were accessed and that personal and business data were taken. Still, it has not disclosed specifics about the attack's source or the affected data.

Although the business was proactive in isolating its network and starting the recovery process, the incident's

The full impact and associated expenses remain to be determined; their negative effects have yet to be determined.

F. 6. BharatPay Hacked

Approximately 37,000 individuals' personal information and transaction details were publicly disclosed following a major data breach at BharatPay, an Indian digital financial services provider, in August 2022.

Employee official email addresses, UPI IDs, mobile phone numbers, hashed passwords, and usernames from Indian banking and insurance companies are among the exposed data.

XVigil, CloudSEK's threat intelligence division, found the issue on August 13.

It was discovered that a cybercrime site had leaked BharatPay's backend database, which included transaction data, bank balances, and personal information about clients from February 2018 to August 2022.

With a network of more than 50,000 retail locations, BharatPay serves consumers and merchants in 11 Indian states. The exposure of sensitive data, including financial information, transaction records, and user PII, is what makes the data breach significant.

Information on SMS providers and API credentials for online bill payment processors was also included in the compromised database.

Callback response logs containing sensitive information, such as phone numbers, transaction IDs, and bank balance amounts—all of which are essential to financial transactions between entities—are among the disclosed data.

G. Rail Yatri Data Breach

A recent hack at the e-booking services website RailYatri brought Indian Railways' cybersecurity back into the public eye.

The rail ticketing platform was found to have over 30 million user records for sale on the dark web. A threat actor claimed to be from RailYatri and published a database on Breach Forums, exposing the December 2022 breach.

37,000 invoices and 31 million user records were among the compromised data. A similar breach occurred at RailYatri in 2020, affecting 700,000 customers.

Although unauthorized parties may have accessed some registered user information, RailYatri confirmed the latest breach and reassured users that no sensitive customer data had been exposed.

Rail Yatri reported the breach to the authorities and remedied it immediately. All IRCTC business partners, including Railway Yatri, were urged by the Railway Board to carry out comprehensive system examinations.

H. CloudSEK Data Breach

A threat actor known as "sedut" targeted CloudSEK Info Security Pvt. Ltd., an Indian cybersecurity company, in December 2022. The attacker's goal was to damage CloudSEK's standing in the community of cyber threat intelligence. The threat actor posted on cybercrime forums that they had obtained confidential information, including client details and source code for VPN credentials.

After a preliminary examination, CloudSEK concluded that the breach was caused by a compromised JIRA user's session cookies (JIRA is a commercial program developed by Atlassian that supports bug tracking, problem management, and agile project oversight). It was an employee's compromised laptop that stole session cookies and passwords. Purchase orders, social media accounts, Confluence servers, the JIRA platform, and other documents were all compromised by the threat actor.

CloudSEK, however, rejected the assertion that it had access to client information, VPN credentials, and specific credentials.

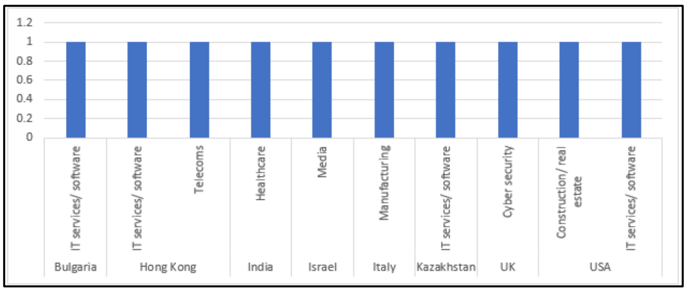
The company's infrastructure, unprotected accounts, and compromised VPN IP addresses were all highlighted in the incident. Additionally, Cloud SEK noted that some of the threat actors' allegations were based on Confluence access or internal documentation.

Top ten data breaches in 2023 [26]

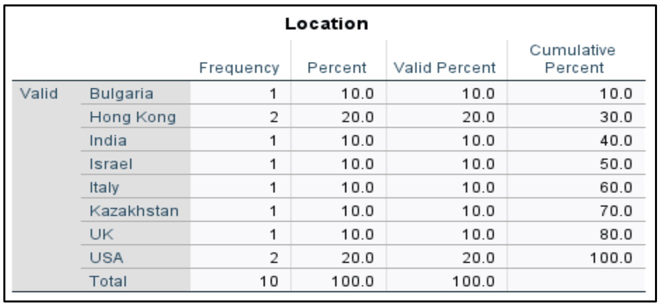
Table I: Shows the Top Ten Data Breaches in 2023

	Organisation Name	Sector	Location	Known Records Breached	Month of Public Disclosure
1	Dark Beam	Cyber security	UK	>3,800,000,000	September
2	Real Estate Wealth Network	Construction/ real estate	USA	1,52,37,76,691	December
3	Indian Council of Medical Research (ICMR)	Healthcare	India	81,50,00,000	October
4	Kid Security	IT services/ software	Kazakhstan	>300,000,000	November
5	Twitter(X)	IT services/ software	USA	>220,000,000	January
6	Tune Fab	IT services/ software	Hong Kong	>151,000,000	December
7	Dori Media Group	Media	Israel	>100 TB*	December
8	Tigo	Telecoms	Hong Kong	>100,000,000	July
9	SAP SE Bulgaria	IT services/ software	Bulgaria	9,55,92,696	November
10	Luxottica Group	Manufacturing	Italy	7,00,00,000	May

*For incidents where we only know the file size of the data breached, we use the formula 1 MB = 1 record. Given that we can't know the exact numbers, as they depend on the types of records included (e.g., images and medical histories are considerably larger files than just names and addresses), we err on the side of caution by using this formula. We believe this underestimates the number of records breached in most cases, but it is more accurate than not providing a number at all.



