GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466

www.aarf.asia,**Email** : editoraarf@gmail.com

DATA BREACH INCIDENTS: TRENDS, IMPACTS AND MITIGATION STRATEGIES

ASST. PROF. VISHAL GANGADHAR AUTI
[Shri Swami Samarth Institute Of Management And Technology, Malwadi-Bota (MCA Department)],Ahamadnager

Abstract

Despite increasing data breach vulnerabilities, we know little about how organizations effectively identify and manage data breach incidents. To address this void, we conceptualize data breach incidents: trends, impact and mitigation strategies review. We conceptualize three areas of data breach risks (data breach Trends, data breach locus, and data breach impact) and Four forms of data breach Mitigation Strategies (Identify The Source Of The Breach And Deploy a Task Force, Secure Physical Areas Related To The Breach, Fix Vulnerabilities, Notify The Company And Relevant Parties) with detailed instances of each. As such, we provide a theoretical foundation for researchers to develop different types of risk management models in the context of data breaches. In addition, it provides insights for how practitioners can orchestrate actions for effective data breach management based on comprehensive profiles of risk items and resolution techniques. Lastly, themes and contextual information are translated into vulnerabilities, impacts, and mitigation efforts. The identified vulnerabilities, impacts, and mitigation efforts of the different breach type/location combinations aim to assist practitioners in the prevention and mitigation of cybersecurity breaches.

Keywords

Data Breaches, Trends, Incident Management, Distributed Denial of Service (DDoS), Literature Analysis, Industrial Control System (ICS), False Data Injection Attack (FDIA), Mitigation Strategies, Fix Vulnerabilities

Introduction

Data breaches involve large scale release of sensitive data to external parties whether intentionally or unintentionally and are regarded as important for information security with wide ranging impacts. Through a string of cyber-attacks on Indian government websites in 2021, hackers managed to lay their hands on a database that comprised the personal data of approximately 1500 Indian citizens. The hackers rendered the data public through PDF files that were available for download. Aadhaar data breach of 815 million citizens, India In October, Resecurity, an American cyber security company, said that the personally identifiable information of 815 million Indian citizens, including Aadhaar numbers and passport details, were being sold on the dark web. A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information). In this study conceptualizes data breach risks and resolutions as the basis for data breach research and management.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

What is a data breach?

A data breach is any security incident in which unauthorized parties gain access to sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) or corporate data (customer data records, intellectual property, financial information). The terms 'data breach' and 'breach' are often used interchangeably with 'cyberattack.' But not all cyberattacks are data breaches—and not all data breaches are cyberattacks. Data breaches include only those security breaches in which data confidentiality is compromised. So, for example, a distributed denial of service (DDoS) attack that overwhelms a website is not a data breach. But a ransomware attack that locks up a company's customer data and threatens to sell it for ransom, is a data breach—so is the physical theft of hard drives, thumb drives, or even paper files containing sensitive information. The global average cost of a data breach in 2023 was $4.45 million, a 15% increase over three years (IBM). Additionally, financial impacts have been researched by focusing on abnormal returns caused by data breaches, security breach announcement effects on market value, financial performance, and stock market returns.

Evolution of Cyber Attacks

Cybercrime has existed since the early days of computer networks, with ransomware attacks seen as early as 1989. The digitization of control systems in CI, which previously operated from electromechanical systems, embeds the vulnerabilities of the digital system. The opening for cyber attackers grows as CIs have evolved their operational technologies. More advanced malware has been developed over the past three decades, posing a constant threat to CIS. Many types of malware are being developed by professional software development organizations and purchased by cyber attackers. This division of malware development and deployment depends on the growing cybercrime economy. Over time, the complexity of malware has increased, and it is used for the ransom of computer systems and CI system sabotage. A modern attacker can source customized malware tools from third-party providers. Ransomware is expected to be more commonly experienced in CI through the Internet of Things (IoT) and CPS. While the technical specifics of a cyber attack can vary, the general flow of such attacks follows a trend. The trend in Industrial Control System (ICS) cyber attacks involves initiating a phishing attack to obtain access or insider access to facility computers. With access, a download or local pen drive can deliver spying and control malware. This malware carries out the primary sabotage actions, and then the exfiltration of the computer system is done, often preceded by a kill disk operation. The kill disk operation writes a binary zero value for all bits in the computer system storage, temporarily rendering it useless. An emerging type of attack is a False Data Injection Attack (FDIA) that targets the data stream of state estimation measurement outputs to cause the system operator to take incorrect control actions, which can have a detrimental physical and economic impact on the power system. The FDIA depends on three assumptions. A) is that the attacker has experience with power system operations and the capabilities of the targeted system. B) The attacker is capable of manipulating meter measurements. C) The attacker has knowledge of the network topology, system electrical parameters, an understanding of the SCADA system, and existing cybersecurity mechanisms.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

