SPIRION

REPORT

PII for sale: A definitive guide to sensitive data breaches

America's top leaks, attacks, and insider hacks of 2021

Cyberattacks are a near constant threat to modern businesses with attacks occurring every 10 seconds.[1] During the month of January 2021 alone, 878.17 million data records were compromised—more than the total 826.53 million records stolen throughout all of 2017.[2]

Every minute of every day, cybercrime collectively costs organizations worldwide over $1.79 billion.[3] These costly breaches won't be disappearing anytime soon, but they'll certainly leave a lasting impact on the organizations that fall victim to these crimes.

The costs of sensitive data breaches go far beyond the $180 estimated fines per lost or stolen data record containing personally identifiable information (PII).[4] The financial impacts of a breach extend to operational losses, a weakened competitive stance, compromised customer trust and brand reputation, and exposed intellectual property. Above all, these assaults cost your customers, employees, and partners their digital identities and the fundamental human right to data privacy.

Hardly a day passes without hearing about the latest big-name data breach, and yet often the detrimental impacts to our personal information go unnoticed. 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 data leaks, cyberattacks, and inside hacks of sensitive information in 2021. Based on this data, this definitive guide outlines actionable steps you can take today to reduce your organization's data exposure and risk in 2022 and beyond.

Data analysis methodology

This Definitive Guide to Sensitive Data Breaches is based on the analysis of more than 1,862 incidents that were reported by U.S.-based organizations from January 1 through December 31, 2021. 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 2021 data breaches that specifically involved the compromise of sensitive data. We analyzed those instances to identify the top sensitive data breaches by the number of 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 2021 in Review Data Breach Annual 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 2021

The world's overnight sprint towards digital transformation accelerated as companies shifted to remote and hybrid work amid the COVID-19 quarantines of 2020. The immediate necessity for remote work environments collapsed what would have surely taken years of preparation to being fully operational down to mere months.

Combining new technology, third-party applications, and home networks enabled employees to work from home during a time when working from the office wasn't viable, but it also presented significant IT challenges and data security risks. As companies managed the rapid changes necessary to keep operations running smoothly in 2021, sophisticated attackers continued to discover vulnerabilities and engineer new vectors for exposing company data.

By mid-August, the number of data breaches reported to state authorities and collected by the ITRC had already exceeded the total number of incidents in all of 2020. According to ITRC, a total of 1,862 data compromises were reported by U.S. organizations in 2021—which surpassed 2017's all-time high. Comparatively, 2020 saw a total of 1,108 incidents.

U.S. DATA BREACHES 2017-2021

Year	Total Incidents[5]	# Sensitive Data Incidents	% Sensitive Data Incidents	Individuals Impacted
2021	1,862	1,543	83%	293,927,708
2020	1,108	882	80%	310,116,907
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 2021 in Review Data Breach Annual Report

With a global average cost of $4.25 million per data breach, preventing these data compromises has become more pressing for enterprises around the world.[6] All told, the economic toll of 2021's rampant data breaches is estimated to have cost organizations more than $7.9 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 modern organizations. There are different types of data exposure 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 (96%) of last year's incidents were data breaches that exposed the data of 189,523,878 individuals as reported by ITRC.[7] However, since data is removed from a system in a breach, privacy victims may be at risk of identity theft and fraud long after the initial breach.

45% of U.S. companies report experiencing a data breach in the past.

In 2021, 47% saw an increase in the volume, severity, and/or scope of cyberattacks.[8]

Source: "2021 Thales Data Threat Report: Data Security in the Era of Accelerated Cloud Transformation and Remote Work." Thales. June 2021.

In contrast to data breaches, a data exposure incident 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 just 3% of the year's total data incidents, but their impact is wide-ranging. Data exposures inadvertently made almost 7 billion records readily accessible to unauthorized users, or 37% of the year's total number of compromised records. In 2021 alone, these incidents left 104 million people's data vulnerable to exposure.

Data leaks also present a substantial risk to sensitive data. The ITRC defines a data leak as the legal collection of data that is misused in ways that do not align with the original intentions for collection. In 2021, seven massive data leaks, including those of Linkedin, Facebook and RockYou, compromised the data of 1.8 billion individuals—demonstrating the catastrophic effect data misuse can have.

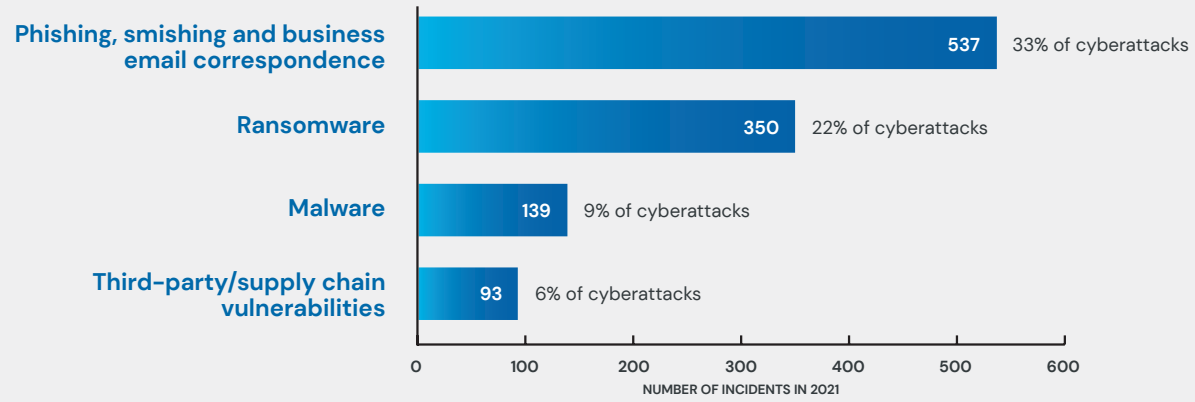
Whether data is intentionally stolen or misused, or data is accidentally exposed or removed from a system, all of these scenarios present a significant risk to data privacy, protection, and compliance.

How did data compromises happen in 2021?

With an increase in potential attack vectors and the challenges of monitoring an expansive off-site footprint, it's clear the pandemic continued to play at least a partial role in compromising sensitive data. A larger attack surface and more vulnerable vectors presented new opportunities for both external and internal actors to access and abuse data. As bad actors become more prevalent and sophisticated, IT teams must vigilantly monitor their data to maintain security and privacy standards.

Many of the data compromises that occurred in 2021 were particularly difficult to detect or avoid. For example, almost one-fourth of the year's compromises started through a third-party or supply chain vulnerability, which can be challenging to identify early, even with end-to-end visibility.

