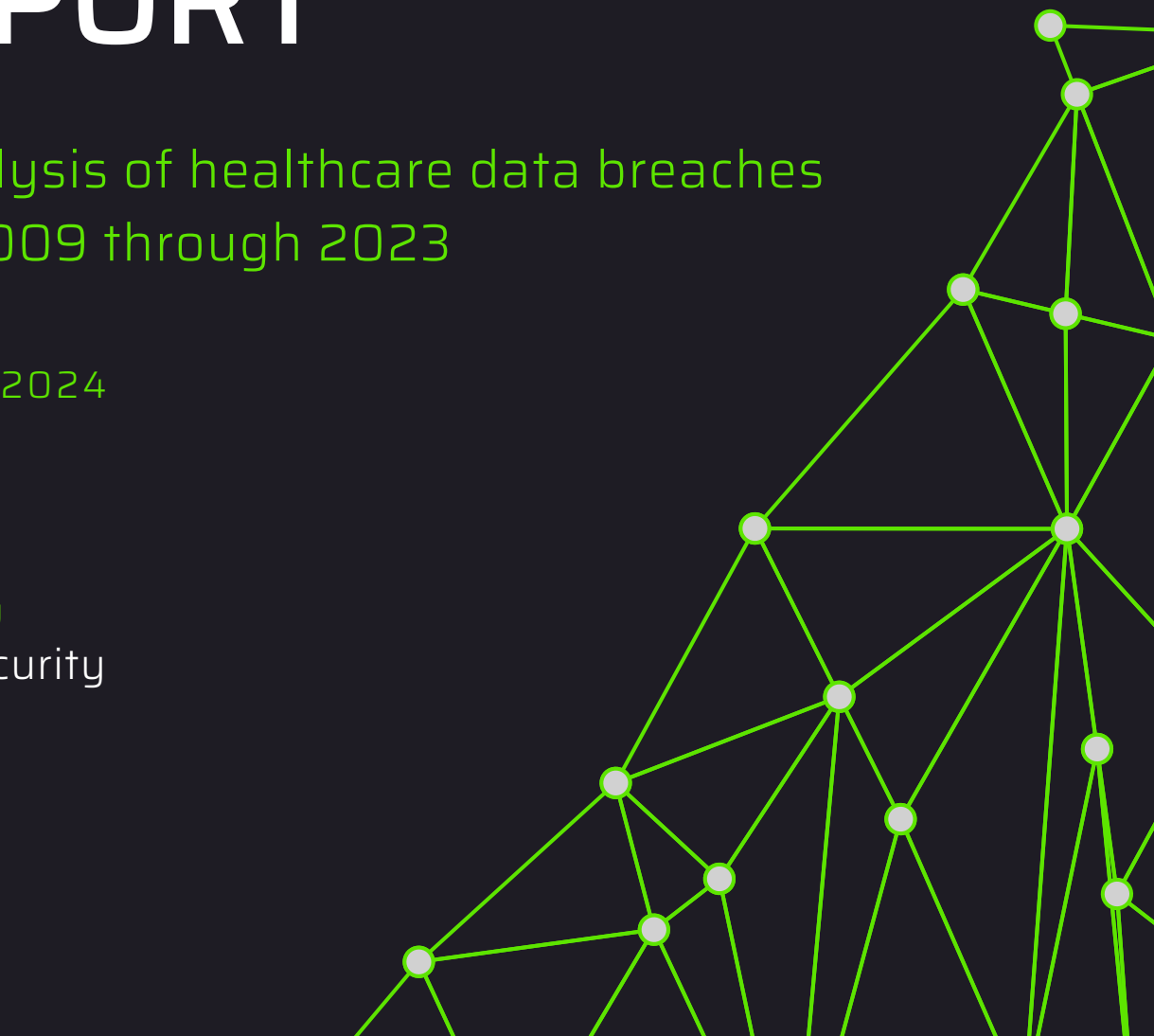
velocity™
By Stern Security

2024 VELOCITY HEALTHCARE DATA BREACH REPORT

An analysis of healthcare data breaches from 2009 through 2023

AUGUST 2024



Prepared by
Stern Security

Table of Contents

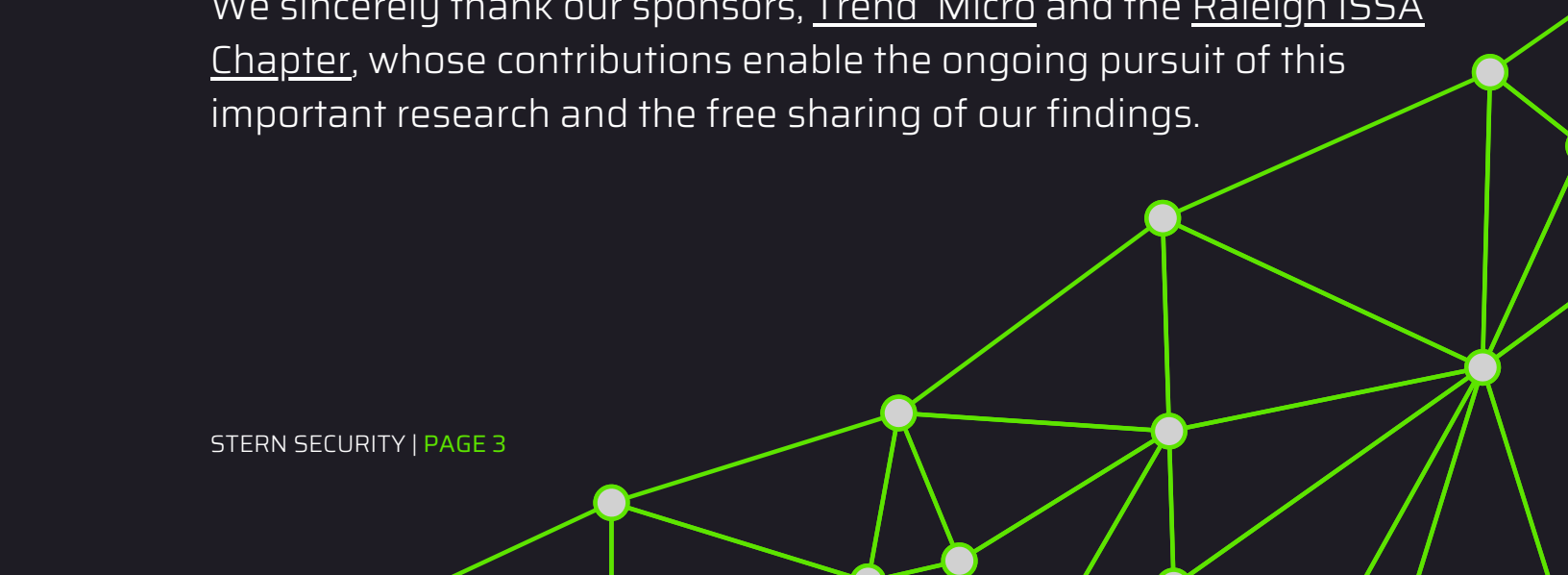
Background

Over 5,900 Healthcare Breaches Analyzed

In its third annual healthcare data breach report, Stern Security has critically analyzed over 5,900 data breaches since the Department of Health and Human Services (HHS) began tracking the information in 2009. Stern Security utilized data from their HealthcareBreaches.com website as well as published information from HHS to create this comprehensive study. Stern Security augmented the HHS data by investigating each breach in 2023 to fully understand the cause of the incident.

This report shows critical insights into healthcare breach trends over the past 14 years. It covers everything from the number of breaches attributed to ransomware to the number attributed to third-parties (business associates). This year, Stern Security has added a new breach categorization – the number of breaches due to the MOVEit file transfer software vulnerability. Once again, a new breach record was established with more healthcare breaches occurring in 2023 than any previous year. This report puts forth a detailed analysis.

