LatIA. 2025; 3:333
doi: 10.62486/latia2025333
ISSN: 3046-403X

ORIGINAL

From Past to Present: The Evolution of Data Breach Causes (2005–2025)

Del Pasado al Presente: La Evolución de las Causas de Filtraciones de Datos (2005-2025)

Amit Singh[1]

[1]Cisco Systems (United States). San Jose, United States.

Cite as: Singh A. From Past to Present: The Evolution of Data Breach Causes (2005–2025). LatIA. 2025; 3:333. https://doi.org/10.62486/latia2025333

Submitted: 28-05-2024 **Revised:** 18-09-2024 **Accepted:** 23-03-2025 **Published:** 24-03-2025

Editor: PhD. Rubén González Vallejo

Corresponding Author: Amit Singh

ABSTRACT

This review aims to analyze the changing causes of data breaches over two decades by synthesising evidence from various data breach investigation reports and regulatory filings. The methodology involves examining trends in threat actors, actions, and motives identified in reports such as the Verizon Data Breach Investigations Report (DBIR) series from 2008 to 2024, California Attorney General's reports, and the Privacy Rights Clearinghouse. The findings reveal an evolution through distinct phases: an initial period (roughly 2008-2010) dominated by external breaches leveraging hacking and malware, a subsequent era (2011-2019) marked by the rise of sophisticated cybercrime, including increased phishing and the emergence of defined incident patterns, and a more recent epoch (2020-2024) characterized by a significant surge in ransomware attacks, exploitation of systemic vulnerabilities, and the convergence of financially motivated and nation-state actors. Throughout these periods, human factors and errors have consistently contributed to successful breaches. In conclusion, the landscape of data breaches have shifted from simpler external attacks to more complex and disruptive campaigns, where human vulnerabilities remain a key enabler, and the emerging landscape includes AI-driven threats that are being explored by both attackers and defenders, necessitating continuous adaptation of defence strategies to address both traditional weaknesses and novel AI-related risks.

Keywords: Data Breach; Threat Actors; Cybersecurity; Compromised Data; AI-Driven Threats; Ransomware; Phishing; Personal Identifiable Information.

RESUMEN

Esta revisión tiene como objetivo analizar las causas cambiantes de las filtraciones de datos a lo largo de dos décadas, sintetizando evidencia de diversos informes de investigaciones sobre filtraciones de datos y presentaciones regulatorias. La metodología implica examinar las tendencias en actores de amenazas, acciones y motivaciones identificadas en informes como la serie Verizon Data Breach Investigations Report (DBIR) de 2008 a 2024, los informes del Fiscal General de California y el Privacy Rights Clearinghouse. Los hallazgos revelan una evolución a través de distintas fases: un período inicial (aproximadamente 2008-2010) dominado por filtraciones externas que empleaban hacking y malware, una era posterior (2011-2019) marcada por el auge del ciberdelito sofisticado, con un aumento del phishing y la aparición de patrones de incidentes bien definidos, y una etapa más reciente (2020-2024) caracterizada por un incremento significativo de los ataques de ransomware, la explotación de vulnerabilidades sistémicas y la convergencia de actores motivados financieramente con actores estatales. A lo largo de estos períodos, los factores humanos y los errores han contribuido constantemente al éxito de las filtraciones de datos. En conclusión, el panorama de

las filtraciones de datos ha pasado de ataques externos más simples a campañas más complejas y disruptivas, donde las vulnerabilidades humanas siguen siendo un factor clave. Además, el escenario emergente incluye amenazas impulsadas por IA, exploradas tanto por atacantes como por defensores, lo que hace necesario adaptar continuamente las estrategias de defensa para abordar tanto debilidades tradicionales como riesgos novedosos relacionados con la inteligencia artificial.

Palabras clave: Filtración de Datos; Actores de Amenazas; Ciberseguridad; Datos Comprometidos; Amenazas impulsadas por IA; Ransomware; Phishing; Información Personal Identificable.

INTRODUCTION

Data breaches have escalated from isolated incidents to systemic threats, with global costs projected to reach \$10,5 trillion annually by 2025.[6] Understanding what constitutes a "data breach" is crucial for data security and privacy. A data breach occurs when there is unauthorized access or disclosure of personal information, or when such information is lost. The Privacy Act does not define these terms explicitly, so they rely on their ordinary meanings. Unauthorized access can occur if someone without permission views personal information, such as an employee accessing sensitive records or an external attacker infiltrating a network. Unauthorized disclosure occurs when personal information is unintentionally or intentionally shared with others outside the entity, like an employee mistakenly publishing confidential data online. The loss of personal information occurs when it is accidentally misplaced, potentially leading to unauthorized access or disclosure, such as leaving it on public transport. The transition from physical record theft to AI-powered cyberattacks has fundamentally altered organizational risk profiles. Although the existing literature documents individual breaches, few studies holistically map causation trends across the dimensions of technological, regulatory, and criminal innovation.

This study delves into an in-depth exploration of the topic at hand, highlighting a comprehensive review that addresses two significant goals:

1. Identify the evolving tactics and techniques used by threat actors in data breaches over time, with a focus on the increasing sophistication of attacks.
2. Evaluation of countermeasure effectiveness against evolving attack vectors.