Cyberattacks accounted for 87% of 2021's events (1,613 incidents) that compromised 188,400,415 individuals by successfully leveraging these top attack vectors:



Human or system errors played a role in 10% of all incidents in 2021, which compromised the data privacy of 104,891,759 individuals through vulnerable vectors:

- Non-configured cloud security of misconfigured firewalls (67 incidents)
- Email correspondence (66 incidents)
- Lost device or document (12 incidents)

It's worth noting that even though non-secured or misconfigured cloud environments weren't as common an attack vector as some may have expected in 2021, these attacks had a huge impact on the companies that reported falling victim to them. These instances were particularly critical for the 64% of companies that sped up cloud migrations in 2020 and 2021—many of which could experience data compromises from cloud transition mistakes in the future.[9]

These instances, plus the 3% of incidents involving physical attacks like device and document theft or improper disposal, are often attributed to unintentional internal actors. In 2021, our research showed that internal actors were responsible for 7% of the year's data compromises, while external actors accounted for 93% of breach incidents.

Some of the year's largest data compromises captured swathes of non-sensitive data records. While this data cannot identify users or customers, it often does include email and password data that can be used in combination to pose a threat to user security or business information.

TOP 10 NON-SENSITIVE DATA COMPROMISES OF 2021

Organization	Total Records Compromised	Individuals Impacted	Attack Vector	Industry
CVS Health	1,148,327,840	N/A	System & Human Error - Third Party/ Supply Chain	Retail
DreamHost	815,000,000	N/A	System & Human Error - Failure to Configure Cloud Security	Technology
Cognyte	790,164,806	N/A	System & Human Error - Failure to Configure Cloud Security	Technology
LinkedIn	N/A	700,000,000	Data Leak - Third Party/Supply Chain	Technology
Facebook	509,458,528	533,000,000	Data Leak - Failure to Configure Cloud Security	Technology
LinkedIn	N/A	500,000,000	Data Leak - Third Party/Supply Chain	Technology
Gravatar	N/A	113,990,759	Data Leak	Technology
OneMoreLead	126,000,000	63,000,000	System & Human Error - Failure to Configure Cloud Security	Business Service
GetHealth	61,000,000	N/A	System & Human Error - Failure to Configure Cloud Security	Technology
ParkMobile	410,000	21,000,000	Cyberattack - Failure to Configure Cloud Security	Technology

Source: Identity Theft Resource Center notified database January 1-December 31, 2021

Emerging trends in cyber attacks

Hackers have become more sophisticated, and attacks in 2021 looked dramatically different than in years past. Rather than targeting individual companies, today's cybercriminals are looking for points of leverage within the supply chain. 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. Third-party and supply chain attacks gained popularity in 2021; 93 well-positioned attacks rapidly spread across 559 entities, contributing to 30% of the year's total impacted organizations.

As in previous years, attackers were successful leveraging social engineering to take advantage of human error. Undetected security gaps from rapid technological acceleration, myriad third-party applications, and compromised APIs have also given rise to sophisticated new attack vectors, such as third-party/supply chain vulnerabilities and ransomware.

Identity Theft Resource Center President and CEO Eva Velasquez emphasizes, **"The number of breaches in 2021 was alarming. Many of the cyberattacks committed were highly sophisticated and complex, requiring aggressive defenses to prevent them."**

In 2021 alone, global ransomware attacks increased by 25% year over year,[10] and as one of the fastest growing cybersecurity threats,[11] it's safe to assume attackers will continue to use this financially lucrative method. 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, manufacturing, and critical infrastructure. As these organizations shift to storing data on the public cloud, misconfigurations present situations where unstructured or uncategorized data can be accessed or stolen without detection, putting millions of sensitive data points at risk. Often, these organizations do not have the data lifecycle management strategy or modern cybersecurity tools to support their rapidly-increasing data sprawl.

The amount of data threatened in a breach in 2021 is 12x higher than 2017. The number of impacted data records is predicted to increase threefold year over year.[12]

Despite more organizations experiencing data compromises, the ITRC reported that 33% of organizations underreported data breaches in 2021. 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. Similarly, the ITRC discovered that many organizations and state agencies did not report their data incidents on a timely basis or failed to include relevant details in 2021. 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.

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 GDPR and CPRA lead to even higher fines for unreported or underreported breaches within a strict notification timeframe.

GDPR penalties in Q3 of 2021 cost companies over $1.14 billion, 3x higher than the GDPR fines issued in all of 2020.[13]

As the California Privacy Rights Act (CRPA)—an amendment to the preexisting California Consumer Privacy Act—goes into effect January 1, 2023, the U.S. may see companies revealing more details around the data breaches they experience. Starting on January 1, 2022, organizations must start gathering and maintaining consumer personal information to align with CRPA requirements. The new guidelines set the tone for future legislation across the U.S. by giving consumers more 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 macro view: a closer look at sensitive data compromises in 2021

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.

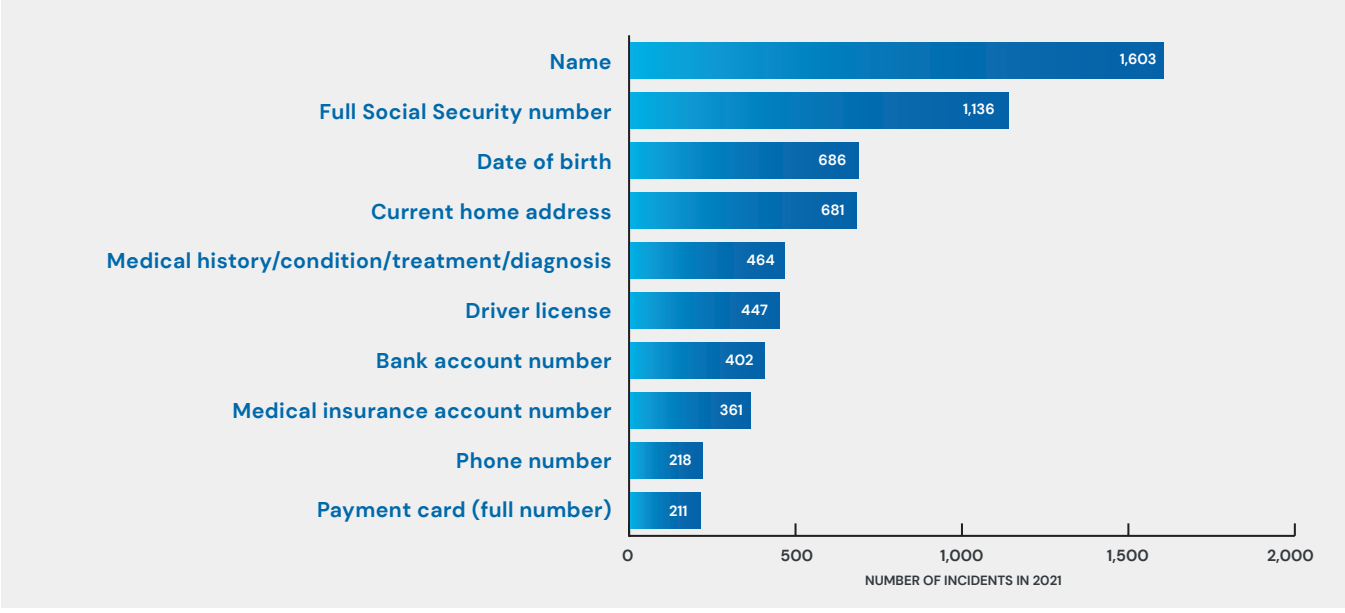
ITRC's 2021 in Review Data Breach Annual Report revealed that 1,543 incidents (or 83% of all incidents) compromised the sensitive data of over 150 million individuals in 2021.