We sincerely thank our sponsors, Trend Micro and the Raleigh ISSA Chapter, whose contributions enable the ongoing pursuit of this important research and the free sharing of our findings.



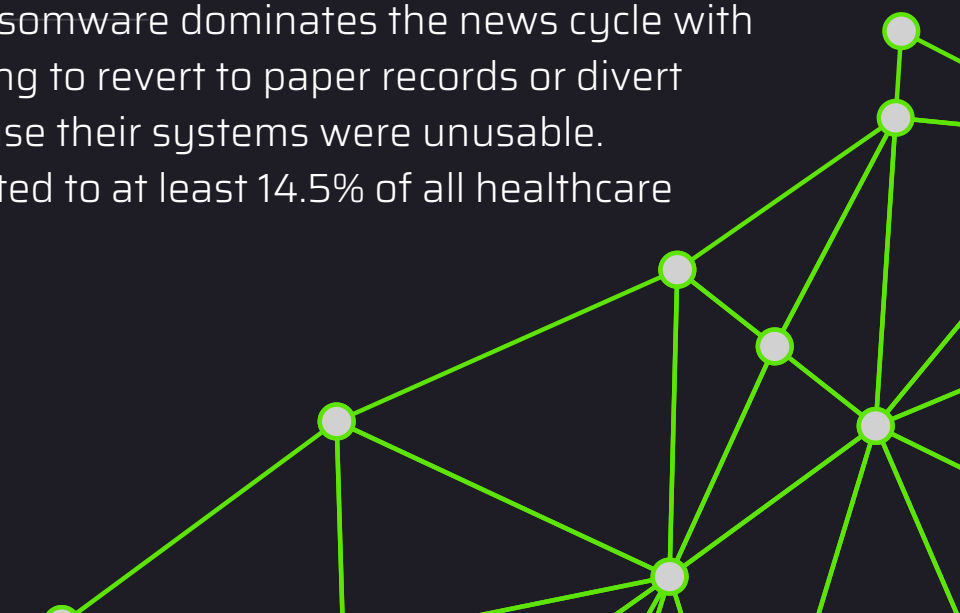
Executive Summary

Over time, cyber-attacks have transitioned from minor nuisances to significant threats against the critical infrastructure. The healthcare industry has been particularly hit hard with 5,904 publicly reported breaches occurring from 10/21/2009 through 12/31/2023. Within those breaches, 555,514,004 Protected Health Information (PHI) records were lost. In 2023 alone, there were 744 reported healthcare breaches with 160,007,574 PHI records lost - both amounts breaking yearly records.

555,514,004

Number of PHI records lost from 10/21/2009 to 12/31/2023

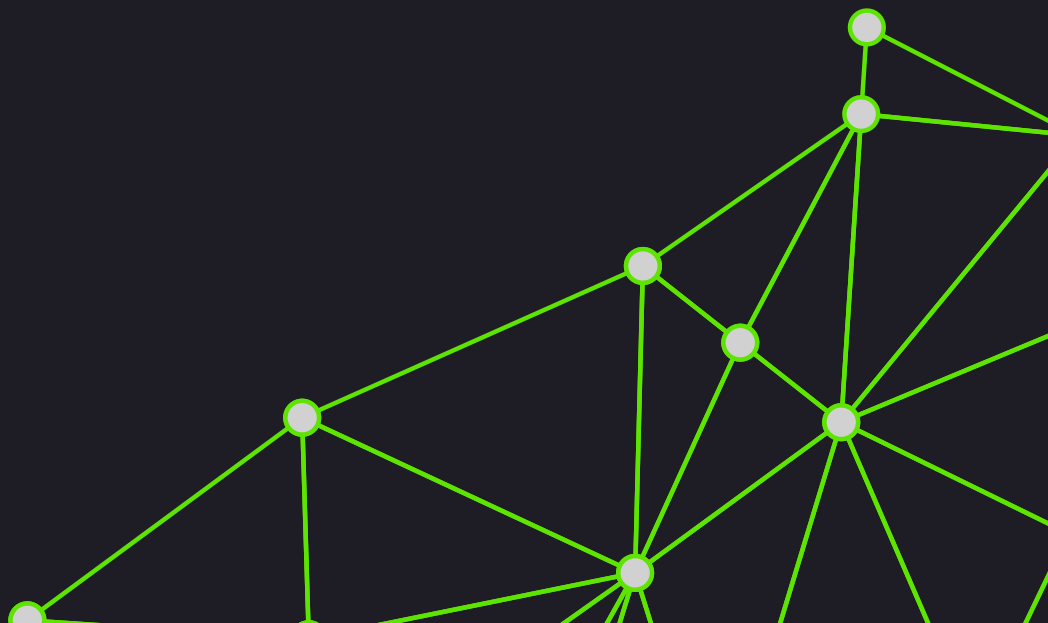
While there are various forms of breaches such as physical theft and unauthorized access of a patient record, there is no surprise that hacking is the top threat. In 2023, 80.8% of healthcare breaches and 94.7% of PHI records lost were due to hacking. Within the hacking category, ransomware dominates the news cycle with stories of hospitals needing to revert to paper records or divert patients elsewhere because their systems were unusable. Ransomware was attributed to at least 14.5% of all healthcare breaches last year.