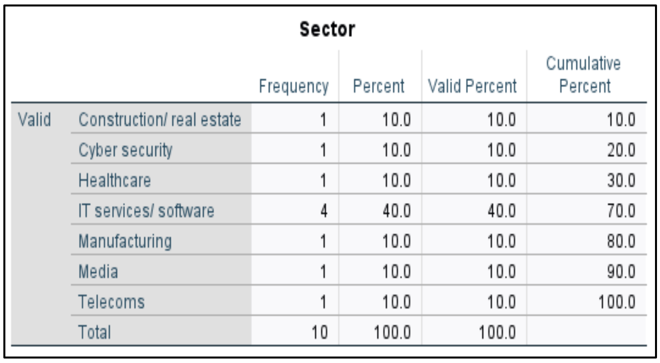
[Fig.1: Shows the Data Breaches Between Location and Sector]



Location

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Bulgaria	1	10.0	10.0	10.0
	Hong Kong	2	20.0	20.0	30.0
	India	1	10.0	10.0	40.0
	Israel	1	10.0	10.0	50.0
	Italy	1	10.0	10.0	60.0
	Kazakhstan	1	10.0	10.0	70.0
	UK	1	10.0	10.0	80.0
	USA	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

[Fig.2: Shows the Statistics of Location]



Sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Construction/ real estate	1	10.0	10.0	10.0
	Cyber security	1	10.0	10.0	20.0
	Healthcare	1	10.0	10.0	30.0
	IT services/ software	4	40.0	40.0	70.0
	Manufacturing	1	10.0	10.0	80.0
	Media	1	10.0	10.0	90.0
	Telecoms	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

[Fig.3: Presents Sector-Level Statistics]

III. OBJECTIVES OF THE REVIEW

This review aims to:

Identify trends in data breaches over recent years.

Analyze the impacts of data breaches on organizations and individuals.

Discuss effective mitigation strategies to prevent future breaches.

IV. LITERATURE REVIEW OR BACKGROUND

There are two main categories into which this data breach study falls. The first group focuses on elements that can reduce the likelihood of data breaches. This method examines the potential causes of data breaches rather than merely addressing them. The goal of this research is to elucidate the mechanisms underlying data breaches to enable more effective implementation of preventive measures. According to this section of the study, employees are primarily responsible for most data breaches, with their disregard for the organisation's security procedures as the primary contributing factor [6].

Table II: Shows the Data Breaches Between 2005 and 2023 in Various Organizations

Author	Findings
Campbell et al. [10]	Discovered that organizations had been imposed heavily by fines when they found that private data loss is informed.
Hovav & D'Arcy et.al [22]	Found that the markets had acted differently to the breach warnings based on whether the firm was either a pure e-tailer or not.
Cavusoglu et al. [11]	Reports indicate that, on average, 2.1% of the organisation's market share is lost following a data breach.
Culnan J.J. etal. [17].	In this study, the researchers identified two major data breaches at ChoicePoint and TJX. They opined that organisations, when framing organisational privacy guidelines, should consider their ethical responsibilities.

The results of several data breaches that occurred across numerous organizations between 2005 and 2023 are presented in this study. Furthermore, this work employs two key approaches to address prior studies on data breaches. We will begin by examining all recorded data breaches since 2005, with particular attention to those that affect a specific business or industry. The effects of data breaches on publicly traded organizations will then be discussed.

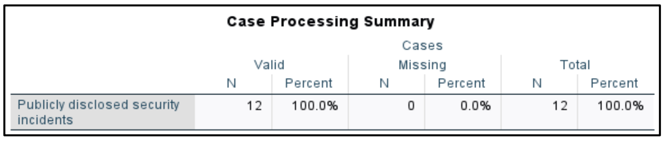
V. METHODOLOGY

To thoroughly investigate publicly disclosed data breaches, we adopt a content analysis approach in this study. In information systems research, for instance, content analysis is frequently used to comprehend the strategic impact of information technology and the significance of e-commerce. This approach aims to demonstrate the importance of information technology in shaping the organisation's strategy by analysing the annual reports that CEOs prepare and deliver to stakeholders. Any kind of textual data can be subjected to content analysis to get ideological conclusions. We use this approach for publicly disclosed data breaches. All of the breaches recorded by the Privacy Rights Clearinghouse are included in the chosen data. Since 1992, the PRC has been a nonprofit organisation committed to protecting individuals' privacy and promoting constructive change. MED Healthcare and Medical Providers (Hospitals, Medical Insurance Services), EDU Educational Institutions (Schools, Colleges, Universities), BSO Businesses (Manufacturing, Technology, Communications, Other), BSR Businesses (Retail/Merchant including Grocery Stores, Online Retailers, Restaurants), BSF Businesses (Financial Services, Banking, Insurance Services), and NGO Nonprofits (Charities and Religious Organizations) are just a few of the organizations we have looked at for data breaches [12]. The Privacy Rights Clearinghouse (PRC) reported breaches in 2023. Based on the tabulated data, graphs have been produced, and the data have been arranged chronologically by year for each entity [7]. To analyze the data, we used SPSS software [8].

The following table presents the findings of the 2023 data breach analysis. [26]

Table III: Displays the Findings of the 2023 Data Breach Analysis

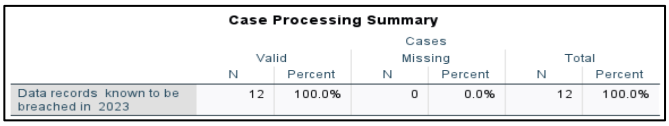
Month	Data Records Known to be Breached in the Year 2023	Publicly Disclosed Security Incidents
January	277618767	104
February	29582356	106
March	41970182	100
April	4353257	120
May	98226877	98
June	14353113	79
July	146290598	87
August	79729271	73
September	381726141	71
October	867072315	114
November	519111354	470
December	2241916765	1351



Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Publicly disclosed security incidents	12	100.0%	0	0.0%	12	100.0%

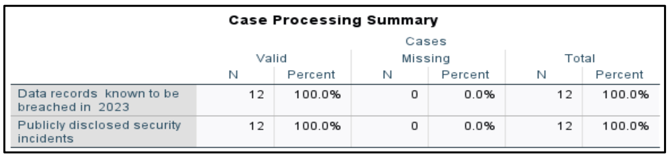
[Fig.4: Shows the Statistics of Publicly Disclosed Incidents]



Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Data records known to be breached in 2023	12	100.0%	0	0.0%	12	100.0%