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 more—can be especially valuable for attackers to buy and sell.[14]

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.

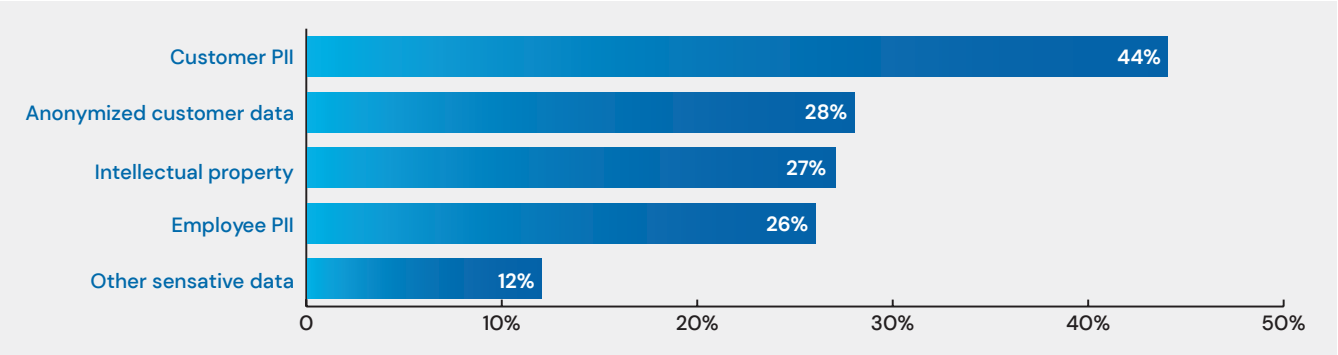
MOST COMMON PII EXFILTRATED DURING SENSITIVE DATA BREACHES IN 2021



Source: Identity Theft Resource Center 2021 in Review Data Breach Annual Report

Customer PII is the most common type of record that is lost or stolen (44% of all data breaches),[15] and employee PII is exfiltrated in 26% of breaches. 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.

PERCENTAGE OF TYPES OF RECORDS COMPROMISED IN DATA BREACHES



Source: Cost of a Data Breach Report 2021." 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, while exposed employee PII cost $176 apiece.[16] Based on these fines alone, organizations are estimated to have lost between $26.5 and $27 billion in 2021 after exposing the sensitive employee or customer data of over 150 million people—not to mention lost business opportunities and reputational damages. The exorbitant cost and loss of trust are just part of the reason organizations must secure vulnerable attack vectors to prevent unauthorized access to sensitive data in 2021 and beyond.

Sensitive data vectors of attack

Exfiltrating sensitive data via targeted cyberattacks was the primary way external actors gained unauthorized access to personal data in 2021. External actors carried out 93% of all sensitive data incidents last year, compromising the personal information of 150 million people.

Cyberattackers successfully executed 96% of all sensitive data breaches by leveraging these top attack vectors to access PII:

TOP ATTACK VECTORS LEVERAGED IN SENSITIVE DATA BREACHES IN 2021

Attack Vector	Percent Total	Total Incidents	Individuals Impacted
Third party/supply chain	25%	356	6,943,686
Phishing, smishing, business email correspondence	23%	330	4,782,380
Ransomware	17%	249	14,077,620
Malware	8%	111	2,533,047

Source: Identity Theft Resource Center notified database January 1-December 31, 2021

Meanwhile, internal actors were responsible for 7% of sensitive data compromises, placing 878,556 people's PII at risk, largely through human error including email correspondence and misconfigured cloud security. While 28% of sensitive data breaches caused by internal actors were due to socially engineered email correspondence methods, the amount of information exposed in these incidents was generally smaller compared to cloud security or firewall configuration issues. The smallest percentage of sensitive data breaches involved physical attacks through document or device theft or improper disposal, accounting for 28 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, companies 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 misconfigured firewalls took well over a year to detect and contain on average last year, while non-secured cloud environments took an average of 87 days. Meanwhile, human and system errors had an average lifecycle of 161 days, presenting substantial risks for companies without robust monitoring capabilities.

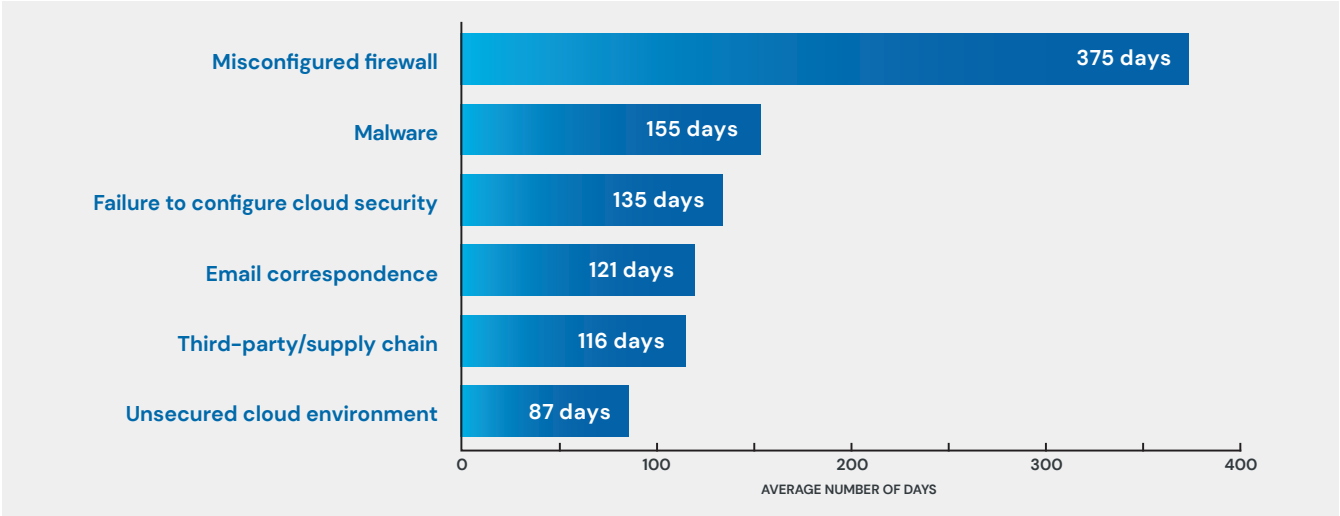
ITRC data revealed that the average sensitive data breach has a lifecycle twice as long as a non-sensitive data breach.

