Gurukul International Multidisciplinary
Research Journal (GIMRJ)*with*
International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0044

e-ISSN No. 2394-8426
Special Issue on
Cyber Crime and Social Media
Issue–III(II), Volume–XIII

A Study of the Impact of Data Breaches at the Wake of Third-Party Services Lapses

***Dr. Sulok Birendrasingh Raghuwanshi**
Assistant Professor in English
Orange City College of Social Work, Nagpur
Mob.: 9850394582
E-Mail: sulokraghuwanshi@rediffmail.com

Abstract:
Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, unauthorized access, or damage. Data breaches can lead to significant financial losses, not only from immediate expenses but also from lost clientele, penalties, and legal costs. A large number of breaches remain undetected for months or even years, complicating the assessment and mitigation of damage in a timely manner. The goal is to safeguard sensitive information, prevent data breaches, and maintain the integrity, confidentiality, and availability of data. The paper aims at underlining the impact data breaches leading to significant financial losses, highlighting the breaches happening due to weaknesses in third-party services or partners and discuss the problem of sensitive information being frequently targeted aiming for identity theft.. There is a need to insist on the need to keep systems updated with the most recent security patches.

Introduction:

Cybersecurity is a field focused on protecting computer systems, networks, and data from digital attacks, damage, or unauthorized access. With the growing reliance on technology and the internet, cybersecurity has become essential to safeguard sensitive information, prevent financial loss, and protect personal privacy. Cybersecurity refers to the practice of protecting systems, networks, and programs from digital attacks, unauthorized access, or damage. The goal is to safeguard sensitive information, prevent data breaches, and maintain the integrity, confidentiality, and availability of data. The **Network Security** protects computer networks from unauthorized access, attacks, or data breaches. This includes firewalls, intrusion detection systems, and secure VPNs. An **Information Security** Ensures that sensitive data is only accessible to authorized users. It includes encryption, data masking, and access control. An **Application Security** focuses on ensuring that software and applications are free from vulnerabilities that hackers can exploit. **The Endpoint Security** protects devices (like computers, smartphones, and tablets) that connect to the network, ensuring they are secure from malware or unauthorized access. On the other hand, the **Cloud Security** protects data stored in cloud environments from cyber threats, ensuring that the cloud infrastructure is safe and that sensitive information is properly encrypted. An **Incident Response** is a structured approach to responding to and managing a cybersecurity breach or attack. This includes identification, containment, and recovery. And finally, a **Disaster Recovery and Business Continuity** plans and processes that ensure an organization can recover from cyberattacks or other disruptions to its IT infrastructure and continue its operations Yuchong Li and Qinghui Liu (2021).

Objectives:

1. To discuss the problem of sensitive information being frequently targeted aiming for identity theft.
2. To underline the impact data breaches leading to significant financial losses.
3. To highlight the breaches happening due to weaknesses in third-party services or partners.
4. To bring forth the problem of data breaches remaining undetected, complicating the assessment and mitigation of damage in a timely manner.
5. To insist on the need to keep systems updated with the most recent security patches.

Hypothesis:

Sensitive information such as credit card details, social security numbers, and personal addresses are frequently targeted, often aiming for identity theft. Data breaches can lead to significant financial losses, not only from immediate expenses but also from lost clientele, penalties, and legal costs. Numerous breaches happen due to weaknesses in third-party services or partners. A large number of breaches remain undetected for months or even years, complicating the assessment and mitigation of damage in a timely manner. Thus there is need of keeping systems updated with the most recent security patches is essential to prevent attackers from taking advantage of known vulnerabilities.

Research Methodology:

The primary causes and impacts of data breaches in cybersecurity, and how can organizations improve their cybersecurity measures to prevent breaches were explored. Previous studies on data breaches published in journals or other cybersecurity-focused publications were reviewed.

Literature Review:

Long Cheng, et. al. (2017) A data breach is the intentional or inadvertent exposure of confidential information to unauthorized parties. In the digital era, data has become one of the most critical components of an enterprise. Data leakage poses serious threats to organizations, including significant reputational damage and financial losses. As the volume of data is growing exponentially and data breaches are happening more frequently than ever before, detecting and preventing data loss has become one of the most pressing security concerns for enterprises. Despite a plethora of research efforts on safeguarding sensitive information from being leaked, it remains an active research problem. This review helps interested readers to learn about enterprise data leak threats, recent data leak incidents, various state-of-the-art prevention and detection techniques, new challenges, and promising solutions and exciting opportunities.