The 11 biggest data breaches of the 21st century

Data breaches affecting millions of users are far too common. Here are some of the biggest, baddest breaches in recent memory. Data breaches can affect hundreds of millions or even billions of people at a time. Digital transformation has increased the supply of data moving, and data breaches have scaled up with it as attackers exploit the data-dependencies of daily life. How large cyberattacks of the future might become remains speculation, but as this list of the biggest data breaches of the 21st Century indicates, they have already reached enormous magnitudes.

So, here it is – an up-to-date list of the 11 biggest data breaches in recent history.

1. Yahoo

Date: August 2013

Impact: 3 billion accounts

Securing the number one spot – almost seven years after the initial breach and four since the true number of records exposed was revealed – is the attack on Yahoo. The company first publicly announced the incident – which it said took place in 2013 – in December 2016. At the time, it was in the process of being acquired by Verizon and estimated that account information of more than a billion of its customers had been accessed by a hacking group. Less than a year later, Yahoo announced that the actual figure of user accounts exposed was 3 billion. Yahoo stated that the revised estimate did not represent a new "security issue" and that it was sending emails to all the "additional affected user accounts."

2. Aadhaar [tie with Alibaba]

Date: January 2018

Impact: 1.1 billion Indian citizens' identity/biometric information exposed

In early 2018, news broke that malicious actors has infiltrated the world's largest ID database, Aadhaar, exposing information on more than 1.1 billion Indian citizens including names, addresses, photos, phone numbers, and emails, as well as biometric data like fingerprints and iris scans. What's more, since the database – established by the Unique Identification Authority of India (UIDAI) in 2009 – also held information about bank accounts connected with unique 12-digit numbers, it became a credit breach too. This was despite the UIDAI initially denying that the database held such data.

3. Alibaba [tie with Aadhaar]

Date: November 2019

Impact: 1.1 billion pieces of user data

Over an eight-month period, a developer working for an affiliate marketer scraped customer data, including usernames and mobile numbers, from the Alibaba Chinese shopping website, Taobao, using crawler software that he created. It appears the developer and his employer were collecting the information for their own use and did not sell it on the black market, although both were sentenced to three years in prison.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

4. LinkedIn

Date: June 2021

Impact: 700 million users

Professional networking giant LinkedIn saw data associated with 700 million of its users posted on a dark web forum in June 2021, impacting more than 90% of its user base. A hacker going by the moniker of "God User" used data scraping techniques by exploiting the site's (and others') API before dumping a first information data set of around 500 million customers. They then followed up with a boast that they were selling the full 700 million customer database. While LinkedIn argued that as no sensitive, private personal data was exposed, the incident was a violation of its terms of service rather than a data breach, a scraped data sample posted by God User contained information including email addresses, phone numbers, geolocation records, genders and other social media details, which would give malicious actors plenty of data to craft convincing, follow-on social engineering attacks in the wake of the leak, as warned by the UK's NCSC.

5. Sina Weibo

Date: March 2020

Impact: 538 million accounts

With over 600 million users, Sina Weibo is one of China's largest social media platforms. In March 2020, the company announced that an attacker obtained part of its database, impacting 538 million Weibo users and their personal details including real names, site usernames, gender, location, and phone numbers. The attacker is reported to have then sold the database on the dark web for $250.

6. Facebook

Date: April 2019

Impact: 533 million users

In April 2019, it was revealed that two datasets from Facebook apps had been exposed to the public internet. The information related to more than 530 million Facebook users and included phone numbers, account names, and Facebook IDs. However, two years later (April 2021) the data was posted for free, indicating new and real criminal intent surrounding the data. In fact, given the sheer number of phone numbers impacted and readily available on the dark web as a result of the incident, security researcher Troy Hunt added functionality to his HaveIBeenPwned (HIBP) breached credential checking site that would allow users to verify if their phone numbers had been included in the exposed dataset.