The average sensitive data breach took 112 days to detect in 2021, while a non-sensitive data breach only took 52 days. It also 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 207 days to detect and contain, whereas external attacks had an average lifecycle of 75 days. Often, monitoring is focused on external cyberattacks, meaning internal errors went unnoticed for 4 months longer on average 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 $4.87 million on average, while breaches that took fewer than 200 days cost companies $3.61 million on average.[17]

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, 2021

Industries most impacted by 2021 sensitive data breaches

While every industry includes organizations that collect and store sensitive data, some sectors are responsible for monitoring substantially more sensitive data. 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 people's personal data in 2021:

INDUSTRIES MOST IMPACTED BY SENSITIVE DATA INCIDENTS IN 2021

Industry	# Incidents	# Individuals Impacted	% Total Individuals Impacted
Professional & business Services	157	52,076,332	35%
Telecommunications	8	47,811,470	32%
Healthcare	447	24,786,844	17%
Retail	110	8,529,013	6%
Financial Services	234	6,263,519	4%
Technology	51	3,256,527	2%

Source: Identity Theft Resource Center notified database January 1-December 31, 2021

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 35% of all sensitive data breach victims last year.

One of the hardest hit professional organizations in 2021 was Astoria Company, a lead generation company that shares volunteered consumer information with multiple businesses in the automotive, medical, and finance industries. The company discovered that, after being hacked by cybercrime group ShinyHunters, its 300 million user database containing 40 million Social Security numbers, 20 million users' bank information and SSNs, and 30 million identifiable personal health records was leaked onto the dark web.[18]

Meanwhile, professional services groups that work with healthcare data saw many sensitive data attacks in 2021. One example is a ransomware attack on Ohio healthcare-focused law group Bricker & Eckler LLP, which exposed the names, addresses, personal health information, driver licenses, and/or Social Security numbers for 420,532 clients.[19]

Telecommunications

Even though the telecommunications sector had fewer than 1% of 2021's data incidents, a single breach by T-Mobile sent this industry to the top of the list. This massive data breach occurred when a hacker gained access to the names, birthdates, driver licenses, Social Security numbers, addresses, and phone numbers of over 47 million T-Mobile customers.[20] The breach went undetected for five months, demonstrating the colossal impact that can happen when malicious actors gain access to a non-secure cloud environment.

Meanwhile, Syniverse—a global telecommunications infrastructure company that routes billions of text messages annually and calls itself the "world's most connected company"—revealed in a September 2021 SEC filing that hackers hid inside its systems for five years, impacting millions of cellphone users worldwide.[21]

Healthcare

After reporting 447 incidents that impacted 24.8 million people, healthcare ranked number one in sheer volume of sensitive data incidents last year, including five of the year's top ten sensitive data breaches.

The largest sensitive data breach (responsible for 13% of the industry's breach victims) occurred at 20/20 Eye Care Network, where misconfigured Amazon Web Services security enabled bad actors to access the names, addresses, birthdates, Social Security numbers, member identification numbers, and health insurance information for 3,253,822 customers.[22] Nearly as catastrophic, a data breach at Forefront Dermatology gave cyberattackers access to the records of 2,413,533 patients, including names, addresses, birthdates, and personal health information.[23] The DNA Diagnostics Center also faced a substantial breach of an unsecured and archived database, where Social Security numbers and payment information may have been revealed for 2,102,436 customers.[24]

Average healthcare data breach costs increased 29.5% year over year, reaching $9.23 million in 2021.[25]

Many healthcare companies also fell victim to ransomware in 2021. The University Medical Center of Southern Nevada was hit with the REvil ransomware attack, resulting in the posting of driver licenses, passports, and Social Security cards for over 1.3 million patients.[26] When the St. Joseph's/Candler hospital system discovered a ransomware breach in June 2021, they were already six months too late: cyberattackers had stolen PII from 1.4 million patients, including personal health information, Social Security numbers, and driver's licenses.[27]

Retail

With the steep rise in e-commerce transactions throughout the pandemic, cyberattackers are looking for more opportunities to gain unauthorized access to data through retailers. Even though these breaches tend to be smaller than other industries, 71% of retail companies reported enduring a data breach at some point and 39% shared they had been breached within the last year.[28]

Luxury department store Neiman Marcus was one of the most prominent examples of a massive cyberattack last year, exposing the names, contact information, credit card information, and login credentials for 4,354,346 users.[29] Automotive leader Volkswagen Group of America also fell victim, exposing the phone numbers, email addresses, and car purchase history or eligibility for over 3.1 million Americans and 3.3 million people total.[30] Together, these two household brands were responsible for 87% of the retail industry's data breach victims in 2021.

Financial Services

Next to healthcare, financial services experienced the second highest volume of total data breaches in 2021, with 82% (234 incidents) involving sensitive data that impacted 6.2 million people. The largest of these attacks occurred at Flagstar Bank, where a supply chain vulnerability with Accellion's file transfer software caused a breach that revealed the names, addresses, and Social Security numbers for over 1.4 million customers. Some of those affected were even surprised to learn that Flagstar had their information; these customers discovered during the notification process that Flagstar had taken over servicing their mortgages.

Meanwhile, online stock trading platform Robinhood confirmed that a November 2021 cyberattack revealed personal information, including email addresses, customer names, and more, for 7 million customers. At least ten customers were confirmed to have sensitive data exposed in the breach.[32]

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 hundreds of millions of people at risk in 2021.

For example, clinical trial software company Deep6.AI exposed more than 886 million personal health records during a data breach in October.[33] Meanwhile, LinkedIn's and Facebook's Q2 data leaks collectively exposed the names and emails of 1.7 billion people.

One of the most impactful sensitive data compromises in the technology sector occurred when SmarterSelect, a U.S. software company that helps organizations manage their scholarship application processes, exposed the data of 1,200,000 students in a data leak. A misconfigured Google Cloud Storage bucket revealed 1.5 terabytes of information, including Social Security numbers, student photos, financial aid information, and more.[34]

TOP 10 U.S. SENSITIVE DATA COMPROMISES OF 2021

Organization	Impact	Sensitive Data Compromised	Attack Vector	Industry
Deep6.ai	886,521,320 exposed records	Personal health information	Third-Party/ Supply Chain	Technology
Astoria Company LLC	50,000,000 individuals	Addresses, phone numbers	Failure to Configure Cloud Security	Business Service
T-Mobile	47,800,000 individuals	Social Security number, phone number, driver license, addresses	Non-secured cloud environment	Telecommunications
Neiman Marcus	4,354,346 individuals	Credit/debit card, email/password	Cyberattack	Retail
20/20 Eye Care Network	3,253,822 individuals	Personal health information	Phishing/Business Email Compromise	Healthcare
Volkswagen Group of America	3,100,000 individuals	Social Security number, driver license, email/password	Non-secure cloud environment	Manufacturing
Forefront Dermatology	2,413,553 individuals	Personal health information, addresses	Phishing/Business Email Compromise	Healthcare
DNA Diagnostic Center	2,102,436 individuals	Social Security number, bank informa-tion	Failure to Configure Cloud Security	Healthcare
Flagstar Bank	1,465,002 individuals	Social Security number, addresses	Accellion Supply Chain	Financial Services
St. Joseph's / Candler	1,400,000 individuals	Social Security number, driver license, personal health information	Ransomware	Healthcare

Source: Identity Theft Resource Center notified database January 1-December 31, 2021

A closer look at the impact of third-party/ 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 far-reaching impact a partner breach can have on their business.