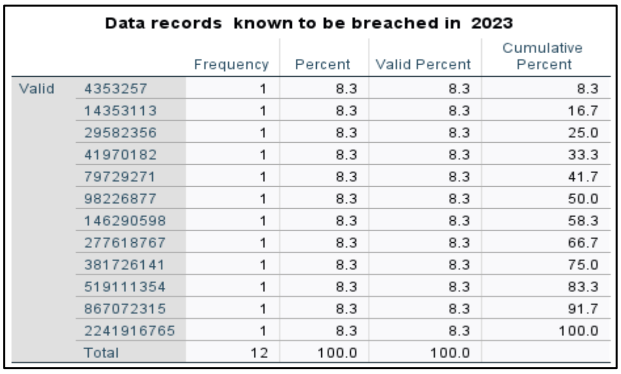
[Fig.5: Shows the Statistics of Known Data Breaches in 2023]



Case Processing Summary

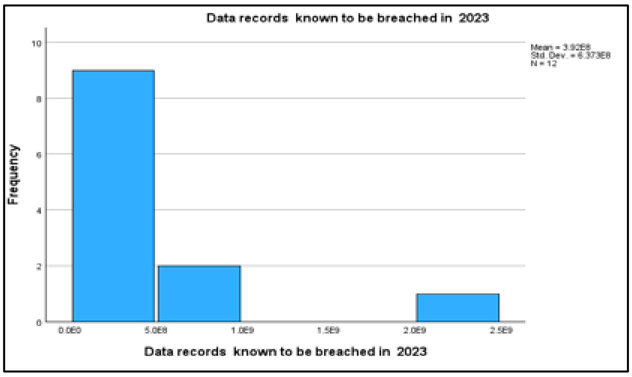
	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Data records known to be breached in 2023	12	100.0%	0	0.0%	12	100.0%
Publicly disclosed security incidents	12	100.0%	0	0.0%	12	100.0%

[Fig.6: Shows the Statistics of Known Data Breaches vs Publicly Disclosed Data]

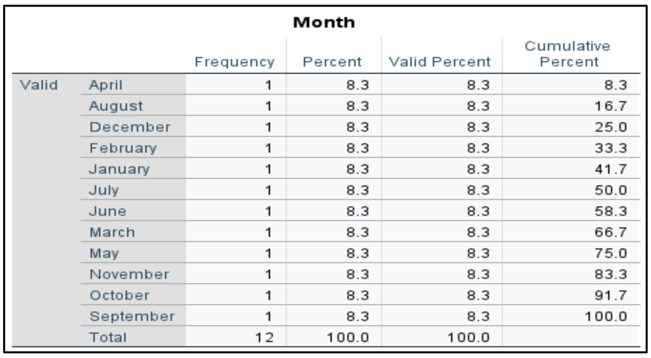


Data records known to be breached in 2023

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	4353257	1	8.3	8.3	8.3
	14353113	1	8.3	8.3	16.7
	29582356	1	8.3	8.3	25.0
	41970182	1	8.3	8.3	33.3
	79729271	1	8.3	8.3	41.7
	98226877	1	8.3	8.3	50.0
	146290598	1	8.3	8.3	58.3
	277618767	1	8.3	8.3	66.7
	381726141	1	8.3	8.3	75.0
	519111354	1	8.3	8.3	83.3
	867072315	1	8.3	8.3	91.7
	2241916765	1	8.3	8.3	100.0
	Total	12	100.0	100.0	



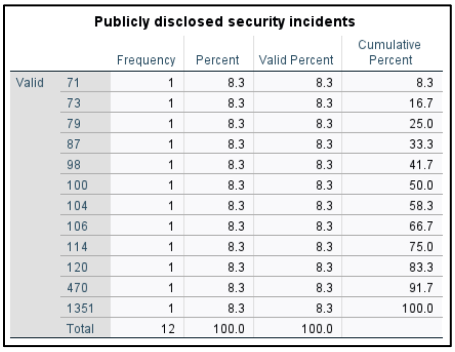
[Fig.7: Shows the Descriptive Frequencies of Known Data Breaches in 2023]



Month

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	April	1	8.3	8.3	8.3
	August	1	8.3	8.3	16.7
	December	1	8.3	8.3	25.0
	February	1	8.3	8.3	33.3
	January	1	8.3	8.3	41.7
	July	1	8.3	8.3	50.0
	June	1	8.3	8.3	58.3
	March	1	8.3	8.3	66.7
	May	1	8.3	8.3	75.0
	November	1	8.3	8.3	83.3
	October	1	8.3	8.3	91.7
	September	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

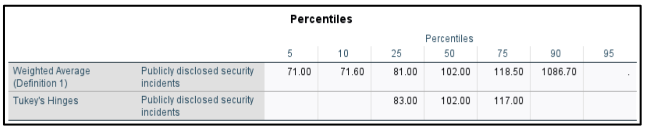
[Fig.8: Shows the Descriptive Frequencies of Known Data Breaches in Months]



Publicly disclosed security incidents

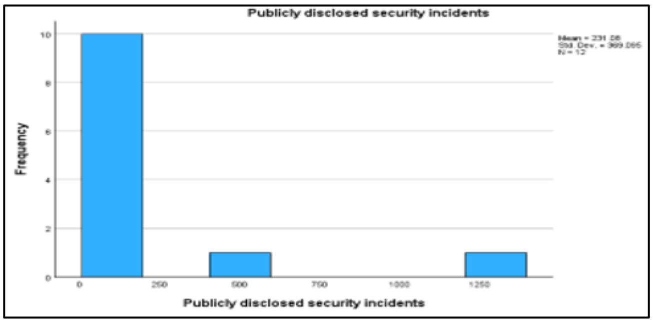
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	71	1	8.3	8.3	8.3
	73	1	8.3	8.3	16.7
	79	1	8.3	8.3	25.0
	87	1	8.3	8.3	33.3
	98	1	8.3	8.3	41.7
	100	1	8.3	8.3	50.0
	104	1	8.3	8.3	58.3
	106	1	8.3	8.3	66.7
	114	1	8.3	8.3	75.0
	120	1	8.3	8.3	83.3
	470	1	8.3	8.3	91.7
	1351	1	8.3	8.3	100.0
	Total	12	100.0	100.0	