"I'd never planned to make phone numbers searchable," Hunt wrote in blog post. "My position on this was that it didn't make sense for a bunch of reasons. The Facebook data changed all that. There's over 500 million phone numbers but only a few million email addresses so >99% of people were getting a miss when they should have gotten a hit."

7. Marriott International (Starwood)

Date: September 2018

Impact: 500 million customers

Hotel Marriot International announced the exposure of sensitive details belonging to half a million Starwood guests following an attack on its systems in September 2018. In a statement published in November the same year, the hotel giant said: "On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred."

8. Adult Friend Finder

Date: October 2016

Impact: 412.2 million accounts

The adult-oriented social networking service The FriendFinder Network had 20 years' worth of user data across six databases stolen by cyber-thieves in October 2016. Given the sensitive nature of the services offered by the company – which include casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, and Stripshow.com – the breach of data from more than 414 million accounts including names, email addresses, and passwords had the potential to be particularly damning for victims. What's more, the vast majority of the exposed passwords were hashed via the notoriously weak algorithm SHA-1, with an estimated 99% of them cracked by the time LeakedSource.com published its analysis of the data set on November 14, 2016.

10. MySpace

Date: 2013

Impact: 360 million user accounts

Though it had long stopped being the powerhouse that it once was, social media site MySpace hit the headlines in 2016 after 360 million user accounts were leaked onto both LeakedSource.com and put up for sale on dark web market The Real Deal with an asking price of 6 bitcoin (around $3,000 at the time).

According to the company, lost data included email addresses, passwords and usernames for "a portion of accounts that were created prior to June 11, 2013, on the old Myspace platform. In order to protect our users, we have invalidated all user passwords for the affected accounts created prior to June 11, 2013, on the old Myspace platform. These users returning to Myspace will be prompted to authenticate their account and to reset their password by following instructions."

11. NetEase

Date: October 2015

Impact: 235 million user accounts

NetEase, a provider of mailbox services through the likes of 163.com and 126.com, reportedly suffered a breach in October 2015 when email addresses and plaintext passwords relating to 235 million accounts were being sold by dark web marketplace vendor DoubleFlag. NetEase has maintained that no data breach occurred and to this day HIBP states: "Whilst there is evidence that the data itself is legitimate (multiple HIBP subscribers confirmed a password they use is in the data), due to the difficulty of emphatically verifying the Chinese breach it has been flagged as "unverified."

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

Data Breach Impact

When it comes to the consequences of data breach, the repercussions are far-reaching and deeply impactful. These breaches have evolved from mere cyber security issues to instigators of financial losses, reputational damage, legal troubles, regulatory fines, and a profound erosion of consumer trust.

According to the Check Point 2023 Mid-Year Security Report, there had been an 8% surge in global weekly cyber attacks in the second quarter of 2023, the most significant increase in two years, highlighting how attackers have cunningly combined next-gen AI technologies with long-established tools to conduct disruptive cyber attacks.

According to IBM's Cost of Data Breach Report 2023, 51% of organisations are planning to increase security investments as a result of a breach.

1. Data Breach Consequences: The Toll on Financial Loss

The financial impact of a data breach is undoubtedly one of the most immediate and hard-hitting consequences that organisations will have to deal with. According to IBM's Cost of Data Breach Report 2023, the average cost of a data breach reached an all-time high in 2023 of USD 4.45 million. This represents a 2.3% increase from the 2022 cost of USD 4.35 million.

Costs can include, compensating affected customers, setting up incident response efforts, investigating the breach, investment in new security measures, and legal fees, not to mention the eye-watering regulatory penalties that can be imposed for non-compliance with the GDPR (General Data Protection Regulation).

Organisations in breach of the GDPR can be fined up to 4% of annual global turnover or 20 Million Euros, whichever is greater. If organisations are under any illusion that these financial penalties will not be enforced, in May 2023, the Irish Data Protection Commission (DPC) imposed a historic fine of €1.2 billion on US tech giant Meta.