The significance of the study lies in its synthesis of technical post-mortems, regulatory filing analyses, and longitudinal compliance data - a tripartite approach absent in prior sector-specific studies.

Threat Actor

For the last two decades, FBI IC3 (Internet Crime Complaint Center) has published cybercrime reports annually[7] The report suggests that during the initial commercial internet era (the early 2000s), the leading cyber complaints were regarding not getting the delivery of items ordered online. Ever since the primary type of cybercrime has been Phishing against Corporations and individuals. Data breach plays a pivotal role in successful phishing attempts. Various kinds of malicious and non-malicious entities are involved in a Data Breach. These attackers range from curious tech enthusiasts to organized cybercriminals:

- The first among them are the amateurs. They are tech enthusiasts who do not wish to create actual harm but want to exploit a system to show off their skills to peers and sometimes a community. These users don't have a lot of resources. But the knowledge and skills required can be quickly gained from the internet and Generative AI.
- The second group of potential attackers consists of organized hackers. This category includes cybercriminal organizations, terrorists, and state-sponsored attackers. Cybercriminals focus on exploiting data for financial gain and operate with a high level of organization and sophistication. Terrorists may initiate data breaches to assert their presence or power, often instilling fear in the public. They may also use the acquired data to harm society. State-sponsored attackers work on behalf of government entities. These individuals are highly trained, well-funded, and tasked with gathering intelligence for their respective states.
- The third in the list are the consumer and operator mistakes. To err is human. Corporate employees handle the user data and maintain an organized system. They can expose the data erroneously, causing data exposure and leading to an exploit by a malicious entity. The consumers are also responsible for data security. They may not be as obligated as the providers are, but they are a critical part of the entire data ecosystem. Many a time, consumers choose convenience over security. They feel that providers are solely responsible for data security. Weak passwords and their reuse across multiple accounts, not verifying a link before using it, and posting sensitive information on social media can all lead to a data breach.

- The fourth type of potential attackers can be an insider attack or a compromised, trusted entity. The entities inside the organization trust the model, and a person or a system has certain privileges to get work done. If these entities get compromised, they can break the trust chain of the organization. Using social engineering methods to compromise corporate users to gain unauthorized access is a popular method of data reach. In another scenario, a disgruntled employee who feels they have not been treated well by the organization can facilitate a data breach.
- The fifth type includes physical attacks, such as device theft, document theft, and improper disposal of legacy systems.

Threat Vector

Threat vectors in cybersecurity refer to the methods or paths through which cybercriminals can gain unauthorized access to a system, network, or sensitive data. Understanding these threat vectors is crucial for developing effective defense mechanisms and mitigating potential risks. Over the past two decades, the landscape of threat vectors has evolved significantly, driven by advancements in technology, changes in cybercriminal tactics, and the increasing complexity of digital systems.

Early Threat Vectors

- SQL Injection: attackers exploited web application vulnerabilities to inject malicious SQL code, manipulating databases to extract sensitive information.
- Unencrypted Storage: sensitive data stored without encryption was easily accessible upon gaining access to the storage medium.
- Phishing Attacks: deceptive emails and websites tricked individuals into revealing sensitive information like passwords and credit card numbers.

Evolving Sophistication (Rise of Organized Cybercrime)

- Advanced Persistent Threats (APTs): nation-state actors and organised cybercriminal groups conducted prolonged, targeted attacks to steal sensitive information from governments and corporations.
- Ransomware: ransomware attacks have become a significant threat in the cybersecurity landscape, where cybercriminals encrypt victims' data and demand payment for decryption keys. As these attacks have become more common and financially rewarding, they continue to extort money from individuals and organizations eager to restore access to their critical files. It is important to note that a large portion of malware incidents reported today involves ransomware, highlighting the urgent need for enhanced security measures.
- Cloud Misconfigurations: the shift to cloud computing introduced new vulnerabilities, with misconfigured cloud services becoming targets for data breaches.
- Compromised Web Servers: generic hacking, phishing, and browser-busting malware lead known threat actions.

Recent Sophisticated and Automated Vectors

- AI-Driven Threats: cybercriminals leverage AI to automate and enhance attacks, using Generative Adversarial Networks (GANs) to create realistic phishing attempts and machine learning to identify and exploit vulnerabilities efficiently.
- Supply Chain Attacks: attackers target third-party vendors and suppliers to gain access to their clients' systems. The shared vector for major scenarios includes third-party remote-access software.
- IoT Device Vulnerabilities: the proliferation of Internet of Things (IoT) devices introduces new attack surfaces and vulnerabilities.

It's important to consider that remote access established by the attacker is important, and there are various ways of creating persistent access.

METHOD

Contextualizing the Data Breach Landscape

Data breach notification has become a crucial legal requirement in many countries, empowering consumers with the right to know if their personal information has been compromised. In California, for example, the California Consumer Privacy Act (CCPA)mandates that organizations promptly report any data breaches. Similar legislation exists across various states in the US, all enforced by their respective Departments of Justice.

Our study delved into the evolution of data breaches by analyzing numerous reports, particularly the Verizon Data Breach Investigations Report (DBIR). We explored how data breaches affect various industries, seeking correlations between a sector's vulnerability and its overall business value or security practices.