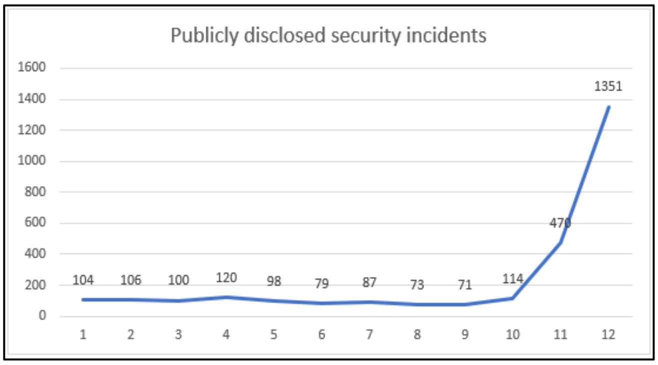
[Fig.9: Shows the Descriptive Frequencies of Publicly Disclosed Data Breaches]



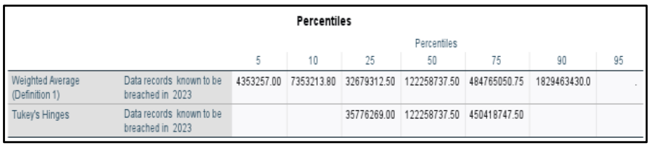
Percentiles

		Percentiles						
		5	10	25	50	75	90	95
Weighted Average (Definition 1)	Publicly disclosed security incidents	71.00	71.60	81.00	102.00	118.50	1086.70	.
Tukey's Hinges	Publicly disclosed security incidents			83.00	102.00	117.00		



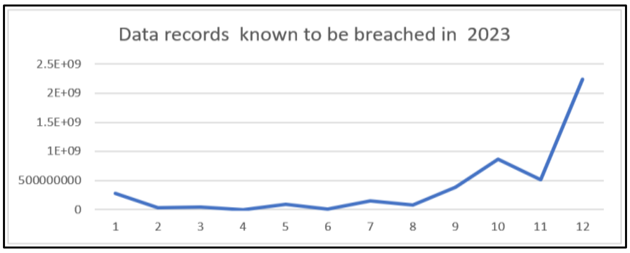


[Fig.10: Shows the Percentiles of Known Publicly Disclosed Data Breaches]

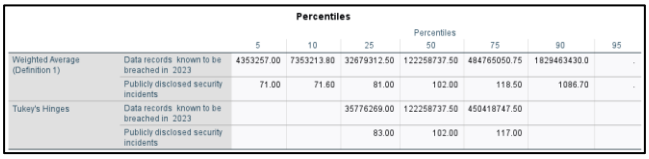


Percentiles

		Percentiles						
		5	10	25	50	75	90	95
Weighted Average (Definition 1)	Data records known to be breached in 2023	4353257.00	7353213.80	32679312.50	122258737.50	484765050.75	1829463430.0	.
Tukey's Hinges	Data records known to be breached in 2023			35776269.00	122258737.50	450418747.50		



[Fig.11: Shows the Percentiles of Known Publicly Disclosed Data Breaches in 2023]



Percentiles

		Percentiles						
		5	10	25	50	75	90	95
Weighted Average (Definition 1)	Data records known to be breached in 2023	4353257.00	7353213.80	32679312.50	122258737.50	484765050.75	1829463430.0	.
	Publicly disclosed security incidents	71.00	71.60	81.00	102.00	118.50	1086.70	.
Tukey's Hinges	Data records known to be breached in 2023			35776269.00	122258737.50	450418747.50		
	Publicly disclosed security incidents			83.00	102.00	117.00		

[Fig.12: Shows the Percentiles of Known Publicly Disclosed Data Breaches in 2023 and Known Data Breaches in 2023]

Types of Data Breaches [24][28][29]

Due to its diverse and ever-evolving nature, the data breaches can be categorised into different types, but some common types stand out:

A. Access Control Breaches

How it works: In this type of data breach, unauthorised individuals gain access to restricted data systems, often through stolen credentials, phishing attacks, or by exploiting system vulnerabilities.

Impact: Stolen sensitive data, financial losses, identity theft, and reputational damage. Examples: Marriott International (2018), Equifax (2017).

B. Malware Attacks

How it works: In this type of data breach, malicious software, such as viruses, worms, or ransomware, infects systems, enabling attackers to steal data, encrypt files for ransom, or disrupt operations.

Impact: Data theft, system disruption, financial losses, and data corruption.

Examples: WannaCry ransomware attack (2017), NotPetya ransomware attack (2017) [5].

C. Phishing and Social Engineering

How it works: In this type of data breach, deceptive emails, texts, or websites trick users into revealing personal information, such as login credentials, or into clicking malicious links that install malware.

Impact: Stolen credentials, data breaches, financial losses, and identity theft. Examples include Business Email Compromise (BEC) scams and fraudulent login-page scams.

D. Denial-of-Service (DoS) Attacks

How it works: In this type of data breach, attackers flood a website or server with overwhelming traffic, making it unavailable to legitimate users.

Impact: Disruption of services, financial losses, and reputational damage.

Examples: GitHub attack (2023), Amazon Web Services (AWS) attack (2020).

E. Insider Threats

How it works: In this type of data breach, an authorised individual with access to sensitive data intentionally misuses it for personal gain, revenge, or espionage.

Impact: Stolen data, intellectual property theft, sabotage, and financial losses.

Examples: Edward Snowden leak (2013), Chelsea Manning leak (2010).

F. Supply Chain Attacks

How it works: In this type of data breach, an attacker compromises a software vendor or service provider to gain access to their customers' data or systems.

Impact: Widespread data breaches, disruption of multiple organizations, loss of trust in supply chains.

Examples: SolarWinds supply chain attack (2020), Kaseya ransomware attack (2021).