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 vulnerable attack vector in one company can be parlayed to infiltrate tens or hundreds of that company's partners and clients. Companies like CaptureRX—a health IT company supporting hospitals around the country to manage prescription discount programs—needs access to sensitive health data to deliver its services. However, that means when CaptureRX experienced a ransomware attack, it exposed 2.4 million patients' personal data across 148 healthcare companies that they work with.[35]

On average, an enterprise used 288 different SaaS applications across their business in 2020. Organizations churn through over 30% of applications each year, presenting the risk of data leaks and security risks.[36]

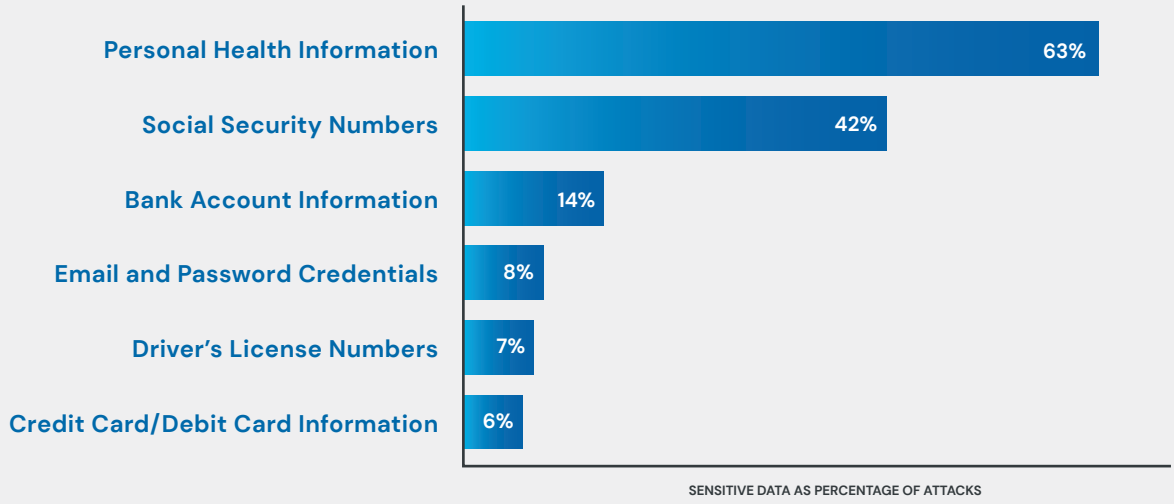
Supply chain and third-party attacks became a top contributor to data compromises in 2021.

A total of 93 third-party attacks impacted 559 organizations, exposing more than 1.1 billion data records. Of these incidents, 83% contained sensitive data, revealing PII for 7.2 million people.

Source: ITRC's 2021 in Review Data Breach Annual Report

Notably, the healthcare industry was impacted in half of all the supply chain attacks in 2021.

MOST COMMON SENSITIVE DATA EXFILTRATED FROM SUPPLY CHAIN ATTACKS IN 2021

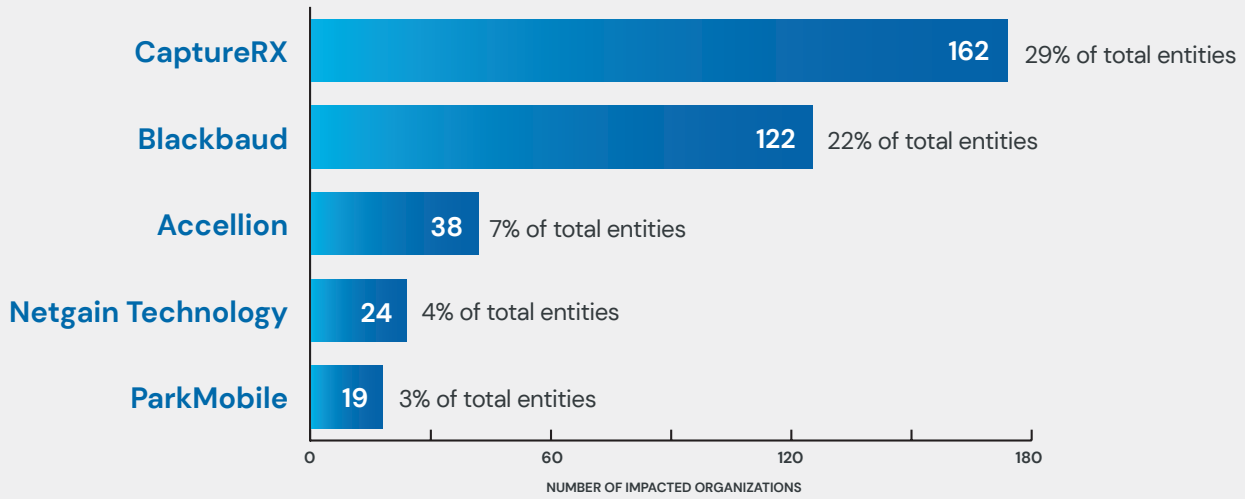


Source: Identity Theft Resource Center notified database January 1-December 31, 2021

Accellion, Netgain Technology, and Elekta—three popular vendors among healthcare companies—were the initial point of leverage for eight of 2021's top ten third-party breaches. These three vendors served as the first access point for some of last year's largest sensitive data breaches in healthcare, including Trinity Health, Northwestern Memorial Healthcare, Apple Valley Clinic, and more.

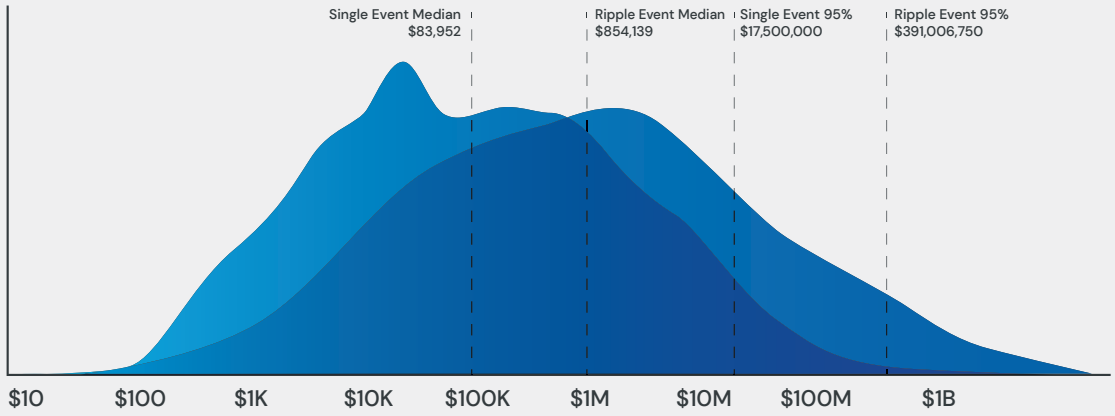
Some third-party cyberattacks have an even larger footprint, like the Kaseya Virtual System Administrator (VSA) servers. In this notable July 2021 REvil ransomware breach, 800 to 1,500 downstream organizations and 1 million endpoints were impacted.[37] The tsunami effect of third-party and supply chain vulnerabilities means breaches can cost upwards of ten times more than a cyberattack limited to one company.[38]

MOST IMPACTFUL THIRD-PARTY BREACH VECTORS IN 2021



Source: Identity Theft Resource Center notified database January 1-December 31, 2021

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

These instances became more common in 2021, as cyberattackers discovered they could create a larger ripple effect by finding a weak point of attack with a service provider. Often, these attacks can take longer to detect and contain than single-party attacks, averaging 116 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. 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.

