SPIRION

WHITE PAPER

# Review of America's Top Cyber Breaches in 2022

**Cyberattacks are a constant reminder that we live in the age of digital transformation, with attacks occurring every 10 seconds.[1]**

The existential threat of cybercrime "represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined," asserts leading industry researcher and publisher Cybersecurity Ventures.[2] They forecast that cybercrime will cost the world $10.5 trillion annually by 2025. "The damage cost estimation is based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities, and a cyberattack surface which will be an order of magnitude greater in 2025 than it is today."[3]

The costs of cyberattacks extend well beyond the estimated fines of $180 per breached data record containing personally identifiable information (PII).[4] Far-reaching repercussions include "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."[5]

Above all, these assaults cost your customers, employees, and partners their digital identities and the fundamental human right to data privacy. That's why at Spirion, we fight the good fight every day to protect what matters most—the sensitive personal data of our colleagues, customers, and communities. After all, data privacy is impossible without proactive data protection.

Learning from these insidious attacks is one of the best options we have to prevent them. We have researched and discovered valuable insights from the top sensitive data breaches of 2022. This definitive guide outlines actionable steps you can take today to reduce your organization's data exposure and risk in 2023 and beyond.

## Data analysis methodology

This Definitive Guide to Sensitive Data Breaches is based on the analysis of 1,833 unique data incidents that impacted and were subsequently reported by 3,583 U.S.-based organizations from January 1 through December 31, 2022. Data was obtained from the Identity Theft Resource Center (ITRC) notified Dashboard, a comprehensive database of publicly reported data breaches in the United States, which tracks 25 different information fields and 63 different identity attributes daily.

Spirion used the ITRC database to identify data breaches in 2022 that specifically involved the compromise of sensitive data. We analyzed those instances to identify the top sensitive data breaches by the number of organizations and individuals impacted, number of records compromised, threat actor, exposure vector, and types of sensitive data exposed by industry sector. We also cross-referenced ITRC's 2022 Data Breach Report for aggregate statistics.

### About the Identity Theft Resource Center

The ITRC is a non-profit organization established to support victims of identity theft in resolving their cases and to broaden public awareness of identity theft, data breaches, cyber security, scams/fraud, and privacy issues. Since 2005, the ITRC has tracked over 10,000 publicly-notified U.S. data breaches daily. You can learn more about ITRC here: https://www.idtheftcenter.org/about-us/

## The Macro View: A Summary of Data Compromises in 2022

According to ITRC, 2022 saw the second highest number of data breaches ever reported by U.S. organizations in a single year, following 2021's all-time record of 1,862 incidents. An average of seven data breach notices were issued every business day in 2022 for an annual total of 1,802 incidents.

**U.S. DATA BREACHES 2017-2022**

| Year | Total Incidents | # Sensitive Data Incidents | % Sensitive Data Incidents | Individuals Impacted |
|---|---|---|---|---|
| 2022 | 1,802 | 1,494 | 83% | 422,143,312 |
| 2021 | 1,862 | 1,557 | 84% | 293,213,506 |
| 2020 | 1,108 | 882 | 80% | 310,218,744 |
| 2019 | 1,279 | 1,084 | 85% | 883,558,186 |
| 2018 | 1,175 | 1,013 | 86% | 2,227,849,622 |
| 2017 | 1,506 | 1,385 | 92% | 1,825,413,935 |

*Source: Identity Theft Resource Center 2022 Data Breach Report*

With a global average cost of $4.35 million per data breach,[6] preventing these data compromises has become more pressing for enterprises around the world. All told, the economic toll of 2022's rampant data breaches is estimated to have cost organizations more than $7.8 billion in aggregate.

## Breaches Aren't the Only Threat to Data Security

While we often refer to any unauthorized data access as a breach, that misconception provides a limited scope into the full extent of security threats faced by Security Operations teams. There are different types of data compromises that can put data into the wrong hands, even if that data appears to be securely stored in your systems.

The National Institute of Standards and Technology (NIST) defines a data breach as an unauthorized transfer of information from a system. The bulk (98%) of last year's incidents were data breaches that exfiltrated the data records of 422,143,312 individuals as reported by ITRC.[7] Since data is removed from a system in a breach, such victims may be at risk of identity theft and fraud long after the initial breach.

**64% of organizations worldwide have experienced at least one form of cyberattack.[8]**

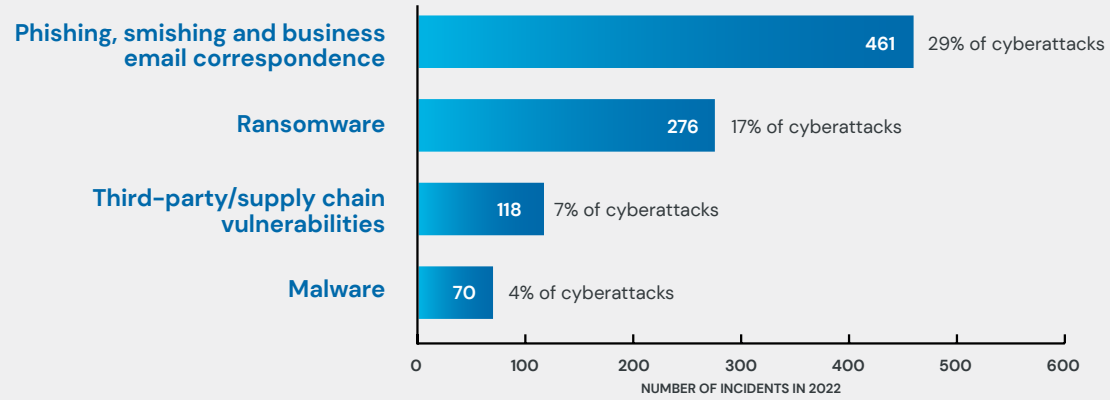
In contrast to data breaches, a data exposure occurs when data is viewable or downloadable but isn't removed from the system. Typically arising from a failure to configure cloud security or misconfigured firewalls, these human errors accounted for 1% of the year's total data incidents, which left 7,146,425 people's data compromised.

Whether data is intentionally stolen or misused, or data is accidentally exposed or removed from a system, all of these scenarios present a significant risk to data privacy, protection, and compliance.

## How Did Data Compromises Happen in 2022?

Many of the data compromises that occurred in 2022 were particularly difficult to detect or avoid. For example, half of the organizations involved in a data breach last year were compromised by a third-party or supply chain vulnerability, which can be challenging to identify early, even with end-to-end visibility.

**Cyberattacks accounted for 89% of 2022's events (1,595 incidents) that compromised 374,992,920 individuals by successfully leveraging these top attack vectors:**




*Source: Identity Theft Resource Center 2022 Data Breach Report*

Human or system errors played a role in 8% of all incidents in 2022, which compromised the data privacy of 24,130,504 individuals through the following vulnerable vectors:

- Email correspondence (55 incidents)
- Non-configured cloud security of misconfigured firewalls (48 incidents)
- Lost device or document (12 incidents)

A minor number (3%) of incidents involved physical attacks, such as device and document theft (28 incidents) and improper disposal (5 incidents). All told, internal actors were responsible for just 5% of the year's data compromises, while external actors accounted for 95% of breach incidents.

The majority (83%) of the year's data breaches involved sensitive data records, but huge swathes of non-sensitive data records were also captured. For instance, a known Twitter software flaw was exploited in two separate attacks last year that exposed the account information of more than 221 million users.[9] While this data alone may be insufficient to identify an individual, it can be correlated across multiple events to pose a real identity threat.

**"There are so many data breaches that identity thieves are now able to harvest multitudes of personal data across events to correlate information by person. Using an email address, name or postal address, they are able to correlate additional pieces of information and obtain a complete profile about a consumer that could be used to steal a tax refund, open a credit card or bank account, or transfer funds out of a financial institution."**

**Todd Feinman**
Co-Founder,
Spirion

The year's top 10 data breaches account for 82% of total victims, leaving 347,893,164 people vulnerable to identity theft crimes. That is more than the entire population of every child and adult living in the United States today.