G. Physical Security Breaches

How it works: In this type of data breach, attackers gain physical access to data storage devices or systems, either through break-ins or through social engineering.

Impact: Stolen data storage devices, loss of data, disruption of operations.

Examples include the Sony PlayStation Network hack (2011) and the Target data breach (2013).

H. Password Guessing and Keystroke Logging

How it works: In this type of data breach, imagine someone trying every combination on your digital lock until they crack it. Password guessing and keystroke logging are brute-force methods to steal login credentials. Guessing relies on common passwords or dictionary attacks, while keyloggers capture what you type, potentially revealing passwords and other sensitive information.

Impact: Stolen credentials can unlock a treasure trove of personal information, leading to identity theft, financial losses, and reputational damage.

Examples: The October 2023 Microsoft Azure vulnerabilities highlighted the importance of strong, unique passwords and multi-factor authentication to bolster security against brute-force attacks [1].

Industries Affected [29][30][31]

The digital era offers numerous possibilities but also poses significant risks, including data breaches. These cyber intrusions cause damage in multiple sectors, resulting in compromised information and monetary losses. Let's examine the data, uncovering the weaknesses and emphasizing the necessity for strong protective measures:

i. Healthcare

Grim Reality: The most breached industry in 2023, with an estimated 50 million patient records exposed – an unsettling 34% increase from 2022 (IBM Security X-Force Threat Intelligence Index 2023) [21].

Costly Scars: Each breach inflicts a hefty financial wound, averaging $10.10 million in 2022 (Ponemon Institute Cost of a Data Breach Report 2023). Beyond monetary losses, reputational damage and patient anxiety add to the toll.

Vulnerable Points: Weak cybersecurity practices, human error, and sophisticated phishing attacks exploit vulnerabilities in outdated systems and data storage.

ii. Retail

Target in the Crosshairs: Point-of-sale systems are prime targets, resulting in numerous breaches in 2023. Financial motivations drive these attacks, which target sensitive payment data such as credit card details.

A Widespread Threat: Nearly all (98%) of point-of-sale data breaches in the hospitality industry in 2021 were financially motivated, highlighting the pervasiveness of the threat (Verizon Data Breach Investigations Report 2023).

Breaches Beyond Money: Stolen data jeopardises not just finances, but also customer trust.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Outdated software, insecure payment systems, and physical security vulnerabilities create fertile ground for these attacks.

iii. Finance

According to the Verizon Data Breach Investigations Report 2023, 79 financial companies experienced breaches that affected 9.4 million consumers, placing them second in the number of breaches in 2023.

According to the Ponemon Institute Cost of a Data Breach Report 2023, the average cost per breach in the banking sector in 2022 was $5.90 million, exceeding the global average.

Hackers frequently exploit payment system vulnerabilities, deploy malware to gain network access, or employ social engineering tactics to trick staff into disclosing confidential information.

Impacts of Data Breaches [29][30][31][32][33]

A data breach can have serious and far-reaching effects. These instances have evolved from straightforward cybersecurity issues into causes of financial losses, reputational harm, legal issues, fines, and a significant decline in consumer trust. Cybercriminals continue to devise creative ways to circumvent security measures and access vital corporate information and credentials, despite the growing emphasis on data protection. Among the more detrimental effects of a data breach are:

VI. FINANCIAL CONSEQUENCES

One of the most pressing issues organisations face is the financial impact of data breaches. The average cost of a data breach hit a record high of USD 4.45 million in 2023, according to IBM's Cost of Data Breach Report 2023. Compared with the USD 4.35 million spent the previous year, this represents a 2.3% increase.

In addition to the substantial fines that may be imposed for noncompliance with the GDPR (General Data Protection Regulation), costs may include compensating affected customers, initiating incident response activities, investigating the breach, purchasing more secure equipment, and incurring legal fees.

A security breach can significantly affect a firm's stock price and overall value. This is what happened to Yahoo following its 2013 data breach. The issue came to light in 2016, when the business was about to be acquired by the U.S. telecommunications company Verizon. The deal went through, with Verizon purchasing Yahoo for $4.48 billion, approximately $350 million less than they had originally requested [4].

A. Reputational Damage

A data breach can have disastrous effects on a company's reputation. According to studies, approximately one-third of consumers in industries such as retail, banking, and healthcare will stop doing business with organisations that suffer a breach.

Additionally, 33.5% will vent their dissatisfaction on social media, and 85%are likely to share their experiences with others.

Information spreads quickly, and within hours of a breach being discovered, a company may be at the forefront of a worldwide news story. The affected company may suffer long-term harm as a result of this negative press and a decline in customer confidence.

Customers are becoming more conscious of the value of their personal information, and companies may seek to emulate rivals that prioritise security if they cannot demonstrate that they have taken the necessary precautions to protect this data. Identity theft can readily result from a data breach when sensitive data is disclosed to unauthorised parties. Hackers might use this information to create false identities and commit fraud, such as creating new accounts or making unlawful purchases.

Reputational harm is permanent and will make it more difficult for a business to draw in new clients, raise capital, and hire staff.

B. Legal and Regulatory Implications

Data protection rules compel organizations to demonstrate that they have taken all necessary precautions to secure personal data. People have the right to file a lawsuit to recover damages if this security is compromised, whether on purpose or accidentally.

We anticipate seeing more collective lawsuits over the consequences of data breaches as they become more frequent and severe.

C. The Impact of Sensitive Data Loss

The consequences of a data breach involving the compromise of private information can be disastrous. Any information that may be used to directly or indirectly identify a person is referred to as personal data. Names, passwords, IP addresses, and credentials are all included in this. It also includes sensitive personal data that can be used to identify an individual, including genetic or biometric information.

A data breach could seriously affect a patient's medical care and, in extreme cases, their life if their critical medical records were lost. Biometric information is also highly valued by cybercriminals because it is significantly more valuable than simple email addresses or credit card numbers.

The consequences of breaches that expose this type of data can be catastrophic and may outweigh any damage to one's finances or reputation.