Industries most impacted by supply chain and third-party attacks

Over 53% of companies report experiencing at least one breach in the past two years caused by a third-party partner.[39] Yet, some industries which store more sensitive data are disproportionately more likely to be impacted by these types of attacks.

- Healthcare experienced 195 third-party cyberattacks in 2021, accounting for half 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.
- Education saw 18% of the year's third-party cyberattacks, many of which were attributable to a ransomware attack against software supplier Blackbaud. This attack, which was initially detected in July 2020, leveraged a weak attack vector in the company's Raiser's Edge donor software to infiltrate approximately 480 of their customers in 2020 and another 122 education, healthcare, nonprofit, and social good organizations during 2021. In total, the sensitive data of more than 602 organizations and 12.8 million people has been compromised throughout the multi-year event.
- Meanwhile, retail witnessed 8% of the year's sensitive data supply chain attacks, while financial services and non-profit organizations experienced 7% and 5% respectively. Despite the large Blackbaud third-party attack affecting manufacturer Volkswagen Group of America, manufacturing as an industry was more impacted by single-event attacks than multi-group attacks.

A closer look at the impact of ransomware on sensitive data loss

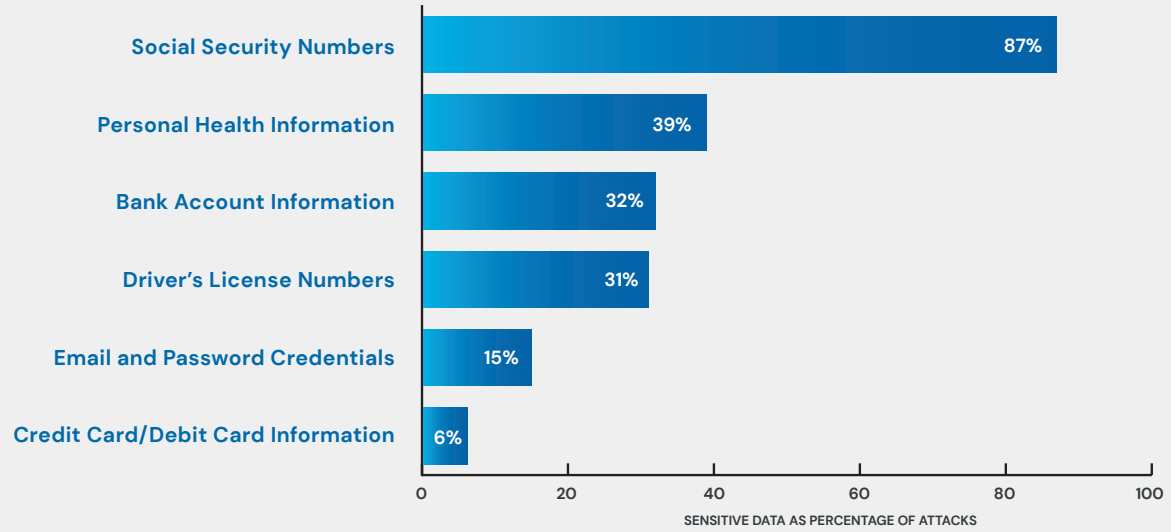
Many of 2021's cyberattacks were attributable to ransomware. Since ransomware often comes with the immediate demand for ransom payments in exchange for companies retrieving their data, these attacks often have a shorter life cycle, averaging 24 days. However, even after paying the ransom, organizations 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.

As the year's second most prevalent attack vector, ransomware was at the source of 280 total incidents, with 249 of those incidents (89%) exposing sensitive data. Even though ransomware only represented 16% of the year's total sensitive data incidents, it still impacted more than 14 million people's PII. Plus, even before ransom payments, a ransomware breach can be one of the costliest cyberattacks to manage; on average, a ransomware breach costs organizations $4.62 million between costs, fees, lost business opportunities, and lost productivity.[40]

63% – percentage of data breaches where financial gain is the primary motivation

81% – percentage of ransomware attacks where financial gain is the primary motivation[41]

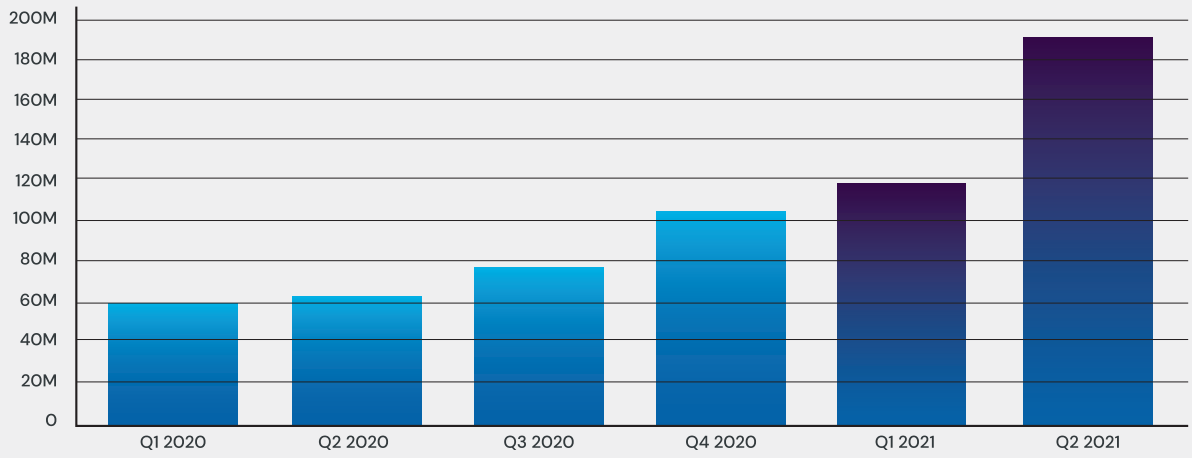
MOST COMMON SENSITIVE DATA EXFILTRATED FROM RANSOMWARE ATTACKS IN 2021



Source: Identity Theft Resource Center notified database January 1-December 31, 2021

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 are rapidly increasing in frequency. 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]

RANSOMWARE GROWTH BY QUARTER BETWEEN Q1 OF 2020 TO Q2 OF 2021



Source: "2021 SonicWall Cyber Threat Report." SonicWall. July 2021.