Pallavi Murghai Goel (2019) The term cyber security is often employed interchangeably with the term protection of information. This paper argues that while cyber security and information protection are significantly similar, these two terms are not completely comparable. In addition, the paper argues that cyber security stretches beyond conventional information security definitions to include not only the protection of information data, but also that of other properties, including the individual himself. In information protection, reference to the human factor is generally linked to human's role(s) in the process of protection. In cyber security this aspect has a further element, namely, humans as possible targets of cyber-attacks or even engaging unknowingly in a cyber assault. This additional aspect has ethical consequences for society as a whole, as it may be seen as a social obligation to protect such marginalized groups, for example children.

Omar F. Keskin et. al (2021) Cybersecurity is a concern for organizations in this era. However, strengthening the security of an organization's internal network may not be sufficient since modern organizations depend on third parties, and these dependencies may open new attack paths to cybercriminals. Cyber Third-Party Risk Management (C-TPRM) is a relatively new concept in the business world. All vendors or partners possess a potential security vulnerability and threat. Even if an organization has the best cybersecurity practice, its data, customers, and reputation may be at risk because of a third party. Organizations seek effective and efficient methods to assess their partners' cybersecurity risks. In addition to intrusive methods to assess an organization's cybersecurity risks, such as penetration testing, non-intrusive methods are emerging to conduct C-TPRM more easily by synthesizing the publicly available information without requiring any involvement of the subject organization. In this study, the existing methods for C-TPRM built by different companies are presented and compared to discover the commonly used indicators and criteria for the assessments. Additionally, the results of different methods assessing the cybersecurity risks of a specific organization were compared to examine reliability and consistency. The results showed that even if there is a similarity among the results, the provided security scores do not entirely converge.

Michel Benaroch (2021) Growing reliance on third-party services, such as cloud computing, is believed to increase client firms' exposure to third-party induced cyber incidents. However, we lack empirical research on the prevalence and scale of third-party induced cyber incidents. Moreover, we do not know who pays more of the price for experiencing these incidents—the client firm and/or the third-party provider firm. Third-party induced cyber incidents are not growing in prevalence any faster than other incidents, but they do compromise greater volumes of confidential data per incident. As to the price paid for third-party induced incidents, the picture is more nuanced. Client (first-party) firms suffer drops in equity returns that are comparable to those for homegrown incidents, while small third-party provider firms suffer significantly larger drops in equity returns and large third-party provider firms do not suffer a discernible drop in equity returns. We discuss implications of these findings for client firms and service providers.

What is Cybersecurity?

Cybersecurity refers to the practice of protecting computers, servers, networks, and data from unauthorized access, attacks, damage, or theft. This is crucial in an era where the internet and technology have become central to businesses, governments, and individuals alike. Protecting the integrity and confidentiality of data as it is transmitted across or accessed via networks. Ensuring that data is protected from unauthorized access or disclosure, securing software applications from vulnerabilities that could be exploited by attackers, protecting devices (laptops, smartphones, etc.) from threats, such as malware. Systems that ensure the right individuals can access the right resources at the right time, often involving multi-factor authentication. The key question is how organizations respond to and recover from cybersecurity incidents like data breaches or ransomware attacks? **Anand Shinde (2021)**

Current Trends in Cybersecurity:

1. **AI and Machine Learning in Cybersecurity**: AI and machine learning are increasingly being integrated into cybersecurity tools for anomaly detection, threat hunting, and automating responses to potential threats. These technologies can analyze vast amounts of data to predict and prevent cyberattacks in real-time.
2. **Ransomware Attacks**: Ransomware has been a growing threat, with attackers encrypting victims' data and demanding payment in exchange for decryption keys. These attacks have increasingly targeted critical infrastructure, healthcare, and large enterprises.
3. **Cloud Security**: As more businesses move to cloud services, ensuring the security of cloud data and applications is more important than ever. Misconfigured cloud settings, weak access controls, and inadequate encryption are among the risks that companies face.
4. **Supply Chain Attacks**: Cyber attackers are increasingly targeting third-party vendors to gain access to larger organizations' networks. These supply chain attacks can be difficult to detect and can cause widespread damage.
5. **Zero Trust Security Models**: The zero-trust model assumes that both internal and external networks could be compromised and requires continuous verification and authentication for every user and device trying to access company resources **Professor Andrea Baronchelli and Elohim Reis (2024).**

What is a Data Breach?