There is no space for complacency in the ever-evolving world of cybersecurity, especially when it comes to the consequences of a data breach, regardless of how prepared your company is to handle one. Establishing a thorough security plan is essential to safeguarding data privacy, reducing risks, and preserving the reputation of your company.

D. The Disruptive Effect of Operational Downtime

Business activities are severely disrupted after a data breach. Organisations must manage the ramifications of data breaches in the aftermath, which necessitates conducting in-depth investigations into the affected systems and their causes. Operations may need to be suspended until investigators have obtained all necessary information. Identifying vulnerabilities may take days or even weeks, depending on the severity of the incident. Such interruptions can significantly affect income and make it more difficult for a business to recover.

According to IBM's Cost of Data Breach Report 2023, it usually takes 277 days to find and handle a breach.

E. Case Studies [26][33][34][35]

Notable Data Breaches

Table IV: Shows the Notable Data Breaches

Year	Biggest Notable Data Breach
2023	Indian Council of Medical Research 815,000,000 records lost (Tech Informed)
	X (formerly Twitter) 200,000,000 records lost (CNN)
	MOVEit 62,000,000 records lost (AP News)
	T-Mobile 37,000,000 records lost (T-Mobile)
	HCA Healthcare 11,000,000 records lost (HCA Healthcare)
2022	Neopets 69,000,000 records lost (CPO Magazine)
	SuperVPN, GeckoVPN, and ChatVPN 21,000,000 records lost (Cybernews)
	Singtel Optun Pty Limited 9,800,000 records lost (Bloomberg)
	Cash App 8,200,000 records lost (TrendMicro News)
	X (formerly Twitter) 5,400,000 records lost (Malwarebytes)
2021	Facebook (Meta) 533,000,000 records lost (Business Insider)
	Syniverse 500,000,000 records lost (SEC)
	Power Apps (Microsoft) 38,000,000 records lost (Wired)
	Amazon Vendors 13,124,962 records lost (Safety Detectives)
	Pandora Papers 11,900,000 records lost (The Guardian)
2020	Pakistani Mobile Operators 115,000,000 records lost (ZD Net)
	SolarWinds 50,000,000 records lost (New York Times)
	MGM Hotels 10,600,000 records lost (ZD Net)
	Dutch Government 6,900,000 records lost (ZD Net)
	Marriott International 5,200,000 records lost (Marriott)
2019	16 Hackers Websites 617,000,000 records lost (The Register)
	MongoDB 275,265,298 records lost (Bleeping Computers)
	Microsoft 250,000,000 records lost (Forbes)
	8 Hacked Websites 127,000,000 records lost (TechCrunch)
	Capital One 100,000,000 records lost (CSO Online)
2018	Aadhaar 1,100,000,000 records lost (ZD Net)
	Marriott International 383,000,000 records lost (New York Times)
	X (Formerly Twitter) 330,000,000 records lost (Reuters)
	Chinese Job-seeking Websites 202,000,000 records lost (Hacken)
	Quora 100,000,000 records lost (New York Times)
	Google 500,000 records lost (Forbes)
2017	River City Media 1,370,000,000 records lost (The Guardian)
	Spambot 711,000,000 records lost (The Guardian)
	Equifax 143,000,000 records lost (CBC News)
	Malaysian Mobile Phone Numbers 46,200,000 records lost (Lowyat)
	AI.Type 31,000,000 records lost (ZD Net)
2016	Yahoo 500,000,000 records lost (CNBC)
	Friend Finder Network 412,000,000 records lost (ZD Net)
	Uber 57,600,000 records lost (New York Times)
	Morgan Stanley 15,000,000 records lost (Reuters)
	MySpace 427,000,000 records lost (Vice)
2015	Deep Root Analytics 198,000,000 records lost (Reuters)
	Experian/T-mobile 15,000,000 records lost (T-Mobile)
	Anthem 80,000,000 records lost (New York Times)
	Securus Technologies 70,000,000 records lost (The Intercept)
	US Office of Personnel Management 14,000,000 records lost (BBC)
2014	eBay 145,000,000 records lost (Business Insider)
	JPMorgan Chase 83,000,000 records lost (New York Times)
	The Home Depot 56,000,000 records lost (Krebs on Security)
	Korea Credit Bureau 20,000,000 records lost (Security Week)
	Sony Pictures 10,000,000 records lost (BuzzFeed News)
2013	These are the 5 largest data breaches that occurred in 2013.
	Yahoo 3,000,000,000 records lost (BBC)
	Court Ventures 200,000,000 records lost (Krebs on Security)
	Multiple American Businesses 160,000,000 records lost (Technology Review)
	Target 70,000,000 records lost (USA Today)
	Excellus Health Plan 9,300,000 records lost (USA Today)
2012	Zappos 24,000,000 records lost (Forbes)
	KT Corp 8,700,000 records lost (Korea Times)
	South Carolina State Department of Revenue 3,987,000 records lost (InfoWorld)
	Three Iranian Banks 3,000,000 records lost (DataBreachToday)
	Apple 1,000,000 records lost (CNET)
2011	Sony PSN 77,000,000 records lost (PlayStation Blog)
	Steam 35,000,000 records lost (BBC)
	Nexon Korea Corp 13,000,000 records lost (Reuters)
	The New York City Health and Hospitals Corp. lost 1,700,000 records (InfoRiskToday)
	The Washington Post 1,270,000 records lost (PC Mag)
2010	Educational Credit Management Corp 3,300,000 records lost (MPR News)
	Gawker 1,500,000 records lost (The Guardian)
	The Ohio State University 760,000 records lost (The Lantern)
	Lincoln Medical and Mental Health Centre, 130,000 records lost (The New York Times)

F. Lessons Learned [25][26][27]

The importance of data protection is a key lesson to be learned from data breaches. Businesses must recognise that data is one of their most important assets. It is essential to maintain basic cybersecurity procedures. This means using antivirus and anti-malware software, establishing strong password rules, and routinely applying updates and patches to systems and software. External hackers are not always the primary source of risk; internal threats may be just as dangerous. Sensitive information may be compromised by employees, whether via deliberate misconduct or negligence.