### TOP 10 DATA BREACHES OF 2022

| Organization | Individuals Impacted | Attack Vector | Industry |
|---|---|---|---|
| Twitter | 221,524,284 | Cyberattack – Unpatched software flaw | Technology |
| NeoPets | 69,000,000 | Cyberattack | Hospitality |
| AT&T | 22,786,997 | Cyberattack – Ransomware | Telecommunications |
| Cash App Lending | 8,200,000 | System & Human Error | Financial Services |
| Beetle Eye | 7,000,000 | System & Human Error – Failure to Configure Cloud Security | Technology |
| Twitter | 5,485,636 | Cyberattack – Unpatched software flaw | Technology |
| Receivables Performance Management | 3,766,573 | Cyberattack | Technology |
| Flexbooker | 3,756,794 | Cyberattack | Technology |
| Eye Care Leaders | 3,372,880 | Cyberattack – Third-party supply chain | Healthcare |
| Advocate Aurora Health | 3,000,000 | System & Human Error | Healthcare |

*Source: Identity Theft Resource Center 2022 Data Breach Report*

## Under-Reporting Data Breaches Undermines Consumer Privacy

Despite more organizations experiencing data compromises, the ITRC reported that 66% of organizations underreported data breaches in 2022 by failing to include victim and attack details.[10] This is the information that individuals and businesses need to adequately assess the risk to their identity information following a compromise. That means that, while many breaches get reported to appropriate channels, the full scope of the breach is often a mystery to those outside of the organization.

**Identity Theft Resource Center President and CEO Eva Velasquez emphasizes:**
**"The trends related to publicly reported data breaches in 2022 reinforce the conclusion that the data breach environment is worse than we know and can prove with quantifiable data. The result is individuals are largely unable to protect themselves from the harmful effects of data compromises which are fueling an epidemic – a "scamdemic" – of identify fraud committed with stolen or compromised information."[11]**

ITRC | IDENTITY THEFT RESOURCE CENTER

Although individual states require companies to notify customers of a breach, currently there are no blanket federal U.S. laws dictating that companies must report every data compromise.

**66% of organizations underreported data breaches in 2022 by failing to include victim and attack details.**

With the California Privacy Rights Act (CRPA) now in full enforcement, the recent under-reporting trend may reverse itself as U.S. companies once again share pertinent details around the data breaches they experience. The new guidelines set the tone for future legislation across the U.S. by giving consumers more "rights-based" control over how their sensitive data is used and limiting how data is shared among organizations. The consequences of not protecting sensitive data—which accounts for 83% of last year's total number of incidents—will become even more significant for companies moving forward.

The breaches themselves cost organizations millions to mitigate, and companies also often face hefty penalties and fines for falling out of compliance with data privacy laws. Stringent standards like General Data Protection Regulation lead to even higher fines for unreported or underreported breaches within a strict notification timeframe.

## Emerging Trends in Cyber Attacks

### DATA BREACH FREQUENCY: THE NEW NORMAL

At the end of 2021, Spirion President & CEO Kevin Coppins shared the following prediction for data breaches in 2022:[12]

**"Organizations will struggle to shift from the reactive 'if' or 'when,' to the proactive reality of 'how often' they'll have to deal with data-related incidents. Vendors for years have said 'it's not if you'll be breached, it's when.'**

**The shift we are starting to see accelerate is organizations experiencing multiple incidents in a single year, and the types of incidents are expanding. This is a direct result of the ever-expanding data universe, accelerated by the global pandemic and the evolving regulations surrounding sensitive data.**

**In 2022, organizations will begin planning to minimize the costs and business impacts as though they expect to experience three or four significant events a year vs. a singular 'black swan' type event. More breach management will be brought in house and organizations will manage data risk much more proactively."**

**Kevin Coppins**
President and CEO, Spirion

How well did Kevin's prediction hold up? Unfortunately, far too well. IBM's newly released Cost of a Data Breach Report 2022 reveals that a whopping 83% of surveyed organizations experienced more than one breach last year.

**83% of organizations surveyed experienced multiple breaches in 2022.**

## EXPLOITING POINTS OF LEVERAGE ACROSS SUPPLY CHAINS

Hackers have also become more sophisticated, and attacks in 2022 looked dramatically different than in years past. With cryptocurrency market volatilities, cybercriminals redirected ransomware campaigns in favor of high leverage points within supply chains. Ransomware attacks fell by 23% while the number of cyberattacks tied to third-party and supply chain vulnerabilities grew by 40% in 2022.

By using a single point of attack to exploit multiple organizations, cyberattackers can gain data more readily than targeting a particular organization and searching for a weak access point. Last year 118 well-positioned supply chain attacks infiltrated 1,743 organizations—more than a three-fold increase in the number of organizations impacted in 2021—ultimately leaving 10,038,594 people's information vulnerable.

Attackers are also going beyond popular industries like healthcare and financial services to target industries with traditionally lagging cybersecurity, like professional and business services, non-profits as well as manufacturing and utilities. Often, these organizations do not have the data lifecycle management strategy or modern cybersecurity tools to support their rapidly-increasing data sprawl.

## NATION STATE ACTORS TARGETING CRITICAL INFRASTRUCTURE

The manufacturing sector, especially critical manufacturing (and other critical infrastructure), has recently come under the spotlight as facing significant risk for a data breach. In addition to being geo-politically targeted by nation-state actors, critical manufacturing faces vulnerabilities arising from supply chain automation across their ecosystem. Those very partnerships add to a level of cyber risk for many critical infrastructure providers – as 54% of confirmed breaches are due to the cybersecurity gaps of other organizations.[13] Microsoft confirms the fact that nation-state cyberattacks against critical infrastructure have doubled in the past year.[14]

On a positive note, it's worth highlighting that the number of cyberattacks stemming from unprotected cloud environments sharply declined by 63% in 2022. In 2021, 24 non-secured cloud environments were the targets of cyberattacks that compromised the personal information of more than 51 million individuals. Last year only 9 such incidents exposed the personal information of 179,723 people.[15]

# The Micro View: A Closer Look at Sensitive Data Compromises in 2022

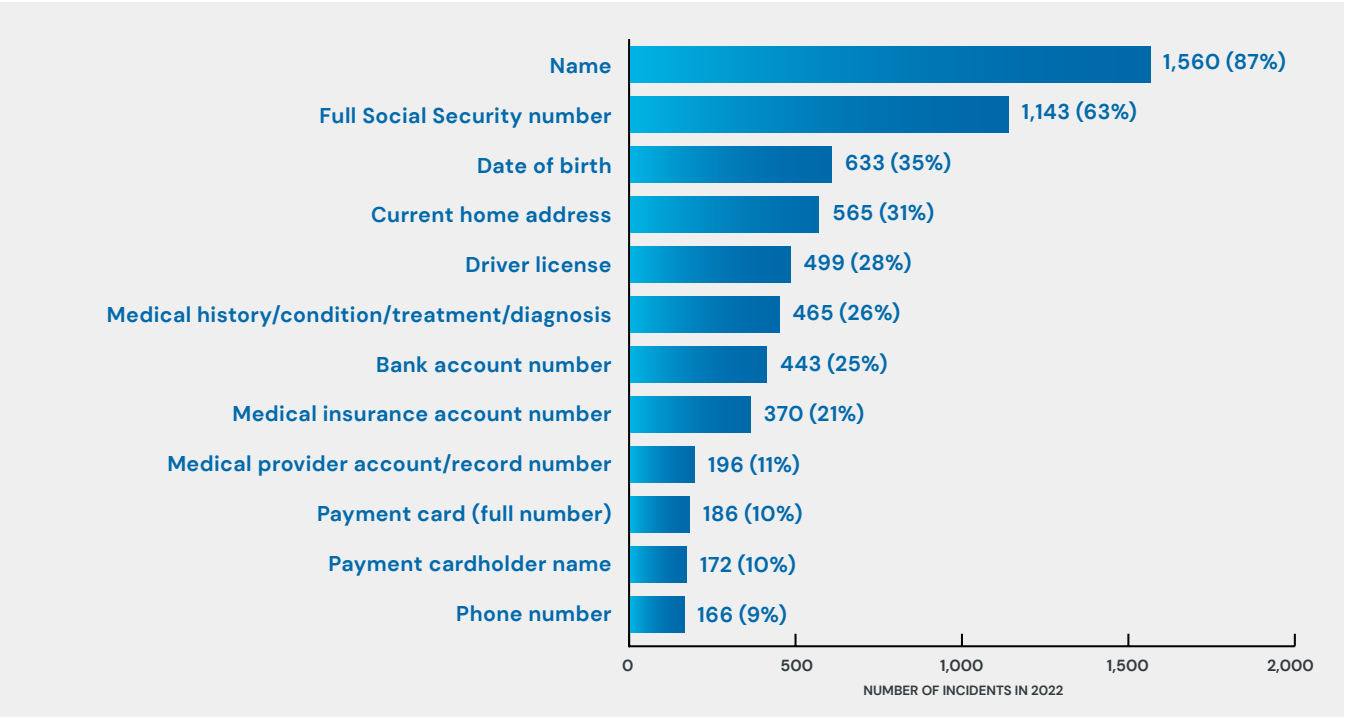
Personally Identifiable Information (PII) is hugely valuable to cyberattackers, which suggests why sensitive data continues to be a primary target for breaches. Every week, virtual underground storefronts emerge on the dark web to help bad actors buy and sell PII stolen through cyberattacks. In fact, the deep, dark web is estimated to be "5,000-times larger than the surface web, and growing at a rate that defies quantification."[16]