A data breach occurs when an unauthorized person or entity gains access to sensitive information such as personal data, financial details, or intellectual property, which is often stored electronically. These breaches can involve hacking, unintentional leaks, or even insider threats.

Types of Data Breaches:

1. **Hacking and IT System Intrusion**: Unauthorized access is gained to a company's network, often through exploiting vulnerabilities in software or systems.
2. **Phishing**: Attackers trick individuals into providing sensitive information by posing as legitimate sources.
3. **Physical Theft**: Laptops or storage devices containing personal or company data are stolen.
4. **Insider Threats**: Employees or contractors intentionally or unintentionally leak information.
5. **Accidental Exposure**: Improper disposal of physical records or unencrypted data being made public.

Instances of Data Breaches (In the Last and Current Decade):

1. **Target Data Breach (2013)**:
   Hackers gained access to Target's point-of-sale systems, stealing credit and debit card information from around 40 million customers, along with personal data from 70 million people. The breach illustrated the risks posed by third-party vendors, as the initial point of entry was a vendor's compromised credentials. It also underscored the need for robust encryption and tokenization methods to protect payment card data.
2. **Yahoo Data Breach (2013-2014)**:

In what became one of the largest data breaches in history, hackers stole information from all 3 billion Yahoo accounts. This included personal information such as names, email addresses, phone numbers, birth dates, and in some cases, encrypted passwords. The breach highlighted the vulnerability of legacy systems and the importance of up-to-date encryption. It also demonstrated the risks of not having a proactive response plan and transparency with users.

3. **Equifax Data Breach (2017)**:
   Personal data, including Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers, of 147 million Americans was compromised. The breach was caused by vulnerability in Apache Struts, a popular open-source web framework. This breach is a key example of the importance of promptly patching known vulnerabilities. In this case, a patch had been available for two months before the breach occurred, emphasizing the risks of delayed updates.
4. **Marriott Hotels Data Breach (2018)**:
   Marriott disclosed that data from up to 500 million customers was stolen, including passport numbers, travel information, and in some cases, payment card details. The breach went undetected for four years. The breach showed the long-term risks of weak monitoring systems and poor integration of acquired company systems. It also stressed the importance of strong security measures for sensitive personal information, such as encryption and access controls.
5. **Facebook (Cambridge Analytica) Scandal (2018)**:
   While technically not a data breach in the traditional sense, this incident saw the misuse of personal data of around 87 million Facebook users. Data was harvested through a third-party app without consent, and shared with political consulting firm Cambridge Analytica. The event sparked debates on data privacy, user consent, and the responsibility of platforms to safeguard users' information. It highlighted the need for companies to be transparent about data usage and third-party access.
6. **T-Mobile Data Breach (2021)**:
   The personal data of over 40 million customers was compromised, including names, phone numbers, and driver's license information. The breach occurred through vulnerability in T-Mobile's network. This breach caused serious concerns about mobile carriers' ability to protect sensitive data.
7. **Facebook (2021)**:
   Data from 530 million Facebook users was leaked online, including phone numbers and other personal details. The data had been scraped from the site due to a security vulnerability that was later fixed. This breach demonstrated the risks of large-scale data scraping, even if the data is not technically stolen through hacking.
8. **Uber Data Breach (2022)**:
   Hackers exploited vulnerability in Uber's network to access sensitive company data, including internal tools and information about its employees. Uber faced public scrutiny over its cybersecurity practices, with additional concerns regarding the safety of user data.

9. **Optus Data Breach (2022)**:
   Personal data, including Medicare numbers, was stolen from 10 million Australians when Optus' network was hacked. The breach triggered significant concerns about data security in telecommunications and the role of encryption.
10. **Australian Broadcasting Corporation (ABC) Data Breach (2023)**:
   In one of the latest breaches, a hacker gained access to employee information, including sensitive personal details. ABC had to evaluate its internal security measures and implement stricter access protocols to prevent future incidents **A. A. Jamal et. al. (2023)**.

Discussions and Analysis:

Personal data like credit card numbers, Social Security numbers, and addresses are commonly targeted, often with the goal of identity theft. Data breaches can result in huge financial losses, not just from the immediate costs but from lost customers, fines, and legal settlements. Many breaches occur through vulnerabilities in third-party services or partners (e.g., Target, Home Depot, and Capital One), emphasizing the need for comprehensive vendor risk management. Many breaches go unnoticed for months or years, making the damage harder to assess and mitigate in a timely manner.