A breach can also significantly impact a company's share price and valuation. This is exactly what happened to Yahoo after it was breached in 2013. The breach was leaked in 2016 when the company was about to be bought over by US telecoms company Verizon. The acquisition went ahead with the company buying Yahoo for a discounted rate of $4.48 billion, around $350 million less than the original asking price.

2. Consequences of Data Breach: The Impact on Reputational Damage

The reputational damage resulting from a data breach can be devastating for a business. Research has shown that up to a third of customers in retail, finance and healthcare will stop doing business with organisations that have been breached. Additionally, 85% will tell others about their experience, and 33.5% will take to social media to vent their anger.

News travels fast and organisations can become a global news story within a matter of hours of a breach being disclosed. This negative press coupled with a loss in consumer trust can cause irreparable damage to the breached company.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

Consumers are all too aware of the value of their personal information and if organisations can't demonstrate that they have taken all the necessary steps to protect this data, they will simply leave and go to a competitor that takes security more seriously. A data breach can easily result in identity theft when sensitive information is exposed to unauthorised individuals. Hackers can use this information to steal a person's identity and commit fraudulent activities, such as opening new accounts or making unauthorised purchases.

Reputational damage is long-lasting and will also impact an organisation's ability to attract new customers, future investment and new employees to the company.

3. Data Breach Consequences: The Disruptive Effect of Operational Downtime

Business operations are significantly disrupted following a data breach. The aftermath demands containment of the consequences of data breach, prompting organisations to conduct extensive investigations into the breach's origins and the compromised systems.

Operations may need to be completely shut down until investigators get all the answers they need. This process can take days, even weeks to identify vulnerabilities, depending on the severity of the breach. This can have a huge knock-on effect on revenue and an organisation's ability to recover.

According to IBM's Cost of Data Breach Report 2023, the average time to identify and contain a breach is 277 days.

4. Consequences of Data Breach: Legal Implications and Actions

Under data protection regulations, organisations are legally bound to demonstrate that they have taken all the necessary steps to protect personal data. If this data security is compromised, whether it's intentional or not, individuals can seek legal action to claim compensation.

As the frequency and severity of data breaches continue to rise, we anticipate more of these group cases tied to the consequences of data breach being brought to court.

5. Data Breach Consequences: The Impact of Sensitive Data Loss

If a data breach has resulted in the loss of sensitive personal data, the consequences can be devastating. Personal data is any information that can be used to directly or indirectly identify an individual. This includes everything from, name, passwords, IP address and credentials. It also includes sensitive personal data such as biometric data or genetic data which could be processed to identify an individual.

The reality is that if a critical patient had their medical records deleted in a data breach it could have a serious knock-on effect on their medical treatment and ultimately their life. Biometric data is also extremely valuable to cybercriminals and worth a lot more than basic credit card information and email addresses. The fallout from breaches that expose this data can be disastrous and exceed any financial and reputational damage.

Regardless of how prepared your organisation is for a data breach, there's no room for complacency in today's evolving cyber security landscape, especially regarding the consequences of data breach. A coordinated security strategy must be in place to protect data privacy, mitigate threats, and safeguard your brand's reputation.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

MetaCompliance specialises in providing the best Cyber Security Awareness Training available on the market. Our products directly address the specific challenges that arise from cyber threats and corporate governance by making it easier for users to engage in cyber security and compliance. Get in touch for further information on how we can help transform cyber security training within your organization.

Data Breach Mitigation

What Is Data Breach Mitigation?

Data breach mitigation is the process of identifying and addressing any security vulnerabilities that cause data to be accessed, modified, or deleted without authorization. The goal of data breach mitigation is to reduce the risk of data loss and protect confidential information from unauthorized access. This might seem like an impossible task, but with the right measures in place and a well-thought-out response plan, you can minimize the impact of a data breach.

How To Go About Data Breach Mitigation

As stated before, data breaches happen regularly; however, what sets successful data breach mitigation efforts apart from the rest is proactive planning and preparedness. To prevent data breaches from turning into major disasters, it's important to have a solid response plan in place.

Below, I've outlined some steps you can take when a data breach occurs :

Step 1: Identify The Source Of The Breach And Deploy a Task Force

The first step in mitigating a data breach is to identify the source of the breach. This could be anything from a malicious hacker, an employee with access to sensitive information, or even an intentional leak.