Progress Software's MOVEit file transfer application made a large impact on the world with the discovery of a massive zero-day vulnerability that intruders exploited. In total, 42 healthcare breaches and over 25% of the Protected Health Information (PHI) exposed were due to the MOVEit vulnerability in 2023.

Most companies rely on third parties (business associates) for essential functionality and services. Unfortunately, business associates continue to have a significant impact on breaches. In 2023 business associates accounted for 37.4% of the healthcare breaches. Business associates were also responsible for 69% of the PHI records lost (110,808,894) which is the highest amount of records exposed by third-parties in any year on record.

Long term trend lines point to a continued increase in the rate of healthcare breaches with hacking leading the surge, and ransomware and third-party sources having the greatest impact.



Findings

Summary

The United States Department of Health and Human Services (HHS) published its first healthcare breach notification on October 21st, 2009. It must be noted that all of the breaches published by HHS contain 500 or more Protected Health Information (PHI) records lost so the data within this report fit the same criteria.

5,904

Number of healthcare breaches from 10/21/2009 - 12/31/2023

In 2023, there were 744 healthcare breaches. These breaches caused a loss of 160,007,574 PHI records earning the title of most records lost in a single year.

160,007,574

HEALTHCARE RECORDS LOST IN 2023

MORE HEALTHCARE RECORDS WERE LOST IN 2023 THAN ANY OTHER YEAR

744

HEALTHCARE BREACHES IN 2023

Initially Underreported Breaches

The total number of breached PHI records is often much greater than the initial reported amount.

Healthcare organizations must report within 60 days any breach with over 499 PHI records lost. However, the exact number is often initially underestimated. For example, in one breach notification, a cancer and diabetes treatment center initially reported a breach of 501 records to HHS, but later updated this to 902,540 records lost. The initial 501 records reported to HHS was most likely a placeholder until the actual number was determined.

At least 24 reported breaches were updated at a later time to reflect a more accurate number of affected individuals amounts. In one case, the number of affected individuals decreased slightly, but the number of compromised records increased in all other reviewed cases.

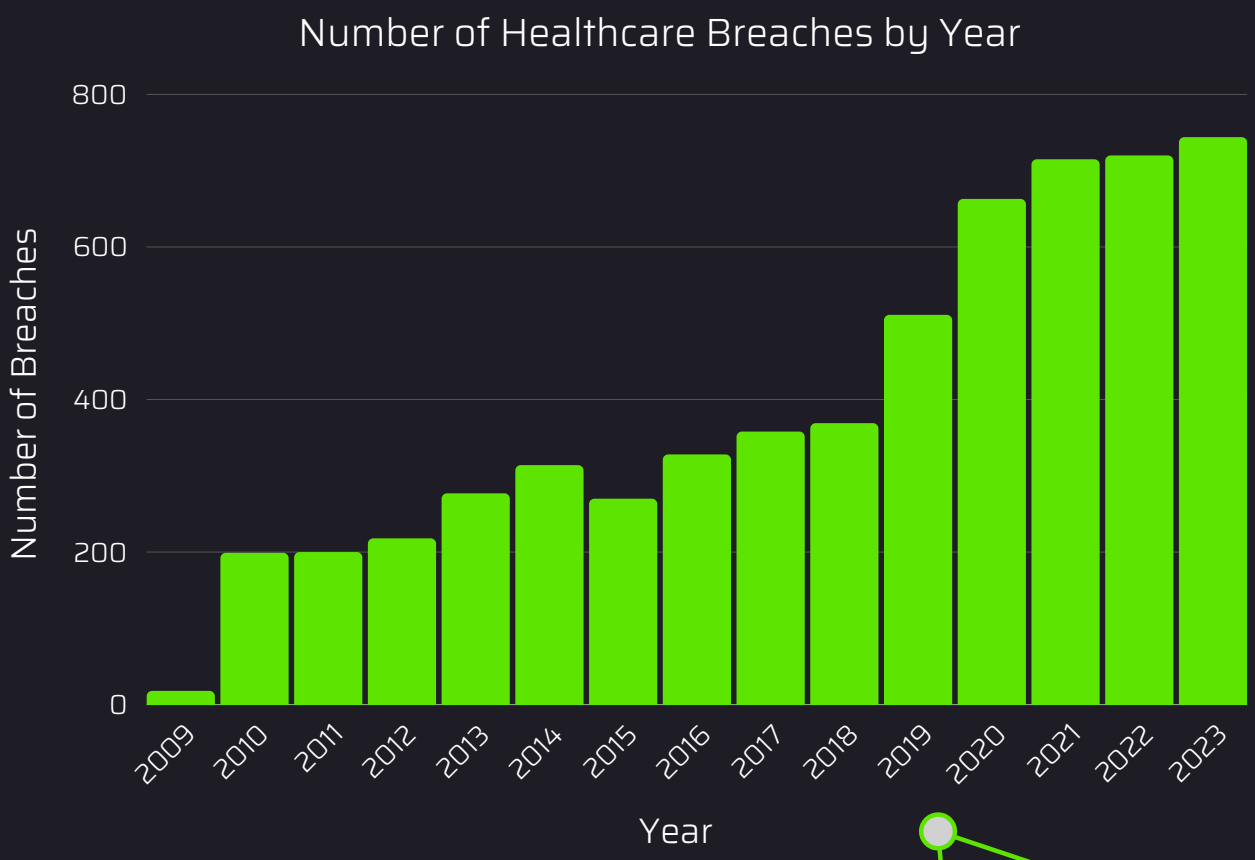
For the most up to date information on healthcare breaches, visit https://www.healthcarebreaches.com.