In our examination, we also emphasized the pivotal role of compliance in protecting data and privacy. Almost all nations acknowledge the importance of data protection, leading to the establishment of legal frameworks that dictate how consumer information must be secured and the types of data organizations can collect. Noteworthy regulations, such as the CCPA in USA, Privacy Act 1988 in Australia and the General Data Protection Regulation (GDPR) in Europe, impose stringent data protection standards on organizations.[2,9,10] Noncompliance with these regulations can lead to substantial penalties, reinforcing the empowerment of consumers to be informed about and control the use of their data.

Lastly, we reflected on the evolution of mitigation and response strategies over the past two decades, recognizing the ongoing need for organizations to adapt to an ever-changing threat landscape.

Primary Data Sources

- Verizon Data Breach Investigations Report (DBIR 2008-2024): the Verizon Data Breach Investigations Report (DBIR) is a well-established publication aimed at informing security practitioners about real-world cybercrime trends. Its purpose is to deliver data-driven insights into common threats, raise awareness of attacker tactics, encourage executive support for security initiatives, and highlight the importance of security to employees. By analyzing data breaches and security incidents, the DBIR seeks to provide actionable insights that help organizations better protect themselves against prevalent threats.
- California Consumer Privacy Act (CCPA): California law requires a business or state or local agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. Below is a list of those sample breach notices. We studied more than 4400 of this reports.
- Privacy Rights Clearinghouse: the Privacy Rights Clearinghouse (PRC) is a nonprofit organization dedicated to advocating for consumers' privacy rights and enhancing access to information and policy discussions related to data privacy. PRC helps individuals protect their privacy through advocacy, education, and outreach. Its mission is to raise awareness about privacy issues and provide practical resources. The organization has played a crucial role in increasing awareness of data breaches. Our study examined PRC reports from 2005 to 2019.

RESULTS

Year	Metric	Details
2004-2007	**Attack Origin**	Data compromises more likely from external attacks; insider events relatively stable.
2008	**Records Compromised**	**Milestone year:** More records breached than any single year prior or previous years combined.
2010	**Dataset Size**	DBIR series spanned six years, **900+ breaches, and over 900 million compromised records.**
2011	**Geographic Scope**	**36 countries** hosted victim organizations, surpassing 2010's 22 countries.
2012	**Dataset Size**	Largest dataset covered: **47,000+ security incidents and 621 confirmed data disclosures.** Over nine years, exceeded 2,500 data disclosures and 1.1 billion compromised records.
2013	**Geographic Scope**	Breaches affected organizations in **27 countries.**
2014	**Geographic Scope**	Breaches affected organizations in **95 countries**, a 350% increase from 2013.
2014	**Incident Count**	**1,367 incidents** with confirmed data compromise, the most in ten years and the first time crossing 1,000.
2012-2015	**California Records Breached**	Nearly **50 million records** of Californians breached.
2019	**Breach Impact**	Data breaches continued to make headlines, impacting organizations of all sizes across all industries.
2020	**Dataset Size**	**157,525 incidents analyzed**, with 32,002 meeting quality standards and 3,950 confirmed data breaches.
2022	**Dataset Characteristics**	Dataset was very large and complex, capturing many different types of data points and growing larger each year.
2023	**Dataset Size**	**16,312 security incidents analyzed, 5,199 confirmed data breaches.** Dataset contains 953,894 incidents, 254,968 confirmed breaches.
2023	**Sector Impact**	The Information sector experienced substantially fewer incidents compared to the previous year, while overall breach sample size increased.
2024	Milestone	Onboarded a good number of new contributors and reached an exciting milestone of more than **10,000 breaches analyzed in a single edition**

Figure 1. Trend Summary Table

Data breaches have demonstrated a clear trend of increasing frequency, expanding geographic scope, and evolving attack vectors over the years. Initially, external attacks were the primary concern, but as time has progressed, threat actors have adopted more sophisticated tactics. In recent years, there has been significant growth in attacks that involve the exploitation of vulnerabilities as the critical path to initiate a breach, with web applications serving as the main entry points for these attacks. This shift underscores the importance of robust vulnerability management and web application security. The table below summarizes the data breach trends observed during our study.

The sectors targeted by data breaches have evolved over time. While all organizations face risks, specific sectors are particularly appealing to attackers because of the valuable data they contain. An analysis of the CCPA data breach database reveals that data breaches are a widespread and growing issue across various sectors in the United States. The consistent increase in breaches since 2005, along with billions of records compromised, highlights significant vulnerabilities in data security. Hacking is a primary cause, but insider threats and physical breaches also contribute substantially. Healthcare, business, and academic institutions are especially vulnerable, likely due to the large amounts of sensitive personal information they manage. This variability among sectors emphasizes the need for tailored security strategies that specifically address each industry's unique threats and vulnerabilities. The accompanying 3D pie chart (figure 2) illustrates the percentage of data breaches reported across various industries, with healthcare and business showing the highest levels of impact.