Thus, it is crucial to implement strict access controls, monitor user behaviour, and provide training on the importance of data protection. The risk of insider threats can be further reduced by conducting routine background checks and maintaining ongoing surveillance.

The speed and effectiveness of the reaction are critical when a security breach occurs. The effect may worsen if the breach is not promptly identified and managed.

Incidents can still occur despite the best protective measures. A business can minimize downtime and quickly restore operations with a robust disaster recovery plan.

G. Mitigation Strategies [24][27][33][35]

Mitigating data breaches entails identifying and remedying security vulnerabilities that enable unauthorised access to private data. The goal of data breach mitigation is to lessen the damage and repercussions that the breach may cause. Begin by identifying your sensitive information and its location within the company to prevent data leaks. Sort your data according to this assessment to determine which pieces of information require the highest level of security. Once sensitive data has been identified, appropriate security measures, such as encryption, access controls, and data loss prevention (DLP) tools, can be implemented.

i. *Preventive Measures [25]*

Organizations can implement several best practices to prevent data breaches:

Encryption: (Protecting data at rest and in transit). Data must be converted from a readable format into an encoded form to undergo encryption. Only after decryption can the encoded data be read or used. Symmetric-key and public-key encryption are the two main types of data encryption; the latter is generally considered substantially more secure.

Encrypting your data makes it more difficult for attackers to exploit any security holes. However, sophisticated attackers may still find ways to circumvent encryption, for example, by obtaining decryption keys if they are not adequately protected. Attackers may exploit situations in which unencrypted data is transmitted or stored.

Access Controls: (Limiting access to sensitive information based on roles). It's possible that people who shouldn't have access to your private information already do. Examine each permission to ensure you aren't granting illegal users' access [23].

Assign different sensitivity levels to all pertinent data to control access to distinct information sets. Highly sensitive data should be accessed only by trusted individuals who currently require it. Identifying any malevolent insiders who might have obtained access to private data with the intention of exfiltrating it is another benefit of this privilege review procedure.

Employee Training: (Educating staff about security protocols and phishing attacks (links sent via email))

ii. Incident Response Plans [32][33]

Reacting to a data breach does not help detect or prevent cybersecurity problems and data breaches before they happen. Occurrence response, as the name suggests, is concerned with a company's reaction to an occurrence. Effective incident response strategies aim to reduce the financial and data-exposure consequences of breaches while accelerating recovery.

To implement the data breach incident response plan, organisations should establish a Cyber Incident Response Team (CIRT) or a Computer Security Incident Response Team (CSIRT). In addition to IT security specialists, the CIRT/CSIRT comprises representatives from the legal, human resources, and public relations departments. These individuals must interact with CEOs, stakeholders, regulatory agencies, and the public at large.

It is impossible to overstate the importance of responding to a data breach incident [20]. Every day, organizations face challenges to their data security, and even seemingly small issues can turn into catastrophic events. It is crucial to ensure that your CIRT/CSIRT members understand their roles, are capable of handling pressure, and respond appropriately.

To accomplish this, you will need to create a data breach response plan and train your CIRT/CSIRT team so that they can work in tandem.

H. Emerging Technologies:[33][34][35]

Data breaches are becoming more frequent and complex. To effectively address these attacks and safeguard sensitive data, individuals and organisations must keep up with the latest advances in cybersecurity technology. Given the proliferation of new threats, constant attention to detail is required.

Data breaches have increased due to cybercriminals' increasingly sophisticated tactics. Ransomware, social engineering techniques, phishing scams, and attacks on Internet of Things devices are among the most recent cybersecurity threats. These detrimental behaviours may result in significant financial losses, reputational harm, and legal repercussions.

It's critical to stay up to date with cybersecurity developments to prevent cyberattacks and protect personal data. Organisations can enhance their security frameworks and reduce potential risks by implementing the latest cybersecurity solutions. Organisations can defend themselves against potential threats and safeguard their data by implementing appropriate measures.

In conclusion, keeping up with the latest advancements in cybersecurity technology is essential for ensuring the security of personal data and the continuity of corporate operations [13] [18].

Technologies such as artificial intelligence (AI), machine learning (ML), Behavioural Biometrics, Zero-Trust Architecture, and Quantum Computing can enhance security by identifying anomalies and potential threats in real time.

I. Future Directions

i. Evolving Threat Landscape

As technology advances, so do cybercriminals' strategies. Businesses need to keep up with new threats so they can modify their security protocols appropriately.

ii. Research Gaps

Further research is needed to evaluate the effectiveness of current mitigation strategies and to explore innovative data protection solutions.

VII. CONCLUSION

A serious risk of Data breaches in the current digital environment. Organisations can better safeguard confidential data and uphold stakeholder trust by being aware of trends, impacts, and mitigation strategies.

VIII. ACKNOWLEDGEMENT

I wish to thank the Multidisciplinary Research Unit SKIMS Soura Srinagar J&K for their support and guidance during the completion of this paper.

DECLARATION STATEMENT

Some of the references cited are older, noted explicitly as [17], [20], and [23]. However, these works remain significant for the current study, as they are pioneering in their fields.

I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/ Competing Interests:** Based on my understanding, this article has no conflicts of interest.
- **Funding Support:** This article has not been funded by any organizations or agencies. This independence ensures that the research is conducted objectively and free from external influence.
- **Ethical Approval and Consent to Participate:** The content of this article does not necessitate ethical approval or consent to participate with supporting documentation.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed solely by the author.