Consumers and employees—even those that only engage with organizations in person—may hand organizations this information without their full knowledge and consent. Every swipe of a credit card or recorded phone call puts people at risk of exposing their data. While companies often need this data to conduct business in our modern society, storing millions of customer and employee PII poses a challenge for IT teams tasked with keeping this data secure.

Breached sensitive data compromises the safety and security of these customers and employees. Information like Social Security numbers, personal health information, and bank account details can pose substantial harm to the financial health and privacy of customers, especially when cyberattackers leverage this information for identity theft or to steal financial assets. Fullz—or a bundle of information with a person's full name, SSN, account numbers, and even voter records—can be especially valuable for attackers to buy and sell.

Meanwhile, even stolen account login credentials can present a major risk for customers, potentially granting attackers access to even more accounts beyond the compromised one.

### MOST COMMON PII EXFILTRATED DURING SENSITIVE DATA BREACHES IN 2022




*Source: Identity Theft Resource Center 2022 Data Breach Report*

Customer PII is the most common type of record that is lost or stolen (44% of all data breaches), and employee PII is exfiltrated in 26% of breaches.[18] Since companies are legally required to notify victims when their data has been exposed, sensitive data breaches often have a significant impact on company reputation that can serve to diminish public confidence and trust in the organization.

### TYPES OF RECORDS COMPROMISED IN DATA BREACHES

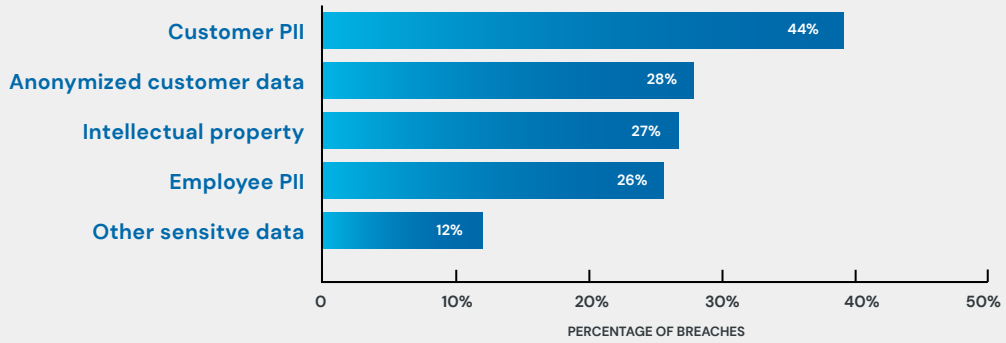



*Image Source: "Cost of a Data Breach Report 2022," IBM, July 2021.*

Since organizations are subject to data privacy fines when sensitive data is exposed, PII instances typically cost organizations much more than non-sensitive breaches. Each piece of exposed customer PII costs organizations approximately $180, and exposed employee PII cost $176 apiece.[18] Based on these fines alone, organizations are estimated to have incurred at least $5 billion in fines after compromising more than 28.5 million sensitive employee and customer data records in 2022. Escalating fines, lost business opportunities, reputational damages and loss of trust are just part of the reason why organizations must secure vulnerable attack vectors to prevent unauthorized access to sensitive data.

**ITRC's 2022 Data Breach Report revealed that 1,494 primary incidents (or 83% of total incidents) compromised the sensitive data of close to 100 million individuals in 2022. However, the second order effect of the breaches was much wider than that. The threat surface of those attacks spread across third-party ecosystems and ultimately infiltrated an additional 1,072 organizations. The ITRC notified database contains 2,566 sensitive data incidents that were publicly reported during 2022. Spirion's sensitive data analysis is primarily based on those sensitive data breaches.**

# Sensitive Data Vectors of Attack

External actors carried out 97% of all sensitive data incidents last year, placing 91,303,788 people's PII at risk. Exfiltrating sensitive data through targeted cyberattacks was the primary way external actors gained unauthorized access to the personal data of 63,595,679 people. In total 2,385 organizations fell victim to cyberattacks – almost half by way of third-party and supply chain vulnerabilities.

Cyberattackers successfully executed 93% of all sensitive data breaches by leveraging these top attack vectors to access PII:

### TOP CYBERATTACK VECTORS LEVERAGED IN SENSITIVE DATA BREACHES IN 2022

| Attack Vector | Total Incidents | Percent Total | Individuals Impacted |
|---|---|---|---|
| Third party/supply chain | 1,082 intrusions | 45% | 7,860,184 |
| Phishing, smishing, business email correspondence | 351 | 15% | 2,309,784 |
| Ransomware | 224 | 9% | 11,346,101 |
| Malware | 67 | 3% | 3,581,505 |

*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

Meanwhile, internal actors were responsible for 3% of sensitive data compromises, placing 6,140,154 people's PII at risk, largely through human error including socially engineered email correspondence and misconfigured cloud security. The smallest percentage of sensitive data breaches involved physical attacks through document and device theft or improper disposal, accounting for 14 data compromises.

Protecting sensitive data often means looking to new attack vectors to detect vulnerable points. Knowing where sensitive data resides and ensuring it's properly classified and encrypted are critical steps to keeping data safe. Organizations must also minimize their technical debt—or the remaining security and coding errors that result from overlooking critical security steps and processes to get a product or platform released faster—to avoid unknowingly exposing PII. Otherwise, attack vectors both within and outside of a company's ability to control and monitor PII can pose costly risks to customer and employee data.