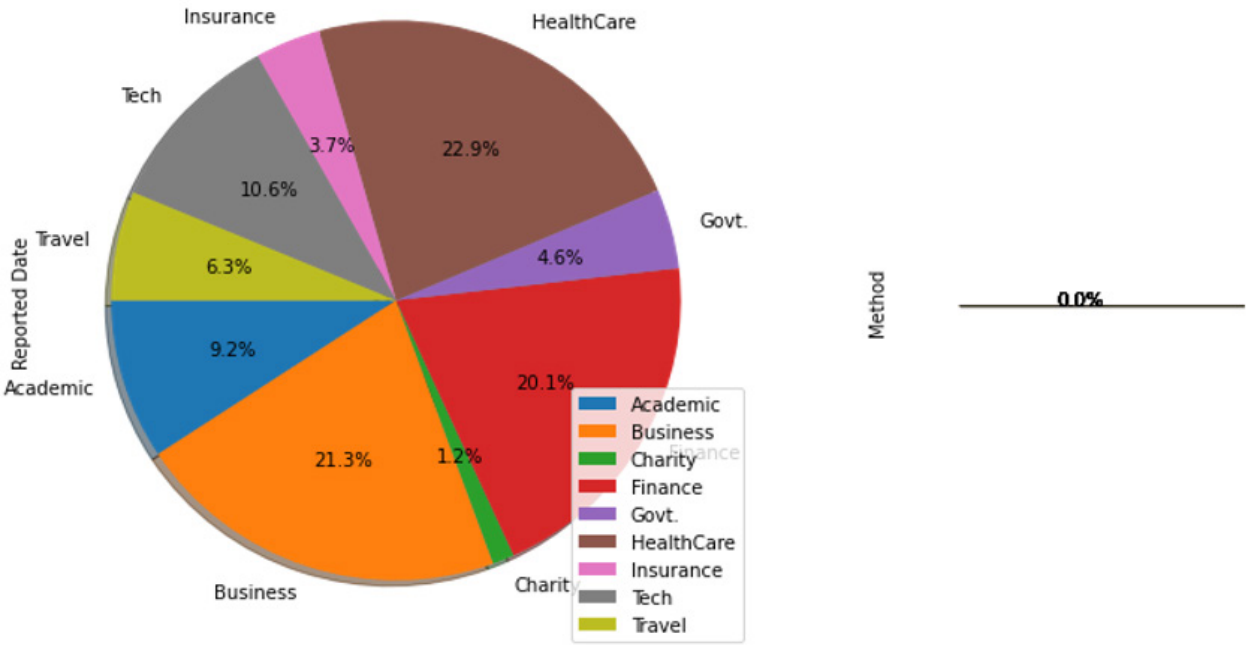

Figure 2. Distribution of Reported Data Breaches by Sector

A similar study by Statista shows the number of data breaches and individuals affected in the United States from 2005 to 2023[4] There has been a sharp increase in data breaches and the number of people impacted during this time. The number of breaches, shown by the blue line, starts low in 2005 but steadily rises, with a big jump in the later years, peaking in 2023. The number of individuals affected, marked by the gray line, also trends upward, but with more ups and downs. This suggests that while the number of breaches has increased consistently, each incident's impact has varied.

The graph features a third line representing the number of exposed records, which mirrors the patterns of the other two metrics. This highlights the rising risks to personal information and increasing cyber threats. Sourced from the Identity Theft Resource Center, it's important to note that those affected may include individuals outside the United States. Overall, the graph underscores the urgent need for better protection of sensitive information.

The Privacy Rights Clearinghouse has released another dashboard that highlights data breach statistics in the U.S. from February 1, 2005, to December 31, 2019.[3] It reports a total of 9009 breaches affecting over 10 billion records. The most common type of breach was "Hacking," followed by "Insider" and "Physical" threats. However, since the advent of Artificial Intelligence and Generative AI, the sophistication of attacks has increased significantly, a trend not reflected in this archival dashboard, which is now outdated.