Cybersecurity Best Practices:

1. **Regular Patching**: Ensuring that systems are up-to-date with the latest security patches is crucial in preventing attackers from exploiting known vulnerabilities.
2. **Encryption**: Data should be encrypted both in transit and at rest to prevent unauthorized access.
3. **Multi-factor Authentication (MFA)**: Using MFA adds an additional layer of security, ensuring that even if credentials are stolen, attackers still cannot access systems without the second factor.
4. **Employee Training**: Employees should be regularly trained on recognizing phishing attempts, following password protocols, and reporting suspicious activity **Joseph Steinberg (2019)**.

Conclusion:

Sensitive information such as credit card details, social security numbers, and personal addresses are frequently targeted, often aiming for identity theft. Data breaches can lead to significant financial losses, not only from immediate expenses but also from lost clientele, penalties, and legal costs. Numerous breaches happen due to weaknesses in third-party services or partners (like Target, Home Depot, and Capital One), highlighting the importance of thorough vendor risk management. A large number of breaches remain undetected for months or even years, complicating the assessment and mitigation of damage in a timely manner. Keeping systems updated with the most recent security patches is essential to prevent attackers from taking advantage of known vulnerabilities. This shall provide an extra layer of protection, guaranteeing that even if login information is compromised, intruders will still be unable to gain access to systems without the secondary authentication factor. Staff should receive regular training on how to identify phishing attempts, adhere to password guidelines, and report any unusual activities.

Suggestions and Recommendations:

1. Sensitive information should be secured from any kind of identity theft.
2. The efforts should be taken for the elimination of weaknesses in third-party services or partners, highlighting the importance of thorough vendor risk management.
3. The system or mechanism should be created, updated and promoted for breaches remaining undetected, avoiding the complication in the assessment and mitigation of damage in a timely manner.
4. The systems should be updated with the most recent security patches for preventing attackers from taking advantage of known vulnerabilities.

Work cited:

Primary Sources:

- Baronchelli, Professor Andrea. and Elohim Reis "How data science can help us to tackle illegaltrade in the dark web." *The Allen Turing Institute* 17th April, 2024 https://www.turing.ac.uk/blog/how-data-science-can-help-us-tackle-illegal-trade-dark-web \
- Benaroch, Michael. "Third-party Induced Cyber Incidents—Much Ado about Nothing?" *Journal of Cybersecurity*, 7 (1), DOI: 10.1093/cybsec/tyab020
- Chang, Long. (2017), Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions: Enterprise Data Breach. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7 (C), DOI:10.1002/widm.1211
- Goel, Pallavi Murghai. (2019), A Literature Review of Cybersecurity. *IJRAR*, 6 (2), DOI: IJRAR1CBP189
- Jamal, A. A., et. al. (2023). A review on security analysis of cyber physical systems using Machine learning. *Materials today: proceedings*, *80*, 2302-2306.
- Keskin, Omar F., et. al. (2021). Cyber Third-Party Risk Management: A Comparison of Non-Intrusive Risk Scoring Reports. *Electronics*, 10 (10), DOI: www.researchgate.net/publication/351567274_
- Shinde, Anand. (2021). *Introduction to Cyber Security*. Notion Press
- Steinberg, Joseph. (2019). *Cybersecurities for Dummies*. Wiley

Secondary Sources:

- "26 billion records exposed in "Mother of All Breaches": Report". *The Times of India. 2024-01-29*. ISSN 0971-8257. Retrieved 2025-01-11.
- "Data breach costs will soar to $2T: Juniper", CUNA, May 15, 2015\
- Jump up to:ª "Data Breach Industry Forecast", Experian (2015)
- "Data breaches compromised 4.5bn records in half year 2018 – Gemalto", The Citizen, October 17, 2018
- "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016". *Forrester. Archived from* the original *on 2025-1-17.*
- "Massive data breach containing more than 26 billion leaked records". *WKBW TV | Buffalo, NY. Jan 25, 2025 – via YouTube.*
- *Song, Victoria (17 January 2019).* "Mother of All Breaches Exposes 773 Million Emails, 21 Million Passwords". *Gizmodo*. Retrieved 2015-01-18.
- Winder, Davey *(Jan 23, 2024).* "Warning As 26 Billion Records Leak: Dropbox, LinkedIn, Twitter Named". Forbes. Retrieved 2025-03-1.