# Sensitive Data Breach Lifecycle

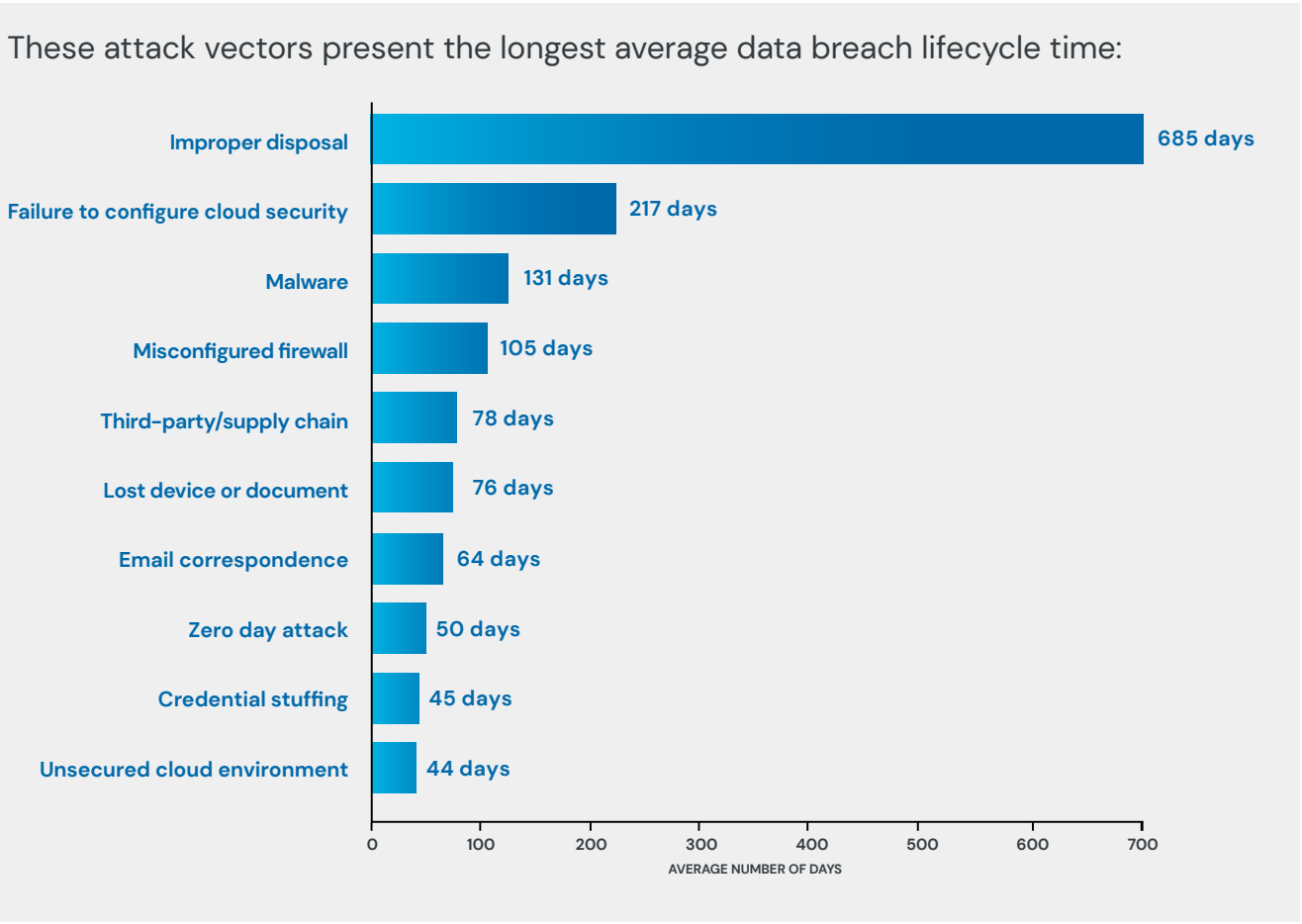
As third-party and supply chain vulnerabilities present more opportunities for cyberattacks, organizations are taking longer to detect and contain data breaches. Without complete visibility into the data lifecycle, sensitive data is often more accessible than companies expect. The longer a breach lasts, the more data may be exposed and available to cyberattackers.

Naturally, some attacks are harder to detect and contain than others. For example, sensitive data breaches due to the improper disposal of storage devices took 22 months to detect and contain on average, while a failure to configure cloud security took 7 months.

ITRC data revealed that the average sensitive data breach has a lifecycle of 67 days from detection to containment. It took twice as long to detect and contain incidents caused by internal actors as external data breaches. On average, the lifecycle of data compromises induced by employees took 147 days to detect and contain, whereas external attacks had an average lifecycle of 65 days. Often, monitoring is focused on external cyberattacks, meaning internal errors went unnoticed for almost three months longer than external attacks last year.

A longer life cycle ultimately leads to ballooning costs. IBM reported that breaches that took over 200 days to identify cost $4.86 million on average, while breaches that took fewer than 200 days cost companies $3.74 million on average.[19]

### AVERAGE NUMBER OF DAYS TO DETECT AND CONTAIN SENSITIVE DATA INCIDENTS BY ATTACK VECTOR




*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

## TOP 10 U.S. SENSITIVE DATA COMPROMISES OF 2022

| Organization | Individuals Impacted | Sensitive Data Compromised | Attack Vector | Industry |
|---|---|---|---|---|
| AT&T | 22,786,997 | Social Security number and email/password | Unknown | Telecom |
| Cash App Investing | 8,200,000 | Other Sensitive Date | System & Human Error | Financial Services |
| Receivables Performance | 3,766,573 | Social Security number | Cyberattack | Financial Services |
| Elephant Insurance | 2,762,687 | Driver license | Cyberattack | Financial Services |
| OneTouchPoint | 2,651,396 | Personal health information | Ransomware | Business Services |
| Lakeview Loan Servicing | 2,537,261 | Social Security number | Cyberattack | Financial Services |
| Nelnet Servicing | 2,501,324 | Social Security number and email/password | Zero Day Cyberattack | Financial Services |
| Connexin Software | 2,216,365 | Social Security number, personal health information and email/password | Cyberattack | Technology |
| U-Haul International | 2,195,831 | Driver license | Cyberattack | Transportation |
| Shields Health Care Group | 2,000,000 | Social Security number, personal health information | Cyberattack | Healthcare |

*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

# Industries Most Impacted By Sensitive Data Breaches

Every company collects and stores sensitive data. However, some industries collect substantially more sensitive data than others. As a result, these industries often experience larger data compromises that impact a greater number of individuals.

The following sectors experienced sensitive data incidents that compromised the most PII in 2022:

### TOP 10 INDUSTRIES MOST IMPACTED BY SENSITIVE DATA INCIDENTS IN 2022

| Industry | # Individuals Impacted | % Total Individuals Impacted | # Incidents | Average # Individuals Impacted Per Incident |
|---|---|---|---|---|
| Financial Services | 28,200,477 | 29% | 329 | 85,716 |
| Healthcare | 25,785,388 | 27% | 1,240 | 20,795 |
| Telecommunications | 22,795,582 | 23% | 8 | 2,849,447 |
| Professional & Business Services | 6,818,276 | 7% | 235 | 29,014 |
| Technology | 4,642,879 | 5% | 74 | 62,742 |
| Transportation | 2,803,559 | 3% | 39 | 71,886 |
| Government | 1,440,048 | 2% | 74 | 19,460 |
| Education | 1,106,152 | 1% | 81 | 13,656 |
| Retail | 983,914 | 1% | 94 | 10,467 |
| Manufacturing | 902,409 | 1% | 143 | 6,311 |

*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

## Financial Services

Financial services is responsible for six of 2022's top ten sensitive data breaches, which impacted 19,767,845 people. Although this sector ranked second only behind healthcare in sheer volume of sensitive data breaches last year, it accounted for the greatest number of reported sensitive data breach victims, 28.2 million people or 29% of the year's total. Additionally, this industry has the second most individuals impacted per incident, with 85,716 people on average.

This industry ranked:

- #2 for third-party/supply chain vulnerabilities
- #2 for insider errors
- #4 for the most ransomware attacks

## Financial services has the second highest average cost of a data breach of any industry—$5.97 million per incident.[20]

Last year, one of the industry's largest attacks occurred at Cash App Investing, where a former employee downloaded company reports that contained full names, brokerage account numbers, brokerage portfolio values and holdings of more than 8.2 million customers. A Cash App spokesperson stated, "While this employee had regular access to these reports as part of their past job responsibilities, in this instance, these reports were accessed without permission after their employment ended."[22] The spokesperson added, "Fortunately, information such as usernames, passwords, dates of birth, Social Security numbers, and bank account information were not compromised, nor were account access codes."

**"More than 175,000 individuals have been impacted by corporate restructuring and downsizing since January 2022. The layoff trend has continued into 2023 with Amazon and Salesforce among those sending pink slips to thousands of employees. When you layoff that many people, even with the strictest of security measures and offboarding procedures, you are bound to lose some sensitive corporate data. Old employee files, payroll records, customer bank accounts, I-9 forms, credit cards—all the things those former employees needed to do their jobs.**

**My prediction is that we will continue to see breaches and misuse of company data from employees that have long since left the companies who were entrusted with that data. More often than not, it won't be nefarious, it will simply be 'I forgot I had those files stored there'."**

**Kevin Coppins**
President and CEO,
Spirion

### Healthcare

After reporting 333 primary sensitive data breaches that further penetrated an additional 907 organizations via third-party and supply chain vulnerabilities, healthcare once again ranked number one in sheer volume of sensitive data incidents last year, which impacted more than 25.8 million individuals as patients' private information was compromised.