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.[43] For the many healthcare companies targeted by ransomware in 2021, that meant private health and patient data was constantly at risk.

Eight of the year's top ten ransomware attacks were levied against healthcare organizations, exposing Social Security numbers, personal health data, and other PII. In total, the ten biggest sensitive data ransomware attacks impacted nearly 9.5 million people. Manufacturing, professional services, financial services, and education also saw substantial ransomware attacks in 2021.

A closer look at the impact of human error on sensitive data loss

Human error often plays an indirect role, contributing to as many as 95% of data breaches.[44] To a great extent, people internal to an organization are often responsible for falling victim to phishing attacks, maintaining poor password health, and increasing the vulnerability of other access points through unconfigured cloud security or misconfigured firewalls. However, even if these situations open the initial point of access, organizations often see beyond these mistakes and look at the overarching security risk the mistake exposed.

10% of 2021's data compromises were directly attributable to human and system errors, which left 3.8 billion sensitive data records vulnerable and exposed.

Whether by accident or malicious insiders, two-thirds of the year's employee errors and intentional acts revealed the sensitive data of more than 2.4 million people.

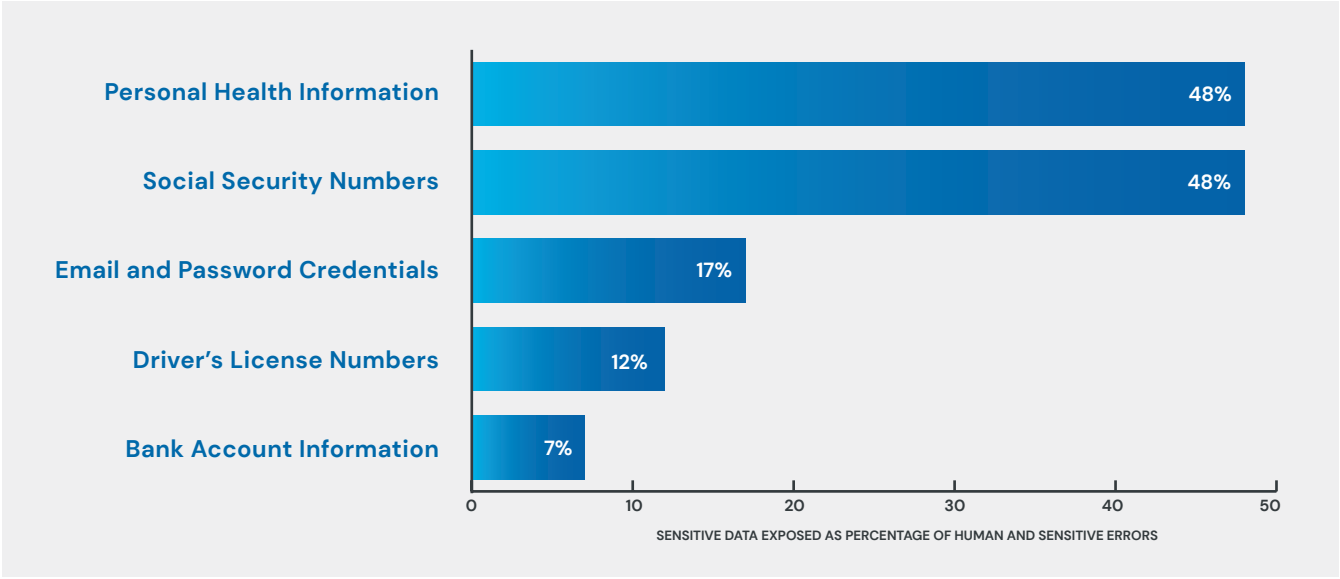
Configuration issues are often to blame for large internal breaches, where security was not properly set up to prevent an attack. Two common configuration issues—failure to securely configure cloud security and misconfigured firewalls—led to seven of the year's most prolific human error breaches. In total, configuration issues were responsible for exposing the sensitive data of 2 million people last year. Even though 33% of enterprises report experiencing unauthorized access to cloud resources, 19% didn't know if unauthorized access actually occurred.[45]

Aside from configuration problems, email correspondence and lost devices or documents are common human errors that lead to data breaches. Even though only 7% of sensitive data breaches started with an internal human or system error in 2021, these occurrences can still pose a major risk to your organization. Data compromised by internal human error tends to go unnoticed for longer periods.

Last year, it more than took twice as long to detect and contain internal errors as external cyberattacks. On average, the lifecycle of data exposures and breaches induced by insiders took 207 days to detect and contain, whereas external attacks had an average lifecycle of 75 days.

Once again, healthcare topped the list for industries where internal actors contributed to widespread sensitive data exposure through human error. Personal health information and Social Security numbers were each exposed in 48% of all sensitive data incidents involving inside actors. Email and password credentials were revealed in 17% of insider incidents while driver licenses were exposed 12% of the time.

MOST COMMON SENSITIVE DATA EXPOSED BY COMPANY INSIDERS IN 2021



Source: Identity Theft Resource Center notified database January 1-December 31, 2021

Beyond healthcare, industries like financial services, technology, and government also experienced sensitive data loss from insider errors. As these industries continue to expand cloud-based storage, misconfigurations are likely to lead to more data loss in 2022.

Protecting your organization from cyber threats

Cyberattacks aren't new; as companies experience a growing volume of data, sensitive data exposure is a constant risk organizations must defend against. However, 2021 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 your organization's purview.

Complacency with cybersecurity poses a critical risk to any modern organization. As data privacy obligations evolve and new privacy laws are passed and come into strict enforcement, organizations must stay vigilant to remain compliant. Otherwise, compliance failures like non-reporting or underreporting breaches can present huge financial consequences and damage your organization's reputation with customers, partners, and employees.

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 remain compliant see much lower breach costs, with a breach costing a compliant organization $2.3 million on average versus $5.65 million for non-compliant organizations.[46]

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 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

Organization	Supply Chain Attacks	Ransomware Attacks	Insider Errors
Professional Services	Healthcare	Healthcare	Healthcare
Telecommunications	Education	Manufacturing	Financial Services
Healthcare	Financial Services	Professional Services	Education
Retail	Retail	Financial Services	Government
Financial Services	Non-profit	Education	Technology

Source: Identity Theft Resource Center notified database January 1-December 31, 2021

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 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.

Overall, reducing your data footprint is one of the single most effective ways to lower your data exposure risk. 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. The data now indicates that organizations must prepare for "how often" they'll suffer an incident. 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.

Organizations are more at risk than ever of experiencing multiple breaches in a short period of time. For example, even though life insurance company Aetna endured three data breaches back in 2017, the organization was recently charged a $1M fine for those HIPAA violations by the Office for Human Rights with the U.S. Department of Health and Human Services.[47] Unfortunately, the organization suffered three separate malware-related breaches again last February, May and July.