Once the source has been identified, you should deploy a task force of security experts to investigate and assess the situation and recommend necessary steps for mitigation. Your security task force is your first line of defense against a data breach and should comprise experienced individuals or organizations who are familiar with your system and security protocols.

Ways to identify the source of a data breach include reviewing system logs, user activity monitoring, network traffic analysis, and penetration testing. You could also interview employees and review your organization's policies and procedures to determine if there were any gaps that allowed the breach to occur.

Step 2: Secure Physical Areas Related To The Breach

Yes, physical areas are just as important to secure in the event of a data breach. Experienced hackers can often use physical access points to gain entry into your system, so it's crucial to ensure these areas are secured and that any suspicious activity is reported immediately.

Your digital forensics team should coordinate with your physical security personnel to ensure all data entry points are secured and monitored. This should be done in a manner that doesn't disrupt the operations of your organization.

GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 12, Issue 03, March 2024 Impact Factor: 8.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editoraarf@gmail.com

Step 3: Fix Vulnerabilities

After completing the above steps, it's time to start fixing any vulnerabilities that may have led to a data breach. There are a lot of factors to consider when fixing vulnerabilities, from patching old software to updating security protocols.

Working with your security task force and digital forensics team to identify any vulnerabilities is a great place to begin. Start by analyzing security information and event management (SIEM) logs and try to understand the root cause. Once you can identify the root cause, you can fix the vulnerability and strengthen security measures.

Another important step is performing a vulnerability assessment. A vulnerability assessment is an audit of your systems, networks, and applications to identify any weaknesses or vulnerabilities that can be exploited.

For organizations that work with a lot of service providers, it's vital to perform a thorough third-party risk assessment. This will help you identify any vulnerabilities in your service providers' systems and networks that could potentially lead to a data breach.

Step 4: Notify The Company And Relevant Parties

Companies must adhere to certain regulations when reporting a security breach that affects personal data, such as the EU's General Data Protection Regulation (GDPR) which requires notification of the Data Protection Authority within 72 hours.

As soon as you identify the source of the breach, notify relevant parties. This includes your customers, any affected business partners or vendors, law enforcement, and data protection authorities.

Notifying affected parties helps prevent further damage and demonstrates that your organization is taking responsibility for the breach. It's also a good opportunity to reassure your customers that you take their data protection and privacy seriously and are taking necessary steps to mitigate any potential damage from the incident.

Conclusion

Taking the right steps when responding to a data breach can be the difference between success and failure. The key is to act quickly, identify the source of the breach, and fix any vulnerabilities. Doing so will help you mitigate further damage and demonstrate that your organization takes data protection and privacy seriously.

References

1. Baskerville, R., Spagnoletti, P., and Kim, J. 2014. "Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response," Information & Management (51:1), pp. 138-151.
2. Benaroch, M., Chernobai, A., and Goldstein, J. 2012. "An Internal Control Perspective on the Market Value Consequences of IT Operational Risk Events," International Journal of Accounting Information Systems (13:4), pp. 357-381.
3. Breach Level Index. 2018. "Data Privacy and New Regulations Take Center Stage," Gemalto

4. Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "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 (9:1), pp. 69-104.
5. Ahmad, A., Maynard, S.B., and Shanks, G. 2015. "A Case Analysis of Information Systems and Security Incident Responses," International Journal of Information Management (35:6), pp. 717-723.
6. Modi, C., Patel, D., Borisaniya, B., Patel, A., and Rajarajan, M. 2013. "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," Journal of Super Computing (63:2), pp. 561-592.
7. Ogie, R. 2016. "Bring Your Own Device: An Overview of Risk Assessment," IEEE Consumer Electronics Magazine (5:1), pp. 114-119.
8. Ryan, J.J., Mazzuchi, T.A., Ryan, D.J., De la Cruz, J.L., and Cooke, R. 2012. "Quantifying Information Security Risks Using Expert Judgment Elicitation," Computers & Operations Research (39:4), pp. 774- 784.
9. Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," Journal of Management Information Systems (32:2), pp. 314-341.
10. Shameli-Sendi, A., Aghababaei-Barzegar, R., and Cheriet, M. 2016. "Taxonomy of Information Security Risk Assessment (Isra)," Computers & Security (57), pp. 14-30.