Last year, healthcare ranked:

- #1 for third-party/supply chain vulnerabilities
- #1 for the most ransomware attacks
- #1 for insider errors

The largest sensitive data breach (responsible for 8% of the industry's breach victims) occurred at Shields Health Care Group, a Massachusetts-based medical services provider specializing in diagnostic imaging, radiation oncology and ambulatory surgical services. In July a cyberattack breached the company's computer systems for about two weeks, compromising the sensitive data of more than 2 million people across 56 partner organizations. Compromised data included full names, Social Security numbers, dates of birth, provider information, billing information, insurance numbers, medical record numbers, patient identification numbers and other medical information.[23]

In September, Indiana-based Community Health Network reported that the misconfiguration of certain pixels used to collect visitor information on some its digital properties—including patient portal and scheduling sites—may have "allowed for a broader scope of patient information collection and transfer to third-party vendors, such as Meta and Google, than it realized."[24] The company believes the misconfiguration goes as far back as 2017 and could have compromised the personal health information, including scheduled procedures, medical record numbers, and insurance information for 1.5 million patients. A Community Health Network spokesperson adds, "We have no indication that any Social Security numbers, financial account numbers or debit/credit card information was collected by or transmitted through the third-party tracking technologies at any time."[25]

**For the 12th year in a row, healthcare was the highest cost industry for a data breach at $10.10 million per incident.[26]**

### Telecommunications

Even though the telecommunications sector experienced only eight sensitive data breaches last year, the impact of each incident was far-reaching and resulted in the highest average number of individuals compromised per event. For instance, a single breach by AT&T sent this industry to the top of the list. This massive data breach occurred when 28.5 million sensitive data records, including Social Security numbers and email/passwords, were spotted on a dark website for 22,786,997 AT&T customers.

According to ITRC, "Cybersecurity researchers found a file on a popular dark website containing 22.8 million unique email addresses and 23 million unique Social Security numbers believed to be related to customers of AT&T. The telecom company did not issue a data breach notice to consumers and denied the information was stolen from their system. AT&T acknowledged the stolen data 'may be tied to a previous data incident at another company,' but did not elaborate."[27]

### Professional/Business Services

Organizations across myriad industries rely on professional and business services for expertise, strategy, and tactical execution. However, that also means these highly networked third-party organizations house valuable business and personal data that attract cyberattackers. In total, professional and business services were responsible for 7% of all sensitive data breach victims last year.

This industry ranked:

- #2 for the most ransomware attacks
- #5 for third-party/supply chain vulnerabilities

One of the hardest hit business services organizations in 2022 was OneTouchPoint (OTP), a Wisconsin-based third-party mailing and printing vendor to various health insurance carriers and medical providers. To perform its services, OTP was provided certain information by its customers. Unfortunately, last April the company discovered encrypted files as part of a ransomware attack, which compromised PII stored on its systems including name, member ID, birth date, address, health assessment details along with diagnosis codes. The ripple effect of the breach was widespread with more than 78 of its customer organizations impacted, including Anthem ACE, Kaiser Permanent, Humana and several affiliates of Blue Cross Blue Shield.[28]

### Technology

The technology sector is at the forefront of digital acceleration and transformation, resulting in many of these organizations being the targets of both massive data breaches and leaks. These incidents collectively put the sensitive data of 7.3 million people at risk in 2022.

One of the most impactful sensitive data compromises in the technology sector occurred when Connexin Software, which provides practice management and electronic medical records software to pediatric physician practice groups, detected a "data anomaly" on its internal network. According to SC Magazine, "After infiltrating Connexin's internal network, threat actors obtained access to and removed some parts of a patient dataset available online that has been leveraged for data conversion and troubleshooting purpose."[29] The breach compromised the personal health information of more than 2.2 million young patients across 120 pediatric physician practices, potentially exposing Social Security numbers, treatment details and health insurance information. Connexin points out that, "The live electronic record system was not accessed in this incident, and the incident did not involve any physician practice group's systems, databases, or medical records system at all."[30]

## A Closer Look at the Impact of Third-Party and Supply Chain Attacks on Sensitive Data Loss

Modern enterprises rely on a multitude of other businesses every day to deliver products and services into the hands of their customers. Sharing data with these partners is an essential component of working together, but organizations often underestimate the "interconnected risks that exist between the vendors, partners and third-parties we work with on a daily basis."[31] This is especially true since the coronavirus pandemic, when the global supply chain became more reliant upon automation.

More third-party applications, open APIs, vendor relationships, and supply chain components present new risks that often extend beyond the purview of traditional IT monitoring. A single intrusion into one company's system can rapidly domino across hundreds or thousands of that company's downstream partners and clients through a chained sequence of breach events. Unless companies are automatically scanning their own IT environment for sensitive data, they may miss the early warning signals of an orchestrated third-party or supply chain attack.

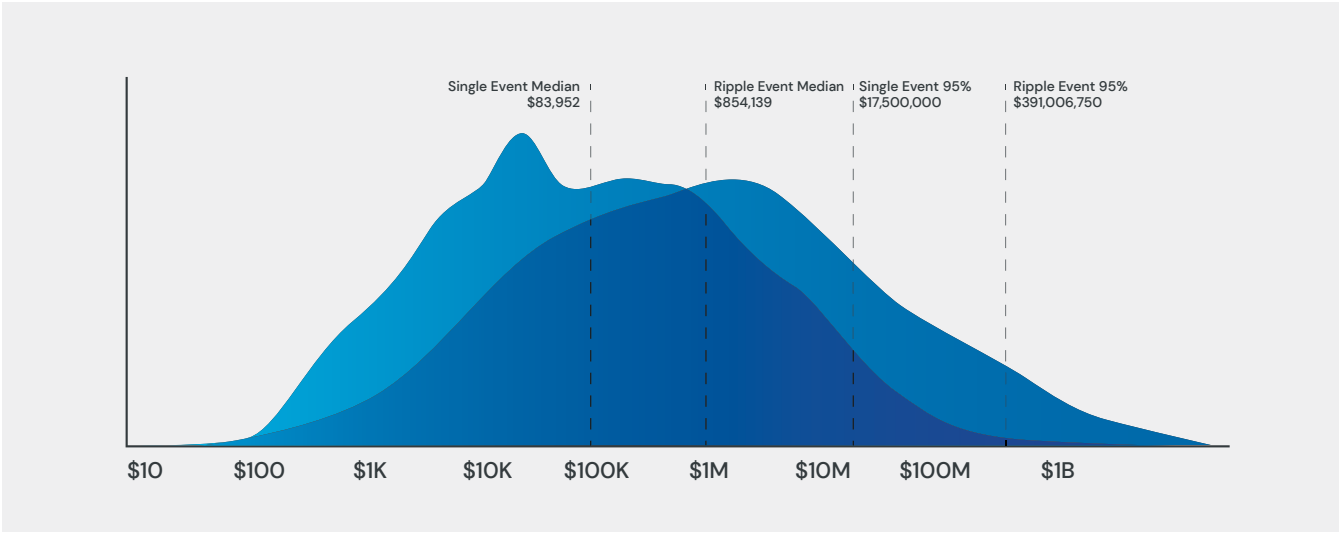
**Gartner predicts that by 2025, 45% of global organizations will be impacted in some way by a supply chain attack.[32]**

In 2022 supply chain and third-party attacks became the favored, high-leverage vector for sensitive data compromises. A total of 118 targeted third-party attacks subsequently infiltrated 1,734 organizations and compromised more than 10 million people. Of these incidents, 62% contained sensitive data, revealing PII for 7.8 million people. Notably, the healthcare industry was impacted in half of all the supply chain attacks in 2022.

| Year | Number of Incidents | Number of Organizations Impacted |
|---|---|---|
| 2022 | 115 | 1,743 |
| 2021 | 84 | 521 |
| 2020 | 69 | 694 |
| 2019 | 104 | 232 |
| 2018 | 82 | 101 |
| 2017 | 103 | 119 |