Other organizations like Humana experienced multiple data breaches in 2021 due to internal error and external third-party attacks. In March, Humana vendor Cotiviti endured a human error data exposure when an employee exposed data during a training event, revealing the personal information of 65,000 health plan members.[48] Not long after, Humana vendor PracticeMax experienced a ransomware attack, which exposed the personal data and billing information for 4,000 Humana customers.[49]

As third-party incidents become more common, the likelihood organizations will experience multiple data breaches within a year will continue to grow. 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.

Security AI and automation play a major role in reducing your data footprint by simplifying data discovery, classification, and remediation. Now that 69% of executives believe their organization would be unable to fight cyberattacks without the help of AI, it's clear that executives are seeing the benefit of these tools, making buy-in for this effective line of defense easier than ever.[50]

IBM found that companies with fully deployed security automation spent an average of $2.9 million on a breach in 2021, while companies without AI support spent an average of $6.71 million.[51]

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. Technical debt is common after an implementation or project, but without the right tools, it can be difficult to discover where coding errors and security concerns continue to linger months after a launch. These gaps can unintentionally expose data and continue to go unnoticed, making the ability to quickly detect a breach even more challenging.

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, many companies don't know what data they're holding on to, making remediating a breach and compliance reporting much more challenging.[52]

Classifying and cataloging the sensitive data across your organization is critical to maintain 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. Inconsistent data management often leads to miscategorization, causing further confusion when a breach occurs. By setting boundaries around data use, access, and modification, you can keep a watchful eye on your company's sensitive information.

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 limiting 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 your company's sensitive data automatically.

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 of your company's 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 your company's 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, your teams 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 Scroxton, Alex. "More data stolen in January 2021 than in all of 2017, says report." Computer Weekly. May 26, 2021.
3 Lostri, Eugenia & Malekos Smith, Zhanna. "The Hidden Costs of Cybercrime." McAfee. 2020.
4 "Cost of a Data Breach Report 2021." IBM. July 2021.
5 Includes data for sensitive and non-sensitive data incidents
6 "Cost of a Data Breach Report 2021." IBM. July 2021.
7 See Table 1.
8 "2021 Thales Data Threat Report: Data Security in the Era of Accelerated Cloud Transformation and Remote Work." Thales. June 2021.
9 "Cloud Trends in 2021 and Beyond: Remote Work Drives Adoption." Spiceworks Ziff Davis. March 2021.
10 Zandt, Florian. "The Industries Most Affected by Ransomware." Statista. November 9, 2021.
11 Morgan, Steve. "Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021." Cybercrime Magazine. October 21, 2019.
12 Scroxton, Alex. "More data stolen in January 2021 than in all of 2017, says report." Computer Weekly. May 26, 2021.
13 "GDPR Fines Exceed $1.1B in Q3." PYMNTS.com. October 4, 2021.
14 "The lucrative cost of cybercrime of PII." Spirion. December 15, 2021.
15 "Cost of a Data Breach Report 2021." IBM. July 2021.
16 ibid
17 ibid
18 "Accellion Data Breach Involving Sensitive Information Impacts Multiple Entities." ITRC. March 17, 2021.
19 Alder, Steve. "PHI of More Than 420,000 Individuals Potentially Compromised in Ransomware Attack on Ohio Law Firm." HIPPA Journal. April 9, 2021.
20 "Notice of Data Breach: Keeping you safe from cybersecurity threats." T-Mobile. October 15, 2021.
21 Alleven, Monica. "Syniverse quietly reveals 5-year data breach." Fierce Wireless. October 5, 2021.
22 "20/20 Eye Care Network and Hearing Care Network notify 3,253,822 health plan members of breach that deleted contents of AWS buckets." Databreaches.net. June 1, 2021.
23 Jercich, Kat. "Forefront Dermatology reports breach of 2.4M patient records." Healthcare IT News. July 20, 2021.
24 Greig, Jonathan. "DNA testing center admits to breach affecting SSNs, banking info of more than 2 million people." ZDNet. November 30, 2021.
25 Cost of a Data Breach Report 2021." IBM. July 2021.
26 Jercich, Kat. "Nevada hospital ransomware attack could affect data of 1.3M patients." Healthcare IT News. August 23, 2021.
27 "1.4 Million Individuals Affected by St. Joseph's/Candler Ransomware Attack." HIPAA Breach News. August 19, 2021.
28 ""2021 Thales Data Threat Report: Data Security in the Era of Accelerated Cloud Transformation and Remote Work." Thales. 2021.
29 Unglesbee, Ben. "Neiman Marcus warns 4.6M customers about data breach." Retail Dive. October 1, 2021.
30 Shepardson, David. "VW says data breach at vendor impacted 3.3 million people in North America." Reuters. June 11, 2021.
31 Reindl, JC. "Flagstar Bank gives customers 2 years of ID-monitoring services after information breach." Detroit Free Press. March 24, 2021.
32 Whittaker, Zack. "Robinhood says millions of customer names and email addresses taken in data breach." TechCrunch. November 9, 2021.
33 Muncaster, Phil. "Misconfigured Database Leaks 880 Million Medical Records." Infosecurity Magazine. October 29,2021.
34 Page, Carly. "US education software company exposed personal data on 1.2M students." TechCrunch. November 22, 2021.
35 Drees, Jackie. "Class action targets CaptureRx over breach that exposed 2.4M+ patients' data." Becker's Health IT. July 22, 2021.
36 Diaz, Ariel. "2020 Annual SaaS Trends." Blissfully. October 23, 2019.
37 Panettieri, Joe. "Kaseya REvil Ransomware Cyberattack: Hacker Charged." MSSP Alert. November 8, 2021.
38 "Information Risk Insights Study (IRIS) Tsunami: Following the wake of damage from major multi-party cyber incidents." Cyentia. 2021.
39 "The Cost of Third-Party Cybersecurity Risk Management." CyberGRX and Ponemon Institute LLC. March 2019.
40 "Cost of a Data Breach Report 2021." IBM. July 2021.
41 C, Ruth. "Ransomware accounts for 81% of all financially motivated cyberattacks in 2020." atlasVPN. January 21, 2021.
42 "Cloudian Ransomware Survey Finds 65% of Victims Penetrated by Phishing Had Conducted Anti-Phishing Training." Cloudian. July 15, 2021.
43 ibid.
44 IBM Security Services 2014 Cyber Security Intelligence Index." IBM Global Technology Services. 2014.
45 In The Dark: Why Enterprise Blind Spots Are Leaving Sensitive Data Vulnerable to Breaches." CloudSphere. 2021.
46 "Cost of a Data Breach Report 2021." IBM. July 2021.
47 "Aetna Pays $1,000,000 to Settle Three HIPAA Breaches." U.S. Department of Health and Human Services. October 28, 2020.
48 "Humana notifies members about data security breach incident." WILX News 10. March 5, 2021.
49 McKeon, Jill. "Third-Party Vendor Ransomware Attack Impacts Humana, Anthem Members." Health IT Security. October 27, 2021. .
50 "Reinventing Cybersecurity with Artificial Intelligence: The new frontier in digital security." Capgemini Research Institute. 2019..
51 "Cost of a Data Breach Report 2021." IBM. July 2021.
52 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