Breach Trends

From 2010* through 2023, healthcare breaches climbed almost every year. During the last six years, the average number of breaches has increased by 75 per year.

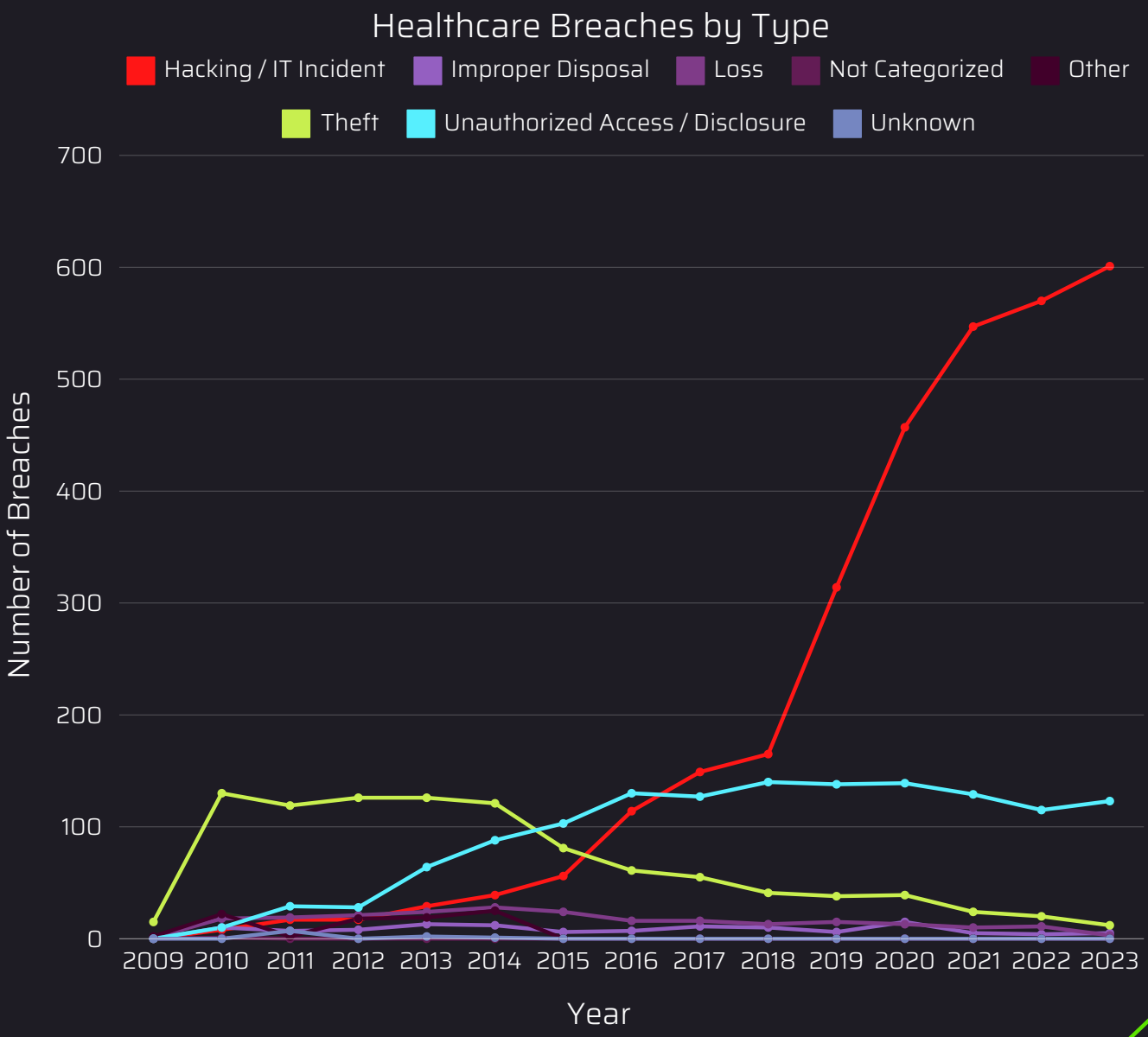
While the number of breaches has not drastically changed from 2021 to 2023, during the past five years there was a 45.6% total increase in breaches.The 744 breaches in 2023 was the largest number of breaches recorded in a single year.

*2009 is not included as it was a partial year total.