*Source: Identity Theft Resource Center 2022 Data Breach Report*

## TOTAL RECORDED FINANCIAL LOSSES FOR SINGLE-PARTY VS. MULTI-PARTY SECURITY INCIDENTS

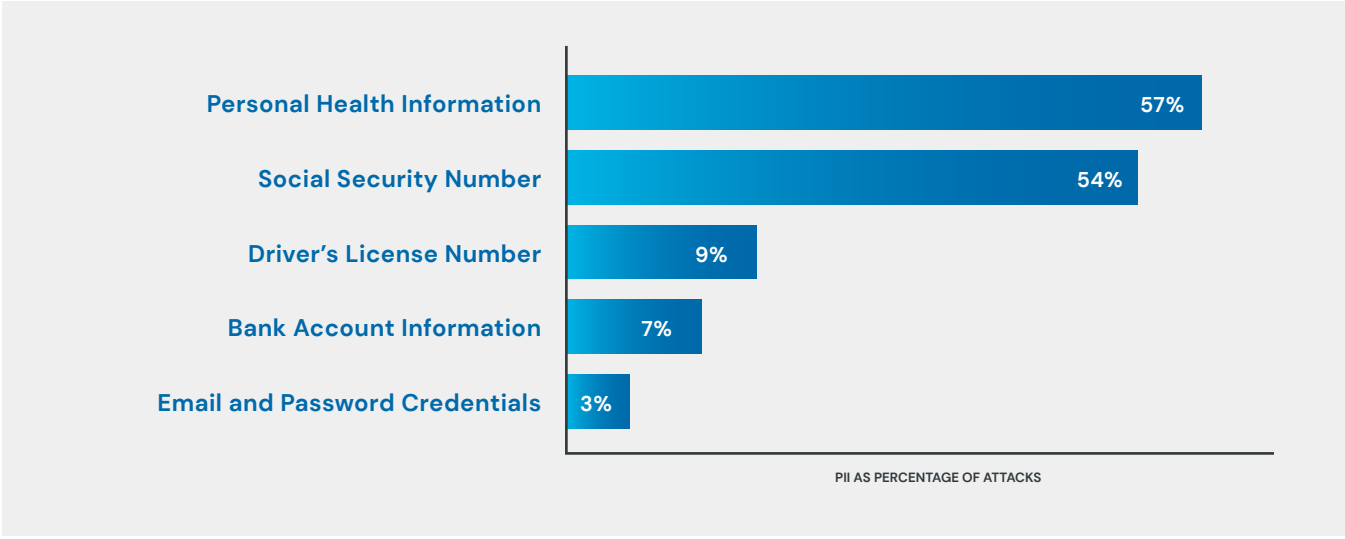



*Source: "Information Risk Insights Study (IRIS) Tsunami: Following the wake of damage from major multi-party cyber incidents." Cyentia. 2021.*

Often, third-party attacks can take longer to detect and contain than single-party attacks, averaging 78 days from initial detection to containment. However, by the time every impacted business detects and remediates the damage, the cyberattack may have experienced a much longer lifespan and provided access to untold volumes of sensitive data.

The ripple effect of third-party and supply chain vulnerabilities means breaches can cost upwards of ten times more than a cyberattack limited to one company.[33] Ponemon Institute revealed that "53% of organizations have experienced at least one data breach caused by a third party. And a data breach costs an average of $7.5 million to remediate."[34]

MOST COMMON SENSITIVE DATA EXFILTRATED FROM SUPPLY CHAIN ATTACKS IN 2022




*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

# Industries Most Impacted by Supply Chain and Third-Party Attacks

Some industries, like healthcare, financial services and education that store more sensitive data, are disproportionately more likely to be impacted by these types of attacks—as we saw last year.

### Healthcare

Healthcare experienced the tsunami effects of 904 third-party downstream system intrusions in 2022, accounting for 82% of the year's top sensitive third-party data breaches. Sharing patient data with third-party vendors plays a major role in successfully running hospital systems, but it also presents more vulnerabilities into the data management lifecycle. One case in point is Eye Care Leaders, an Electronic Medical Records system provider, which served as the first access point for some of last year's largest sensitive data breaches in healthcare, including Texas Tech University Health Science and Wolfe Clinic. Eye Care Leaders experienced a database incident that compromised patient health records and other PII, including health insurance details, Social Security number, and driver license of more than 3.3 million individuals.

### Financial Services

Financial services also felt the ripple effects of 27 third-party cyberattacks that infiltrated 96 organizations and impacted 873,842 individuals. One of the industry's largest third-party breaches stemmed from a ransomware attack against Professional Finance Company (PFC), which manages accounts receivables for hundreds of healthcare organizations around the country. PFC needs access to sensitive patient data to deliver its services. However, that connectivity also means that when PFC experienced a ransomware attack last February, it subsequently exposed 1.9 million patients' personal data across 618 of their customer organizations.

### Education

Although the sheer number of third-party data incidents decreased year-over-year in the education sector, 2022 witnessed the "largest breach of student information in the nation's history when threat actors gained access to the data of 2.1 million students in a single assault—a classic supply chain attack," according to ITRC.[35] That well-positioned attack targeted Illuminate Education, which provides a popular attendance and grading platform used by school systems across the U.S.

**TOP 5 THIRD-PARTY/SUPPLY CHAIN BREACHES IN 2022**

| Company | Number of Third-Parties Impacted | Number of People Impacted |
|---|---|---|
| Professional Finance Company | 618 | 1,918,941 |
| Illuminate Education | 611 | 2,108,045 |
| Shields Health Care Group | 56 | 1,804,069 |
| OneTouchPoint | 43 | 2,651,396 |
| Eye Care Leaders | 37 | 3,372,880 |

*Source: Identity Theft Resource Center 2022 Data Breach Report*

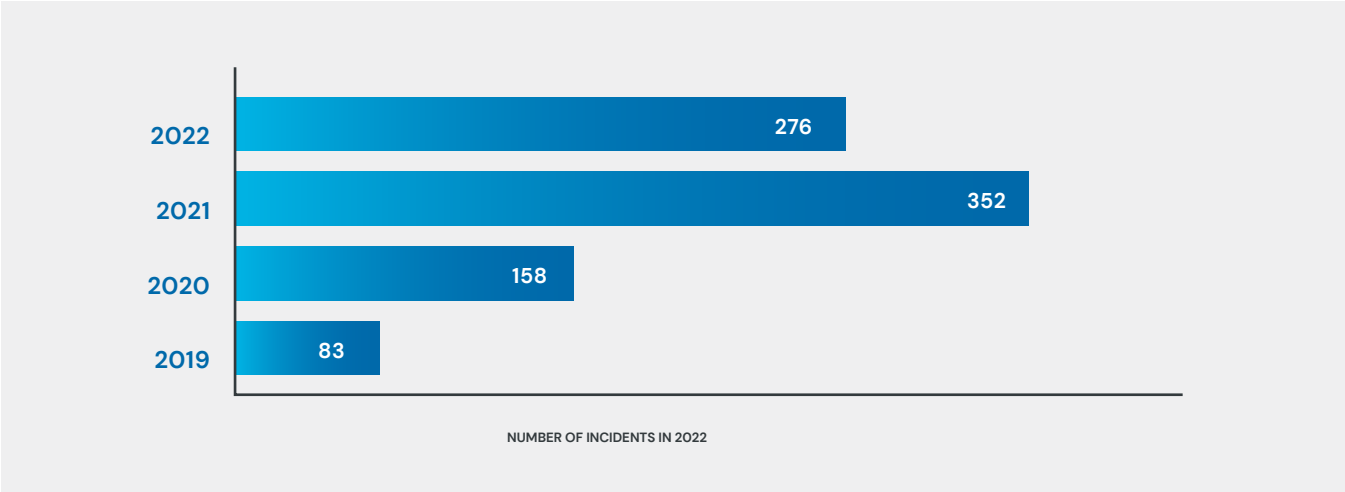
## A Closer Look at the Impact of Ransomware on Sensitive Data Loss

In 2022, businesses around the globe encountered a ransomware attack every 11 seconds.[36] As the year's third most prevalent attack vector, ransomware was at the source of 276 total incidents, with 224 of those incidents (82%) exposing sensitive data. Even though ransomware only represented 18% of the year's total sensitive data incidents, it still impacted more than 12 million people's PII. Attackers often gain access through phishing attacks or accessing public cloud storage, but even with perimeter defenses and employee training to prevent social engineering, unfortunately, these attacks continue to happen with shocking frequency.