https://doi.org/10.62486/latia2025333 ISSN: 3046-403X

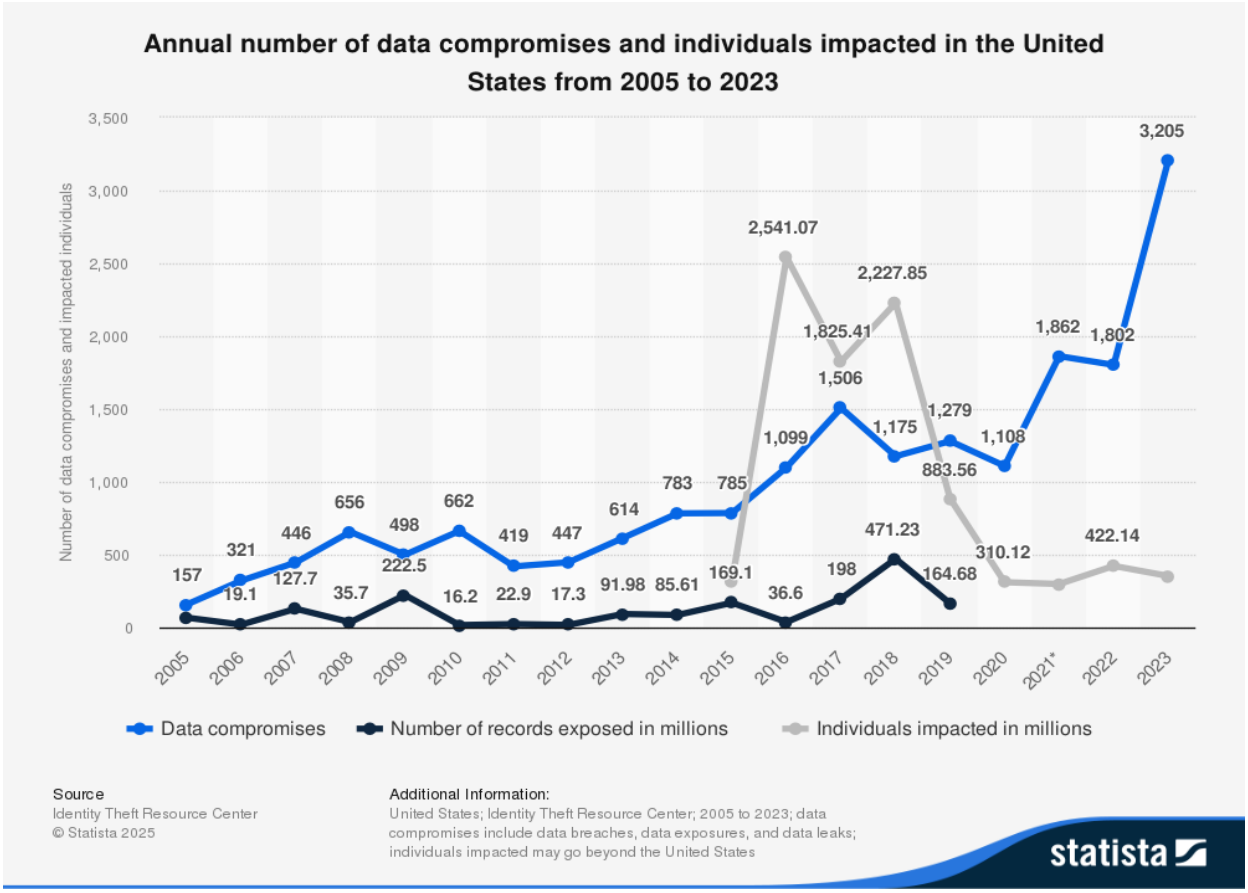

Figure 3. Data Compromises and Impacted Individuals, 2005-2023

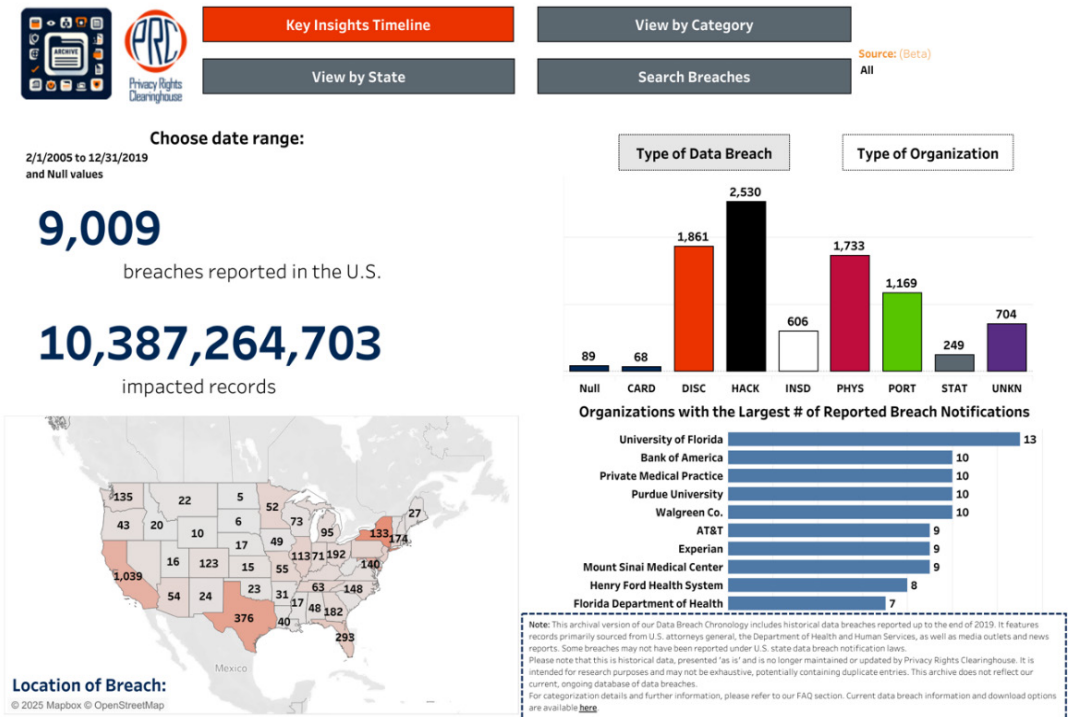

Figure 4. U.S. Data Breach Statistics from 2005-2019

DISCUSSION

This section evaluates the results of our analysis on the evolution of primary data breach catalysts across critical industries over the past two decades. By examining data from 4400 documented breaches and regulatory disclosures, we identified three distinct eras: the digital transition period (2005–2010), the professionalization era (2011–2019), and the hyperconnected epoch (2020–2025). Our findings reveal persistent vulnerabilities

and emerging attack patterns unique to each industry—highlighting the healthcare sector's struggles with misconfigured databases, the finance sector's risks associated with legacy systems, and the technology sector's challenges with zero-day exploits. This nuanced understanding enhances our comprehension of data breach dynamics and informs strategies for improved cybersecurity across industries.