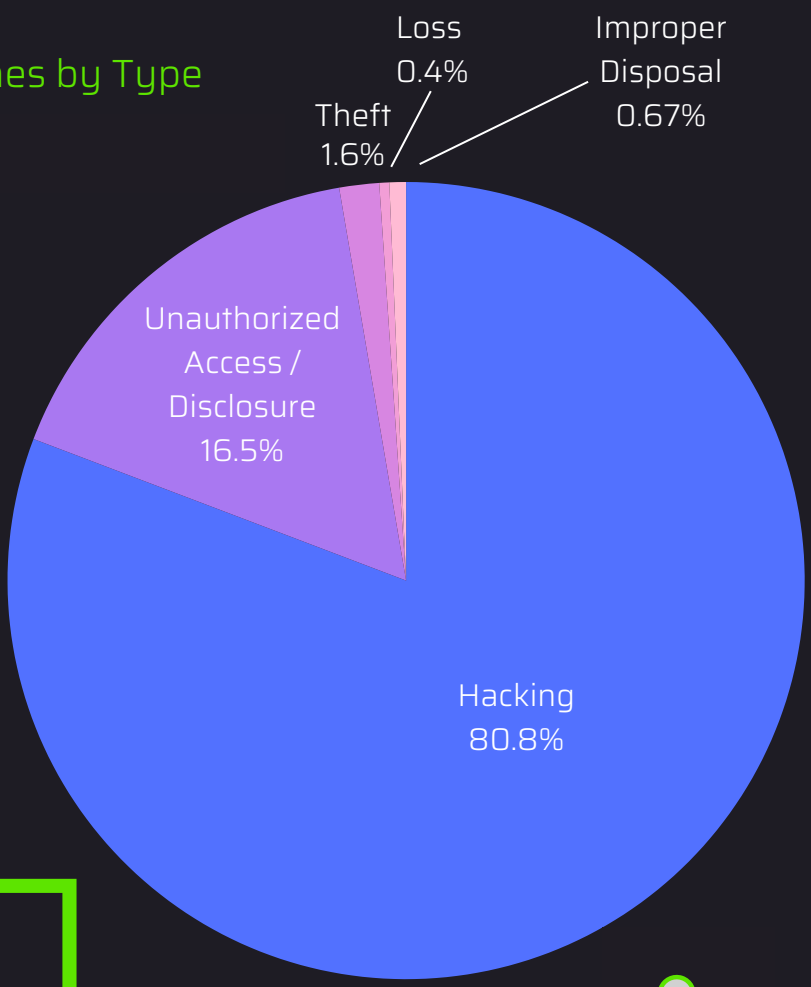
Breach Categories

Healthcare breaches are divided into different categories depending on how the breach occurred. The primary categories are Hacking, Theft (physical), and Unauthorized Access/Disclosure. Examples of Unauthorized Access/Disclosure include patient records sent to the incorrect patient, inadvertently published PHI, and healthcare workers accessing data that they were not authorized to do so. While there are multiple types of data breaches, hacking is the most prevalent and this is clearly visible in the graphs.



In 2023, 80.8% of healthcare breaches and 94.7% of PHI records lost were due to hacking. The number of breaches due to "Unauthorized Access/Disclosure" came in at a distant second place, but still had a visible impact on breach counts.