According to Enterprise Strategy Group, 79% of organizations surveyed experienced a ransomware attack in 2021.[37] Attackers successfully monetized their illicit system access, exfiltrating data in 41% of reported ransomware incidents. They also went back to where they found initial success: almost one-third of surveyed organizations fell victim to multiple successful ransomware attacks during the same timeframe.[38]

Adding insult to injury, ransomware victims increasingly face double extortion. "Before encryption, attackers can exfiltrate and threaten to publicize the organization's sensitive data. The organization must therefore pay twice: an extortion fee to keep its data private and a ransom to decrypt its data." Even before ransom payments, a ransomware breach can be one of the costliest cyberattacks to manage; on average, a ransomware breach costs organizations $4.54 million between costs, fees, lost business opportunities, and lost productivity.[39] By 2031 ransomware is expected to cost organizations around the world up to $265 billion annually.[40]

## RANSOMWARE YEAR-OVER-YEAR GROWTH

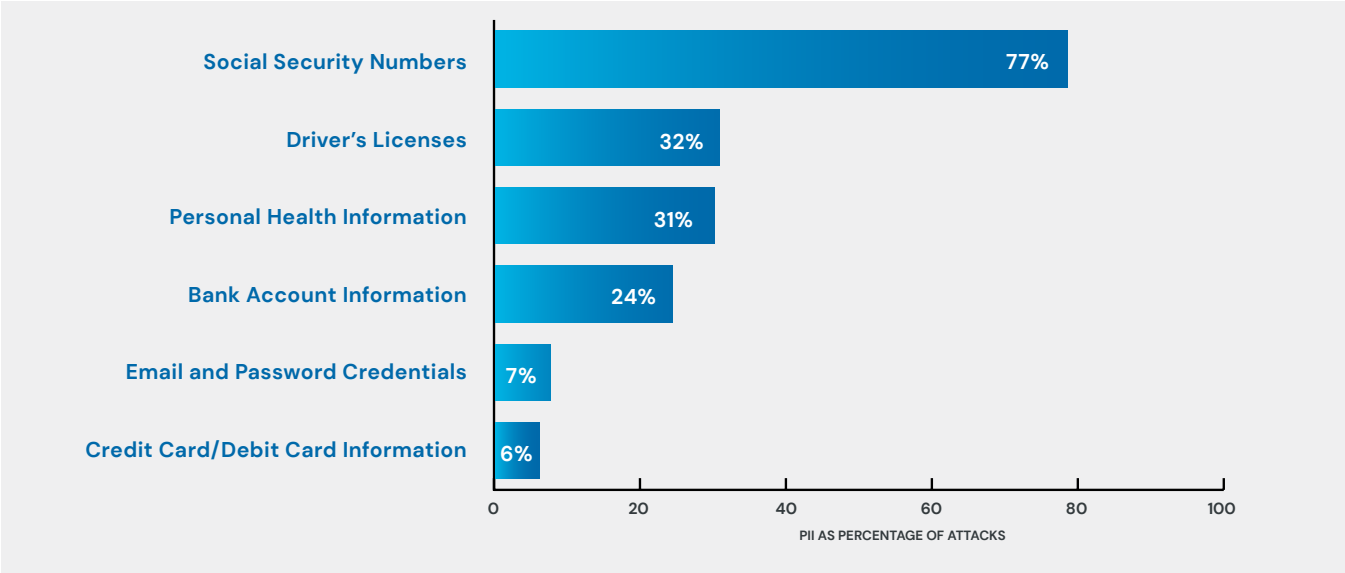



*Source: Identity Theft Resource Center 2022 Data Breach Report*

Ransomware strikes happen quickly, with attackers demanding an average payment of $223,000 within the first 12 to 24 hours of access. In a matter of hours, these attacks are designed to have a wide-reaching effect, impacting everything from employee and customer PII and financial data to operations success.[42]

Since ransomware often comes with the immediate demand for ransom payments in exchange for companies retrieving their data, these attacks often have a shorter life cycle, averaging 24 days. However, even after paying the ransom, organizations fortunate enough to have retrieved some or all of their data must still deal with the impact of having millions of sensitive details accessed by an attacker.

## MOST COMMON SENSITIVE DATA EXFILTRATED FROM RANSOMWARE ATTACKS IN 2022




*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

Half of the year's top ten ransomware attacks were levied against healthcare organizations, exposing Social Security numbers, driver license, personal health data, and other PII. In total, the ten biggest sensitive data ransomware attacks impacted more than 8.1 million people. Professional services, manufacturing, education and critical infrastructure also saw substantial ransomware attacks in 2022.

Many organizations believe ransomware is only a monetary threat. Yet, even after paying exorbitant ransom and often untraceable fees, only 57% of companies report getting back all of their data.[42] For the many healthcare organizations targeted by ransomware in 2022, that meant private health and patient data was constantly at risk.

A data security platform that offers discovery, classification and data protection can stop a ransomware attacker from data exfiltration—especially those unknown and unprotected data stores—thereby limiting an organization's exposure to extortion.


**"A proven monetary model for bad actors, ransomware will continue to be a scourge, but we will see its expansion onto the geo-political stage in 2023. Ransomware will push more into the critical infrastructure that keeps our society humming—as we have recently seen with the Dubai airport attack and energy groups being taken offline state-side—with the goal of being a drag on society as a whole."[43]**

## Protecting your organization from cyber threats

Cyberattacks aren't new; as companies continue to push the frontier of digital transformation, sensitive data exposure is a constant risk organizations must defend against. However, 2022 clearly demonstrated that despite monitoring and preparations to avoid cyberattacks, bad actors will continue to innovate clever new ways to access and leverage attack vectors, both within and beyond an organization's purview.

**Strengthening data discovery, classification, and remediation practices through automation plays a significant role in remaining compliant, detecting breaches early, and keeping the enterprise secure.**

Companies that automate data protection are reported to experience a significant reduction in breach costs, with a breach costing fully automated organizations $3.15 million on average versus $6.2 million for organizations that have not yet fully automated data protection.[44]

Now is the time to prioritize ransomware and third-party risk management protection. That means taking a continuous and proactive stance to strengthen vulnerable attack vectors, reduce your attack surface, and limit the data partners and vendors have access to. This is especially critical for those industries most vulnerable to attack, as recapped in the table below.

**TOP 5 U.S. INDUSTRIES MOST VULNERABLE TO SENSITIVE DATA BREACHES BY INITIAL ATTACK VECTOR IN 2022**

| Supply Chain Attacks | Ransomware Attacks | Insider Errors |
|---|---|---|
| Healthcare | Healthcare | Healthcare |
| Financial Services | Professional Services | Financial Services |
| Retail | Manufacturing | Government |
| Manufacturing | Education | Education |
| Professional Services | Financial Services | Technology |

*Source: Identity Theft Resource Center notified database January 1-December 31, 2022*

One way to strengthen your cybersecurity defenses is by regularly reviewing and inspecting known vulnerable attack vectors, like ensuring cloud security and firewalls are configured correctly. When prioritized, avoidable mistakes like non-secured or misconfigured systems can easily be fixed before a bad actor can gain access. Fixing these mistakes can also reveal new vulnerable attack vectors before they are exploited. Similarly, it's important to update third-party software the moment critical security patches and updates are available. Maintaining an open line of communication with the vendor can help you plan for updates that may require more downtime.

As data breach incidents continue to proliferate, it's no longer a viable option to manually maintain data protection defenses. Without continuous automation, it's no longer a question of "if" your organization will be breached; in fact, it's no longer about "when" you'll be breached, either.

## Data breaches can, and do, strike twice

The data now indicates that organizations must prepare for "how often" they'll suffer an incident. ITRC data supports this disturbing trend. In 2021, more than 24 organizations in the ITRC notified database reported that they had fallen victim to multiple data breaches. Last year, twice the number of organizations experienced multiple breaches in a short period of time.

In one such instance "a series of breaches announced by threat actors and cybersecurity researchers – but not Twitter – more than 400 million accounts attached to an estimated 221 million users were offered for sale by cybercriminals in an illicit identity marketplace. The information was believed to have been scraped from Twitter by identity thieves who took advantage of a software flaw that was reported to have been fixed earlier in 2022 but was still vulnerable to exploitation."[45]

Still other organizations like California Department of Corrections and Rehabilitation and United Healthcare were breached four and five times respectively throughout 2022. In February, California Department of Corrections and Rehabilitation (CDCR) suffered a data breach that exposed Covid test information, in addition to mental health and medical records, potentially

impacting 236,000 inmates. CDCR endured additional breaches in July and August. In October CDCR reported it had been impacted by the CorrectCare breach, a third-party health administrator under contract to process medical claims. United Healthcare similarly endured five breaches during 2022—four due to downstream third-party intrusions that exposed Social Security number, personal health information and email/passwords of an unreported number of its members.