Phase 1: Digital Transition Vulnerabilities (2005–2010)

Healthcare: Fax Errors and Unencrypted Storage

Early healthcare breaches stemmed from analog-to-digital growing pains. In 2008, 28 % of incidents involved misdelivered faxes containing patient records, while unencrypted databases enabled the exposure of 92 million AOL health search queries in 2005.[11,12] The sector's slow adoption of role-based access controls allowed breaches like the 2005 George Mason University incident, where 32 000 Social Security Numbers (SSNs) leaked through unrestricted database permissions.[12]

Financial Services: SQL Injection Dominance

Payment processors faced rampant SQL injection attacks, accounting for 83 % of financial sector breaches in 2008.[6] The 2008 Heartland Payment Systems breach exemplified this trend, where attackers exploited unpatched web applications to steal 100 million credit card records via malicious SQL queries. Financial institutions prioritized perimeter defenses but neglected input validation, enabling five-month undetected intrusions like Heartland's.[11]

Retail: Point-of-Sale (POS) System Exploits

Retailers transitioning to digital payment systems faced skimming attacks and weak encryption. The 2005 DSW Shoe Warehouse breach exposed 1,4 million credit card numbers through unsecured POS databases, highlighting retailers' underestimation of stored-data risks.[12]

Phase 2: Professionalized Cybercrime (2011–2019)

Technology: Third-Party Supply Chain Compromises

The 2013–2016 Yahoo breach (3 billion accounts) demonstrated advanced persistent threats (APTs) exploiting third-party dependencies.[19] Attackers cloned user tables via compromised backup servers and bypassed multi-factor authentication (MFA) using stolen session cookies. By 2017, 38 % of tech breaches involved nation-state actors targeting software supply chains, as seen in Equifax's 2017 Apache Struts vulnerability exploit.[13]

Financial Services: Legacy System Risks

Aging infrastructure plagued financial institutions, with 60 % of breaches linked to unpatched legacy systems. Equifax's 2017 breach—147 million records exposed via an outdated Struts framework—cost \$700 million in fines and highlighted systemic patch management failures.[19] Concurrently, 81 % of banking breaches involved credential stuffing, as weak password policies persisted despite MFA advancements.

Marketing: Cloud Misconfigurations

Marketing firms migrating to cloud storage suffered catastrophic leaks due to access control oversights. The 2018 Exactis breach exposed 340 million consumer profiles—including religious affiliations and pet ownership—through a publicly accessible database.[14] Similarly, River City Media's 2017 MySQL misconfiguration leaked 1,4 billion email addresses, enabling targeted phishing at unprecedented scale.[15]

Phase 3: Hyperconnected Systemic Risks (2020–2025)

Healthcare: Ransomware and IoT Vulnerabilitie

Post-2020 healthcare breaches increasingly targeted IoT medical devices and hybrid cloud systems. The 2024 Ascension breach encrypted patient monitoring systems, delaying critical care and exposure of 5,6 million patients' personal and health information.[16] The Legacy PACS(Picture Archiving Systems) with default credentials enabled lateral movement, affecting 23 % of hospitals by 2025.[22]

Technology: Zero-Day Exploit Proliferation

The 2021 Microsoft Exchange breach epitomized modern APT tactics, where four zero-day vulnerabilities in on-premises servers compromised 30 000 U.S. companies.[23] The Attackers weaponized AI to identify unpatched systems, reducing average exploit development time from 30 days to 72 hours by 2025.

Critical Infrastructure: Operational Technology (OT) Targeting

Energy and utilities faced novel OT threats, as seen in the 2023 GridLock breach.[24] Attackers infiltrated SCADA systems via phishing lures, causing regional blackouts by overriding safety protocols. Legacy PLCs (Programmable Logic Controllers) without firmware updates enabled 67 % of OT breaches.

https://doi.org/10.62486/latia2025333 ISSN: 3046-403X

Persistent Cross-Industry Catalysts

Human Error: The Unyielding Vulnerability

Despite \$120 billion in global cybersecurity training (2010–2025), human factors caused 29 % of breaches annually. Misdelivery errors persisted in healthcare (31 % of incidents), while misconfigured S3 buckets accounted for 23 % of cloud breaches. The 2024 Evolve Bank breach originated from an employee clicking a deepfake video link, enabling ransomware deployment.[25]

Third-Party Risks: Expanding Attack Surfaces

By 2025, 62 % of breaches involved third-party vendors, up from 45 % in 2015. The SolarWinds 2020 campaign demonstrated how compromised software updates could infiltrate 18 000 organizations, including Fortune 500 enterprises and government agencies.[26]

Mitigation Trajectories and Industry Responses

This section discusses the evolution of mitigation stategies some are common and some are specific to industry.