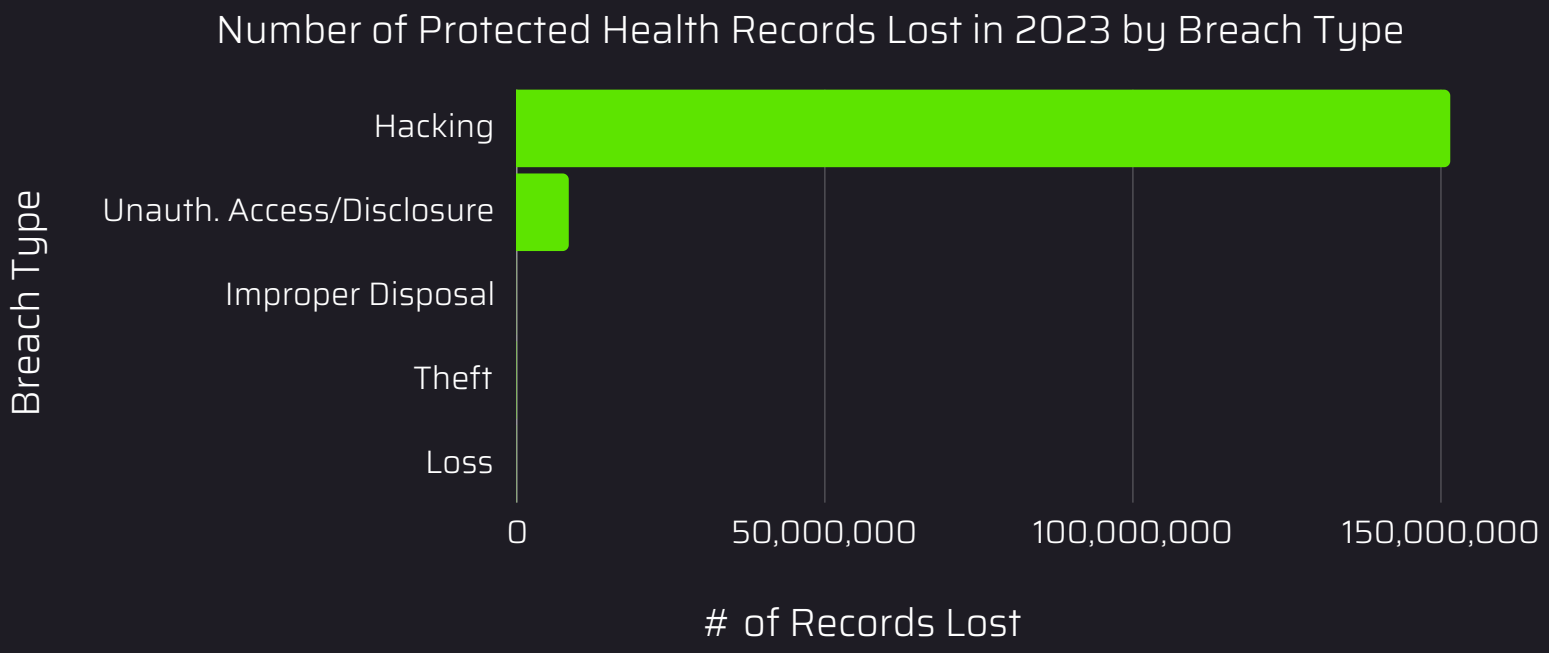
2023 Healthcare Breaches by Type



81%

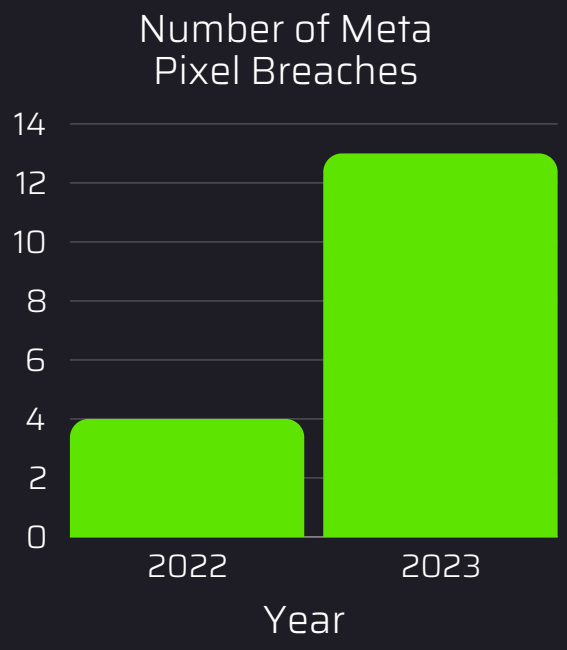
BREACHES DUE TO HACKING

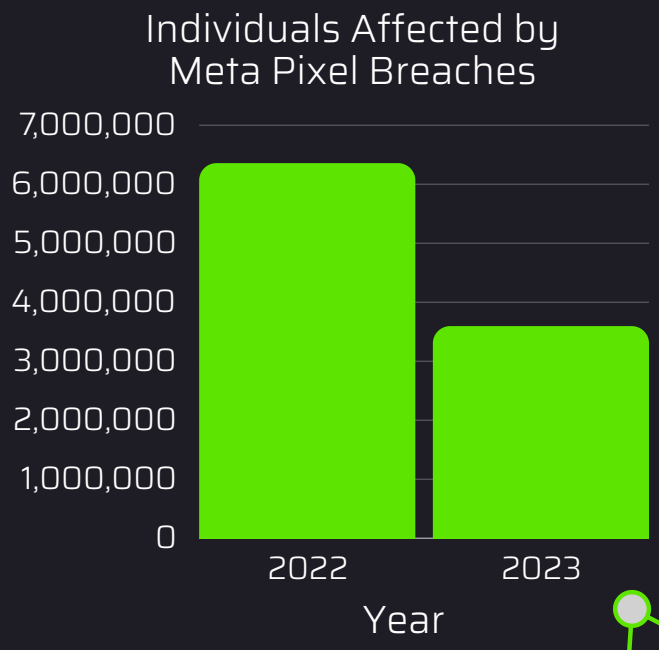
Not surprising, most of the PHI records lost in 2023 were due to hacking. During the year, 151,514,089 PHI records were lost due to hacking alone. To put this in perspective, the PHI lost due to hacking in 2023 is roughly equivalent to 45% of the population of the United States. Unauthorized Access/Disclosure claimed the second spot for records lost by breach type with 8,436,940 individuals affected. The next breach types had tens of thousands of records lost which are figures completely dwarfed by hacking.



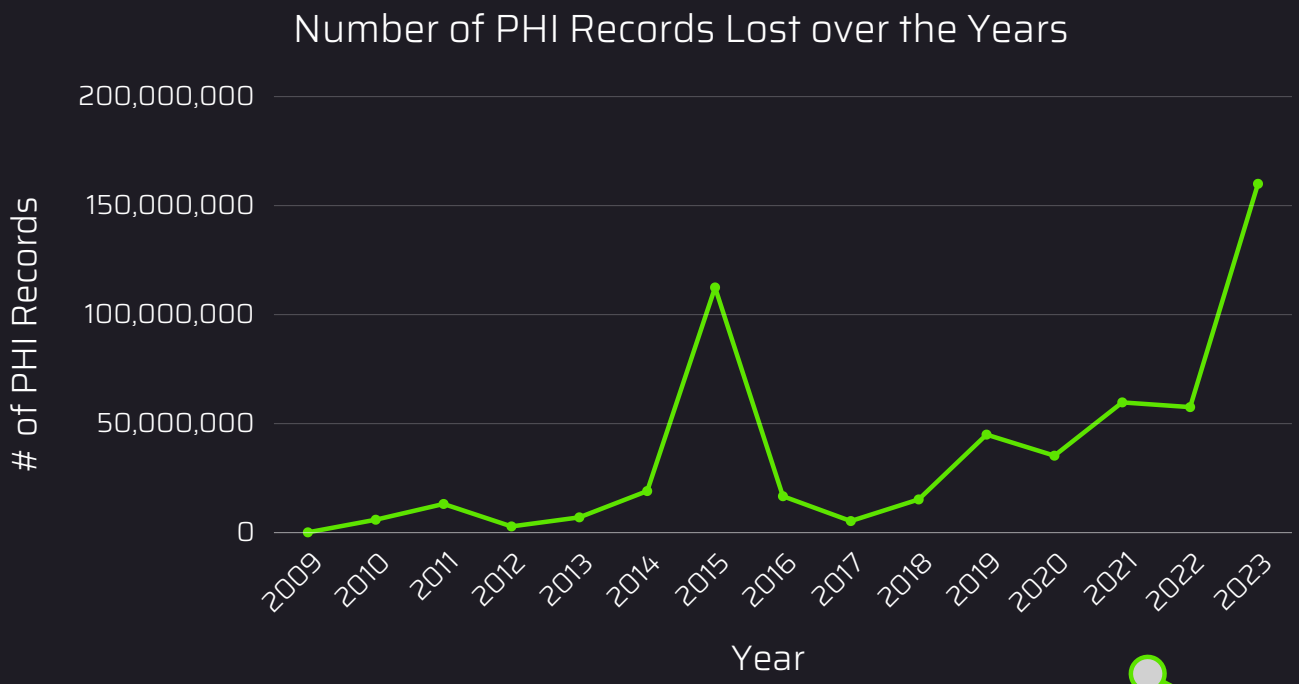
Stern Security researched all of the breaches that occurred in 2023 to gain more insight into how the breaches occurred. Among types of hacking incidents, ransomware remains a dominant threat as at least 14.5% (or 108 breaches) of all healthcare breaches in 2023 were known due to ransomware. Within these 108 ransomware incidents, 37,916,806 patient records were exposed. Phishing was the cause of at least 38 breaches.