REFERENCES

1. Nalajala S (2020). Data Security in Cloud Computing Using Three-Factor Authentication. Lecture Notes in Electrical Engineering, Vol.637. https://www.researchgate.net/publication/339709490_Data_Security_in_Cloud_Computing_Using_Three-Factor_Authentication
2. Herath, T., & Rao, H. R. (2020). Protection motivation and deterrence: a framework for security policy compliance in organizations. European Journal of Information Systems, 18(2), 106-125. https://www.tandfonline.com/doi/full/10.1057/ejis.2009.6
3. Chintala R.R(2019). FPGA implementation of Katan block cypher for security in wireless sensor networks, International Journal of Emerging Trends in Engineering Research 7(11). https://www.warse.org/IJETER/static/pdf/file/ijeter157112019.pdf
4. A consolidated approach for estimation of data security breach costs, May 2016 DOI: https://doi.org/10.1109/INFOMAN.2016.7477530
5. Amudhavel J, Reddy L.S.S. "Effects, challenges, opportunities and analysis on security-based cloud resource virtualization - 2017." Journal of Advanced Research in Dynamical and Control Systems, Vol. 9, Special issue 12. https://www.researchgate.net/publication/320134073
6. P. R. Clearinghouse. Privacy Rights Clearinghouse's Chronology of Data Breaches. Accessed: Nov. 2017. [Online]. Retrieved from https://www.privacyrights.org/data-breaches
7. Jabber B. (2019). A novel sampling approach for balancing the data and providing health care management systems for the government. International Journal of Advanced Trends in Computer Science and Engineering, Vol.8, Issue 6. https://www.warse.org/IJATCSE/static/pdf/file/ijatcse12862019.pdf
8. Vijaya Chandra J (2019). Authentication and authorization mechanism for cloud security, International Journal of Engineering and Advanced Technology, vol.8, Issue 6. https://www.researchgate.net/publication/335842661_Authentication_and_Authorization_Mechanism_for_Cloud_Security
9. Gurajada L.B., Security attacks in wireless sensor networks (2018). International Journal of Engineering and Technology Vol. 7, Special Issue 32. https://www.researchgate.net/publication/324817452_Security_Attacks_in_Wireless_Sensor_Networks_A_Survey
10. The role of data privacy in marketing Conceptual/Theoretical Paper Published: 22 September 2016 Volume 45, pages 135–155, (2017) https://www.researchgate.net/publication/308578866_The_Role_of_Data_Privacy_in_Marketing
11. Cavusoglu, H., Mishra, B., & Raghunathan, S. (2017). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(I) 69-104. https://www.tandfonline.com/doi/abs/10.1080/10864415.2004.11044320
12. Reddy V.J (2020). Mining regular patterns in cloud databases. Test Engineering and Management, Vol.83.
13. C. R. Centre. Cybersecurity Incidents. Accessed: Nov. 2017. [Online]. Retrieved from https://www.opm.gov/cybersecurity/cybersecurityincidents
14. Kurt C Stange (2025). Doing qualitative research. 2025 Apr 4;57(6):450–451. DOI: https://doi.org/10.22454/FamMed.2025.142040
15. Creswell, J. W. (2017). Qualitative inquiry and research design: Choosing among five approaches. Thousand Oaks, CA: Sage Publications. https://psycnet.apa.org/record/2006-13099-000
16. Creswell, J. W. (2016). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Pearson Education https://www.researchgate.net/publication/324451568_Educational_Research_Planning_Conducting_and_Evaluating_Quantitative_and_Qualitative_Research_6th_Edition
17. Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organisational privacy: Lessons from the ChoicePoint and TJX data breaches. MIS Quarterly, 33(4), 673-687. https://www.jstor.org/stable/pdf/20650322.pdf, works remain significant, see the declaration
18. Doyle, K. (2016). Information security in health care - four critical errors. Retrieved from http://www.itworld.comlsecurity/68838/informationsecurity-health-care-fourcritical-errors
19. Experian (2019). Healthcare breaches and fraud are here to stay. Retrieved from http://www.experian.comlblogs/databreach/2015/05/15/healthcare-breaches-fraudare-here-ostayl
20. Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61-83. https://econpapers.repec.org/article/blarmgtin/v_3a13_3ay_3a2010_3ai_3a1_3ap_3a61-83.htm, works remain significant, see the declaration
21. ITR Centre. Data Breaches Increase 40 Per cent in 2016, Finds New Report from Identity Theft Resource Centre and Cyber Scout. Accessed: Nov. 2017. [Online]. Retrieved from http://www.idtheftcenter.org/2016databreaches.html
22. Hovav, A. & D'Arcy, J. (2019). The impact of denial-of-service attack announcements on the market value of firms, Risk Management and Insurance Review, 6(2),97-121. https://onlinelibrary.wiley.com/doi/abs/10.1046/J.1098-1616.2003.026.x
23. Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization, European Journal of Information Systems, 18(2), 140-150. https://link.springer.com/article/10.1057/ejis.2009.7, works remain significant, see the declaration
24. ISACA. (2018). Top business/technology issues survey results. Retrieved from http://www.isaca.orglKnowledge-Center/Pages/Top-Business-Technology-IssuesSurvey-Results.aspx
25. ISMG. (2017). Healthcare information security today. Retrieved from http://www.healthcareinfosecurity.comlp-his-survey-2021.
26. https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023
27. https://www.breachsense.com/blog/data-breach-mitigation/
28. https://burningtree.co.uk/data-breaches-unveiled-lesson-learned-and-best-practices/#:~:text=1.,of%20their%20most%20valuable%20assets.
29. https://perception-point.io/guides/endpoint-security/7-data-leakage-prevention-tips-to-prevent-the-next-breach/
30. https://thecyberexpress.com/top-10-data-breaches-in-india-cybercrime/
31. https://www.getastra.com/blog/security-audit/list-of-data-breaches/
32. https://www.metacompliance.com/blog/cyber-security-awareness/emerging-technologies-and-their-impact
33. https://www.secoda.co/learn/most-common-types-of-data-security breaches#: ~:text=Security%20breaches%20can%20take%20various, across%20a%20multitude%20of%20industries.
34. https://www.lepide.com/blog/best-practices-for-your-data-breach-incident-response-plan/
35. https://www.eccu.edu/blog/technology/the-latest-cybersecurity-technologies-and-trends/

AUTHOR'S PROFILE

Raja Irfan Ahmad Mir hails from Jammu and Kashmir, India. He holds an MTech in CSE from Shri Mata Vaishno Devi University, Katra, Jammu and Kashmir. Having the Experience of more than 3 years in Teaching. Currently, he has approximately 6 publications in various journals. He currently works in the Multidisciplinary Research Unit at SKIMS, Soura, Jammu and Kashmir, India.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.