As third-party incidents become more common, the likelihood organizations will experience multiple data breaches within a year will continue to grow. This new reality calls for organizations to dramatically shift how they address the triple threat of compliance demands, breaches, and fraud—starting with an anchored understanding of their sensitive data footprint. Decreasing your data footprint goes beyond managing your internal IT practices and security: organizations must regularly review the vendors they work with, the data they release through those vendor relationships, and the myriad attack vectors that could expose a company to a data incident. Automation play a major role in reducing your data footprint by simplifying data discovery, classification, and remediation.

**IBM found that companies with fully deployed security automation spent an average of $3.15 million on a breach in 2022, while companies without automation support spent an average of $6.2 million.**[45]

## 3 Steps to Preemptively Protect Your Sensitive Data

Detecting, containing, and remediating data breaches takes even longer when companies don't know where their data is stored, who has access to it, and where their weak attack vectors are located. Proactively protecting your organization's sensitive data from breaches, exposures, and leaks may seem daunting, but it doesn't have to be difficult.

**Here are three actionable steps you can take today to secure your sensitive data:**

### 1. Locate all PII

Undiscovered data may be stored in places you wouldn't expect, but without end-to-end visibility across all the endpoints and systems within your IT environment, you may have unknown data at risk of a breach. New data is created every second, and data moves through your organization faster than any person can track.

Understanding where your data lives is a critical first step to reducing exposure. Once you know which endpoints allow access to certain data, your team can easily recognize and strengthen attack vectors that might provide unauthorized access to bad actors.

## 2. Classify and catalog sensitive data

Discovering data records is valuable, but only if you understand what information that data contains. When 80-90% of a company's data is unstructured and not stored in a structured database, many companies don't know what data they're holding on to, making remediating a breach and compliance reporting much more challenging.[46] Classifying and cataloging the sensitive data across your organization is critical to maintaining a strong security posture. By tagging records for specific collection, storage, access, and security parameters, you can more effectively and efficiently manage your growing data.

When using and protecting your sensitive data, context can make a huge difference as to how that data should be managed. Classifying sensitive data based on context can help you determine the most vulnerable and exposed departments within your organization so you can target them first when remediating risk. Inconsistent data management often leads to miscategorization, causing further confusion when a breach occurs.

## 3. Remediate unnecessarily exposed sensitive data

Once data is located and cataloged, companies can take control of where and how their sensitive data is stored. Creating security controls and managing where data is stored can reduce the risk of unnecessarily exposing data. Identifying where data is hiding can provide myriad benefits to your IT team. For example, if data shows up somewhere it doesn't belong, that can indicate where IT needs to remove access or lock down systems to prevent data leaks and breaches. If data is exposed somewhere where it's not intended to be stored, that reveals an opportunity for IT to fix a weak attack vector.

With an end-to-end view of what data was accessed in a breach, your team can effectively report incidents and results to the CEO, Board of Directors, relevant government agencies, and people whose data was impacted in a timely and compliant manner.

# How Spirion can help

Data privacy is critically important in today's technology-first world, but privacy is impossible without security. Traditionally, data discovery, classification, and remediation were necessary, but arduous and time-consuming processes for overworked IT teams. Spirion saves IT time and resources by protecting sensitive data automatically.

Spirion is STEP ONE in sensitive data governance and effective data breach management. With Spirion, organizations can discover the complete landscape of sensitive structured and unstructured data across their IT infrastructure—including on networks, in the cloud, on remote file servers, and on physical devices—with industry-leading 98.5% accuracy. The contextual, automated discovery process continuously captures all sensitive data, eliminating blind spots to reduce the risk of breach or unauthorized access without interrupting day-to-day business operations.

Once data is discovered, automatic data classification allows analysts to better understand their data without applying data compliance and security rules manually. Alongside reducing the risk of human errors, Spirion's Sensitive Data Platform leverages automated playbooks to embed accurate, purposeful labels to data for protection and user access throughout the data lifecycle. These playbooks are designed to align with internal security policies and today's ever-changing regulatory compliance standards for optimal protection and user access.

After the contextually classified data is automatically cataloged, security, privacy and risk management can understand the data within the full IT infrastructure at a glance. From here, automated remediation and data hygiene processes move, encrypt, or delete sensitive data based on sensitivity and use cases. Those processing actions include collection, retention, logging, generation, transformation, use, disclosure, sharing, and disposal of personal data across the entire landscape.

Through secure data erasure, relocation, and containment, companies can reduce their data footprint and further protect their attack surface from breaches. By integrating preferred data security solutions like DLP, IRM/DRM, SIEM, firewalls, and encryption, your organization also decreases regulatory non-compliance risks.

All together, these automated data discovery, classification, and remediation tasks streamline and simplify your data management strategy. With the Spirion Sensitive Data Platform, your organization can preemptively protect sensitive data and reduce the impact of potential data breaches automatically.

1 "Cyber Security Report 2021." Check Point. 2021.
2 "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, November 13, 2020
3 Ibid
4 "Cost of a Data Breach Report 2021." IBM. July 2021.
5 "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, November 13, 2020
6 "Cost of Data Breach Report 2022," IBM, July 2022
7 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
8 "How Many Cyber Attacks Happen Per Day in 2023?," Tech Jury, January 31, 2023
9 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
10 Data Privacy & Security: Industry Predictions and Expert Advice for 2023, Spirion, January 2023
11 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
12 Ibid
13 PII for Sale: Sensitive Data Breaches of 2021, Spirion, January 2022
14 "Addressing the Trust Deficit in Critical Infrastructure: Global Cybersecurity Risk Measurement and Transparency are Key," Security Scorecard, January 2023
15 Microsoft Digital Defense Report 2022, 2022
16 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
17 "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybersecurity Ventures, November 13, 2020
18 "Cost of a Data Breach Report 2021." IBM. July 2021.
19 Ibid
20 "Cost of Data Breach Report 2022," IBM, July 2022
21 Ibid
22"Cash App is notifying 8.2 million U.S. customers of a data breach," Mashable, April 6, 2022
23 Data Privacy & Security: Industry Predictions and Expert Advice for 2023, Spirion, January 2023
23 "Notice of Data Security Incident," Shields Health, July 25, 2022
24 "Community Health Network reports online tracking data breach affecting 1.5 million," Healthcare IT News, December 5, 2022
25 Ibid
26 Ibid
27 "," IBM, July 2022
28 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
29 "Additional Orgs Report Aftermath of OneTouchPoint Data Breach," Health IT Security, September 7, 2022
30 "Over 2.2M pediatric patients impacted by Connexin Software breach," SC Magazine, December 1, 2022
31 Ibid
32 "Data Breach Investigations Report 2022," Verizon, 2022
33 "7 Top Trends in Cybersecurity for 2022," Gartner, April 13, 2022
34 "Information Risk Insights Study (IRIS) Tsunami: Following the wake of damage from major multi-party cyber incidents." Cyentia. 2021.
35 "The Rise Of Third-Party Digital Risk," Forbes, July 14, 2020
36 "2022 Data Breach Report," Identity Theft Resource Center, January 2023
37 "Ransomware Statistics in 2022: From Random Barrages to Targeted Hits," DataProt, January 2023
38 "The Long Road Ahead to Ransomware Preparedness," Enterprise Strategy Group, 2022
39 Ibid
40 "Cost of Data Breach Report 2022," IBM, July 2022
41 "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," Cybercrime Magazine, June 2, 2022
42 "Cloudian Ransomware Survey Finds 65% of Victims Penetrated by Phishing Had Conducted Anti-Phishing Training." Cloudian. July 15, 2021.
43 Ibid
44 Ibid
45 " 2023 Data Privacy Predictions Part 1," Privacy Please Podcast, S3, E142
46 "Cost of Data Breach Report 2022," IBM, July 2022
47 "Cost of Data Breach Report 2022," IBM, July 2022
48 Harbert, Tam. "Tapping the power of unstructured data." MIT Sloan School of Management. February 1, 2021.


## Talk to a Spirion data security and compliance expert today: expert@spirion.com

Spirion has relentlessly solved real data protection problems since 2006 with accurate, contextual discovery of structured and unstructured data; purposeful classification; automated real-time risk remediation; and powerful analytics and dashboards to give organizations greater visibility into their most at-risk data and assets. Visit us at spirion.com



4192023 REP-PPI22-003