Last year, the Facebook Meta Pixel breaches were a major story. These breaches occurred as multiple hospitals utilized the software to track visitor usage within their patient portals. Unfortunately, Facebook was not only collecting visitor statistics, but also PHI. While the number of documented Meta Pixel breaches increased in 2023 to 13 incidents (from 4), the number of individuals affected decreased to 3,595,926 from 6,358,104 the previous year.



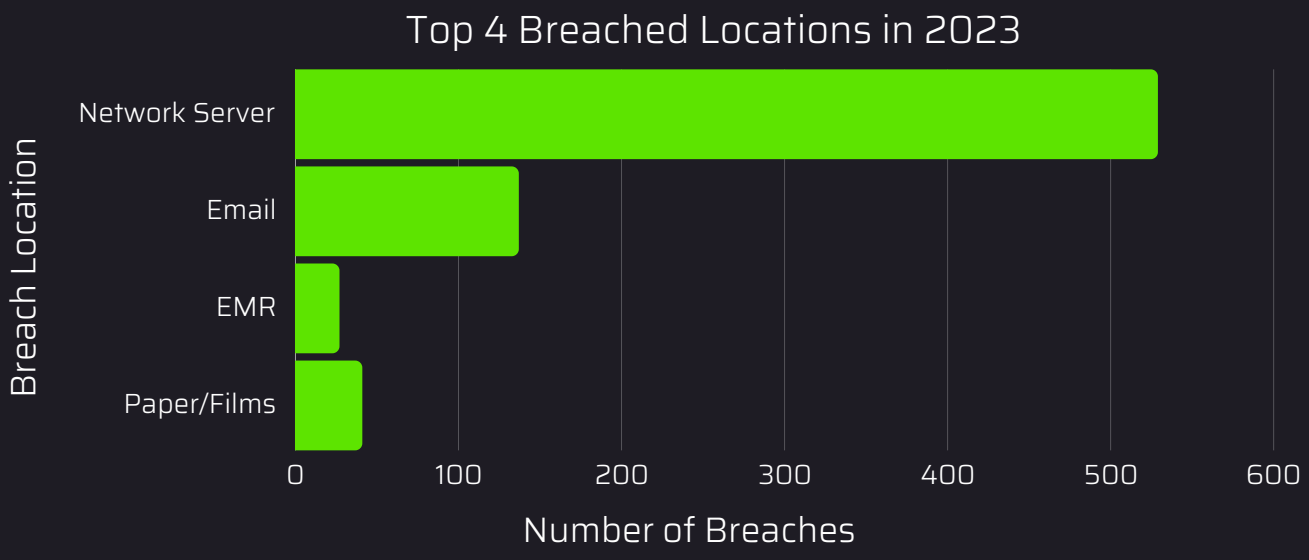


There were more individuals affected by healthcare breaches in 2023 than any other year on record. This title was previously held by the year 2015. In 2023, there were 160,007,574 patient records lost. Not only did 2023 have more breaches than any other year on record, but the breaches were larger. In 2015, the year with the second number of records lost, there were six breaches with more than 1 million patient records lost. Most records were exposed in 2015 by a massive single event (Anthem Inc. breach). However, in 2023, there were 30 breaches with more than 1 million patient records lost! There was a 177.9% increase in records lost in 2023 over the previous year.



Breach Location

The Department of Health and Human Services (HHS) tracks the type of system that the breach occurred. The top four sources included Network Server, Email, Electronic Medical Record (EMR), and Paper/Films. It must be noted that some breaches involved multiple device types.



14.5%

Healthcare breaches caused by ransomware in 2023

MOVEit Breaches

One exploit can make a large impact on an industry, and in 2023, this exploit involved the popular MOVEit software. MOVEit is a file transfer application created by Progress Software and is offered in either an on-premise or cloud-hosted environment. Many companies utilize this software to transfer confidential data. These file transfer systems are usually externally accessible, but access is limited to authorized accounts.

1. **5/27/2023**
   Evidence of first exploits
2. **5/31/2023**
   Vulnerability announced and Patch Released
3. **6/5/2023**
   ClOp ransomware group claims responsibility
4. **6/11/2023**
   First healthcare breach due to MOVEit exploit

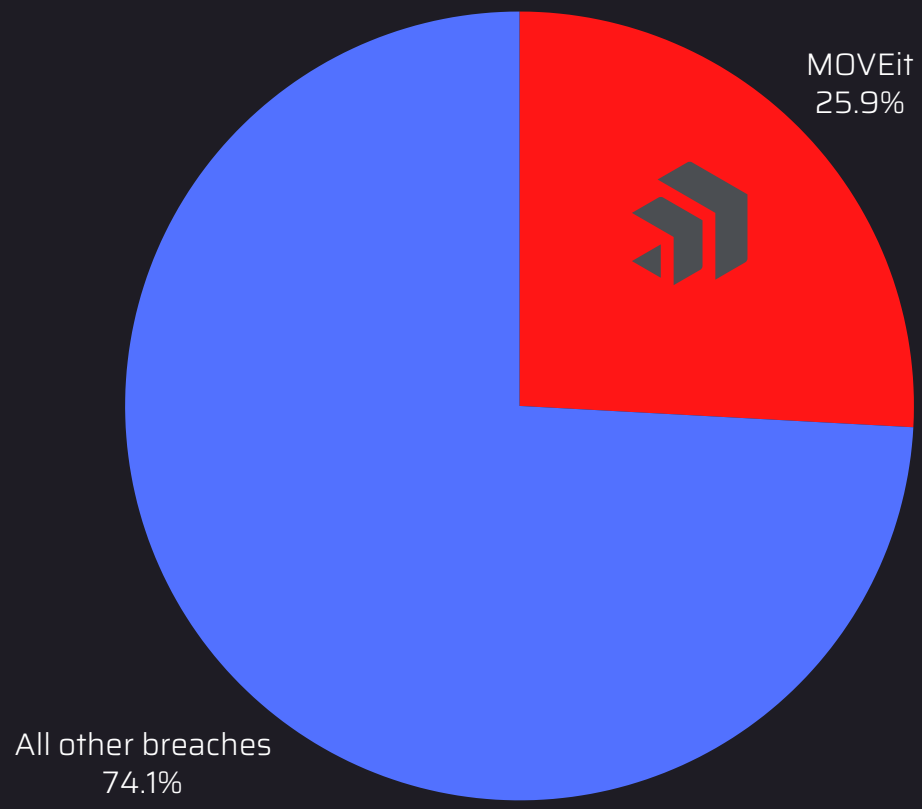
On May 31st, 2023, Progress Software announced a critical "zero-day" SQL injection vulnerability (CVE-2023-23397) in their MOVEit application which enabled unauthorized access for intruders. The vulnerability had a CVSS score of 9.8. Although Progress Software released a patch on May 31st, 2023, security researchers discovered evidence of successful exploits dating back to at least May 27th, 2023. On June 5th, 2023, the CLOp ransomware group claimed responsibly for the exploit. The first healthcare breach due to the MOVEit exploit was reported on June 11th, 2023 and others continued throughout the year.