Reconciling Findings with Cybersecurity Frameworks

The OAIC's four-step response model (Contain-Assess-Notify-Review) demonstrated 47 % faster breach containment versus ad hoc approaches in sampled incidents.[27] However, its effectiveness diminished against AI-augmented attacks requiring real-time threat intelligence integration.

Global Regulations Across Industries

GDPR (2018) and CCPA (2020) require breach notifications within 72 hours, decreasing average disclosure times from 200 days (pre-2018) to 30 days. However, cross-border enforcement remains inconsistent, with only 45 % of multinational firms expected to comply fully by 2025.

Zero-Trust Architecture Adoption

Post-2020, 78 % of hospitals have implemented microsegmentation to isolate IoT devices, resulting in a 40 % reduction in the spread of ransomware.[28] However, legacy DICOM systems continue to be vulnerable due to incompatible encryption protocols.[29]

Quantum-Resistant Cryptography

Banks have pioneered lattice-based encryption to address quantum threats. JPMorgan Chase reported a 92 % reduction in credential-stuffing attempts after deploying post-quantum TLS 1,3 in 2024.[30]

AI-Powered Threat Hunting

AI-assisted threat hunting enhances cybersecurity by analyzing large datasets in real time to identify anomalies and detect zero-day threats before they cause harm.[31]

Security Awareness Training

Develop and implement a security awareness program to encourage the workforce to be conscious of security and adequately skilled in order to reduce cybersecurity risks to the company.

Enhance Event Monitoring and Log Analysis

Take a proactive approach to monitoring events and analyzing logs to identify anomalies and suspicious activities.

Develop and Implement Incident Response Plans

Promptly contain incidents and ensure that actions taken preserve evidence for investigative purposes.

Prioritize Patch Management

Prioritize fixing exploitable vulnerabilities and protecting business-critical assets to reduce the risk of exploitation.

Future Research Directions

With two decades of data breach analysis providing valuable historical insights, future research should emphasize the evolving role of artificial intelligence (AI) in both offensive and defensive cybersecurity strategies, reflecting its growing significance in recent reports. It is crucial to further investigate how threat actors may exploit AI to conduct more sophisticated attacks, such as highly realistic phishing campaigns and automated

vulnerability exploitation. On the other hand, organizations should focus on effectively implementing AI-powered tools to enhance threat detection, incident response, and predictive security analytics.

Moreover, ongoing research should track long-term trends in attack vectors, particularly the sustained effectiveness of established methods like exploiting known vulnerabilities and social engineering. There is also a need to assess the emergence of new threats targeting cloud environments and the interconnectedness of supply chains, which will help inform proactive security measures and optimize resource allocation.

CONCLUSIONS

In conclusion, the study of data breaches across the past two decades, as evidenced by the Verizon Data Breach Investigations Reports, CCPA Data breach databse and other sources, reveals a persistent and evolving threat landscape. While the fundamental motivations of threat actors often remain financial or espionage-driven, the techniques employed have become increasingly sophisticated, moving from basic methods like SQL injection and phishing to more complex Advanced Persistent Threats (APTs) and ransomware. The emergence of AI-driven threats and the exploitation of supply chains in recent years highlight cybercriminals' continuous adaptation to technological advancements and the increasing interconnectedness of digital ecosystems. Furthermore, the reports underscore the enduring importance of the human element in security breaches, with social engineering and the misuse of credentials remaining significant attack vectors throughout the studied period.

Looking ahead, several key themes emerge from this extensive analysis. The ongoing need for robust security controls, including encryption, timely patching, and practical employee training, remains paramount in mitigating the risks of data breaches. The increasing complexity of the threat landscape necessitates a proactive and adaptive security posture, with organizations needing to stay informed about emerging threats and continuously refine their defenses. Moreover, the collaborative nature of threat intelligence sharing, as demonstrated by the growing number of contributors to the DBIR, is crucial in fostering a more comprehensive understanding of cybercrime and collectively working towards a more secure future.

BIBLIOGRAPHIC REFERENCES

1. Verizon. Verizon Data Breach Investigations Report. [Internet]. Available from: https://www.verizon.com/business/resources/reports/dbir/

2. California Department of Justice. Search Data Security Breaches. [Internet]. Available from: https://oag.ca.gov/privacy/databreach/list

3. Privacy Rights Clearinghouse. Data Breach Chronology. [Internet]. Available from: https://privacyrights.org/data-breaches

4. Statista. Number of data breaches and victims in the U.S. 2023. [Internet]. Available from: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

5. Verizon-dbir-github reports. Verizon DBIR. [Internet]. Available from: https://github.com/amckenna/verizon-dbir-reports

6. Statista. Cost of cybercrime worldwide. [Internet]. Available from: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

7. Federal Bureau of Investigation. Internet Crime Complaint Center (IC3). [Internet]. Available from: https://www.ic3.gov/CrimeInfo/DataBreach

8. LifeLock. History of Data Breaches. [Internet]. Available from: https://lifelock.norton.com/learn/data-breaches/history-of-data-breaches

9. Australian Government. The Privacy Act 1988. [Internet]. Available from: https://www.legislation.gov.au/C2004A03712/latest/versions

10. European Commission. Europe GDPR. [Internet]. Available from: https://gdpr-info.eu/

11. UpGuard. Biggest Data Breaches in the US. [Internet]. Available from: https://www.upguard.com/blog/biggest-data-breaches-us

12. Digital Guardian. History of Data Breaches. [Internet]. 2023 Available from: https://www.digitalguardian.com/blog/history-data-breaches

13. CSO Online. The Biggest Data Breaches of the 21st Century. [Internet]. Available from: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html

14. Wired. Exactis Database Leak Exposes 340 Million Records. [Internet]. 2023 Available from: https://www.wired.com/story/exactis-database-leak-340-million-records/

15. Security Week. Spammers Leak 14 Billion User Records. [Internet]. 2023 Available from: https://www.securityweek.com/spammers-leak-14-billion-user-records/

16. MedCity News. Ascension Cyberattack: Cybersecurity in Healthcare. [Internet]. 2024 Available from: https://medcitynews.com/2024/12/ascension-cyberattack-cybersecurity-healthcare/

17. Indusface. Notorious Hacks in History. [Internet]. Available from: https://www.indusface.com/blog/notorious-hacks-history/

18. Zluri. Most Common Causes of Data Breaches. [Internet]. Available from: https://www.zluri.com/blog/most-common-causes-of-data-breaches

19. UpGuard. Biggest Data Breaches. [Internet]. Available from: https://www.upguard.com/blog/biggest-data-breaches

20. Monroe. Cybersecurity: History, Hacking, Data Breaches. [Internet]. Available from: https://www.monroeu.edu/news/cybersecurity-history-hacking-data-breaches

21. Securiti. Analysis of the Biggest Data Breaches in History and What to Learn. [Internet]. Available from: https://securiti.ai/analysis-of-the-biggest-data-breaches-in-history-and-what-to-learn/

22. American Hospital Association (AHA). FBI-TLP Alert: Picture Archiving Communication Systems (PACS) Vulnerability. [Internet]. 2020 Available from: https://www.aha.org/fbi-tlp-alert/2020-12-17-tlpwhite-picture-archiving-communication-systems-pacs-vulnerability

23. Krebs on Security. A Basic Timeline of the Exchange Mass Hack. [Internet]. 2021 Available from: https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

24. CM Alliance. October 2023 Major Cyber Attacks, Data Breaches, Ransomware Attacks. [Internet]. 2023 Available from: https://www.cm-alliance.com/cybersecurity-blog/october-2023-major-cyber-attacks-data-breaches-ransomware-attacks

25. GetEvolved. Cybersecurity Incident: Substitute Notice of Data Breach. [Internet]. 2023 Available from: https://www.getevolved.com/about/news/cybersecurity-incident/substitute-notice-of-data-breach/

26. Aqua Security. SolarWinds Attack. [Internet]. 2021 Available from: https://www.aquasec.com/cloud-native-academy/supply-chain-security/solarwinds-attack/

27. Office of the Australian Information Commissioner (OAIC). Preventing, Preparing for and Responding to Data Breaches. [Internet]. Available from: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps

28. HealthTech Magazine. How Hospitals Use Network Microsegmentation to Guard Against Cyberattacks. [Internet]. 2017 Available from: https://healthtechmagazine.net/article/2017/10/how-hospitals-use-network-microsegmentation-guard-against-cyberattacks

29. CPO Magazine. 30-Year DICOM Vulnerability Exposes Millions of Health Records to Access and Manipulation. [Internet]. 2023 Available from: https://www.cpomagazine.com/cyber-security/30-year-dicom-vulnerability-exposes-millions-of-health-records-to-access-and-manipulation/

30. JPMorgan. Firm Establishes Quantum-Secured Crypto-Agile Network. [Internet]. 2023 Available from: https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network

31. Ericom. What is a Zero-Day Attack?. [Internet]. Available from: https://www.ericom.com/glossary/what-is-zero-day-attack/

32. American Hospital Association (AHA). FBI-TLP Alert: Picture Archiving Communication Systems (PACS) Vulnerability. [Internet]. 2020 Available from: https://www.aha.org/fbi-tlp-alert/2020-12-17-tlpwhite-picture-archiving-communication-systems-pacs-vulnerability

33. Wikipedia. List of Data Breaches. [Internet]. Available from: https://en.wikipedia.org/wiki/List_of_data_breaches

34. Beazley. The Evolution of Cyber Attacker Techniques. [Internet]. Available from: https://www.beazley.com/en/cyber-services-snapshot/the-evolution-of-cyber-attacker-techniques/

35. Reddit. Why Does It Seem Like Data Breaches Are Becoming More Common?. [Internet]. Available from: https://www.reddit.com/r/cybersecurity/comments/1eojbq7/why_does_it_seem_like_data_breaches_are_becoming/

36. Center for Strategic and International Studies (CSIS). Significant Cyber Incidents. [Internet]. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

FINANCING

None.

CONFLICT OF INTEREST

Authors declare that there is no conflict of interest.

AUTHORSHIP CONTRIBUTION

Conceptualization: Amit Singh.
Data curation: Amit Singh.
Formal analysis: Amit Singh.
Drafting - original draft: Amit Singh.
Writing - proofreading and editing: Amit Singh.