26%

PHI records breached in 2023 due to the MOVEit exploit

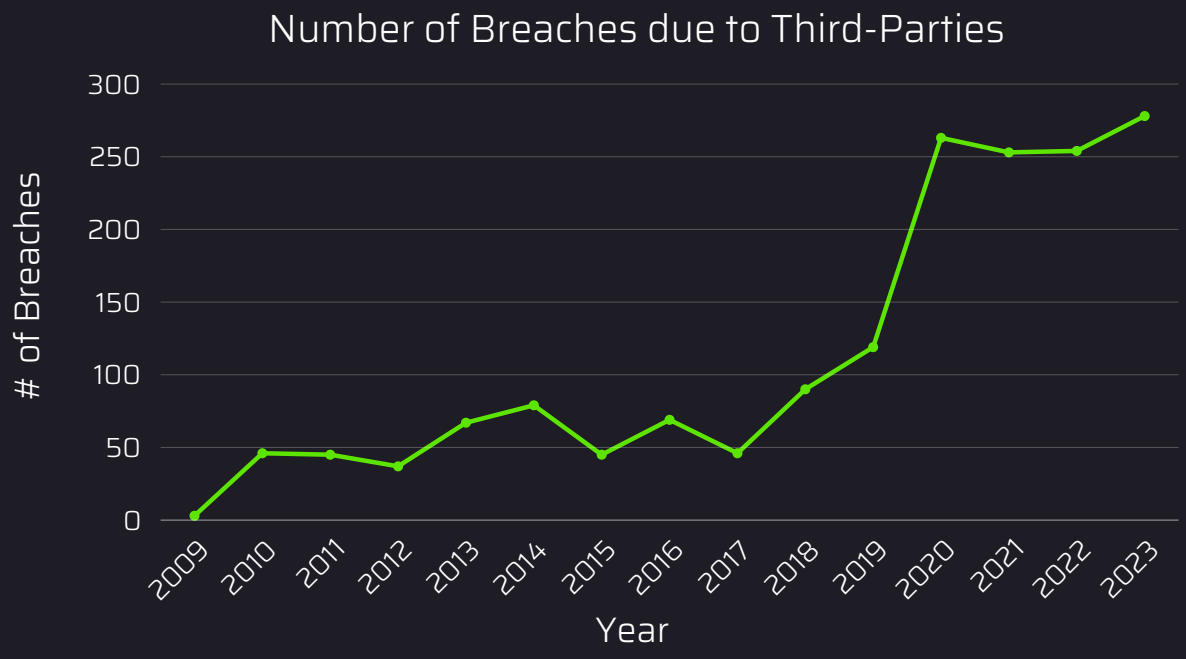
In total, 42 healthcare breaches in 2023 were attributed to the MOVEit vulnerability. This resulted in the exposure of 41,380,105 protected health information (PHI) records. Out of all of the PHI breached in 2023, 25.86% were due to the MOVEit vulnerability. While 2023 had more healthcare breaches than any other year on record, without the MOVEit vulnerability, 2023 would have dropped down to third place for the number of breaches in a year.

Percentage of PHI Records Lost in 2023 due to MOVEit



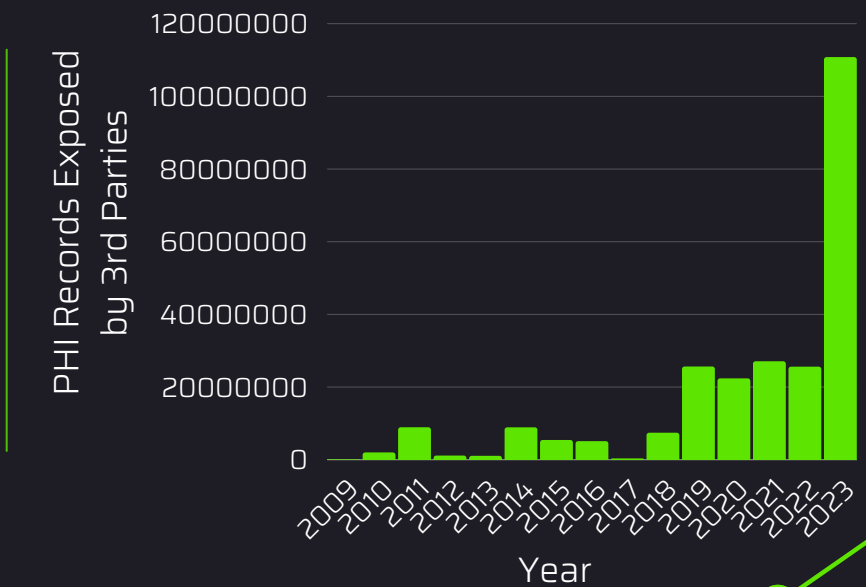
Third-Party Breaches

Third-parties, referred to as “Business Associates” in healthcare, have had a significant impact on breaches. In 2023, while third-parties were responsible for 37.4% of the healthcare breaches, they were responsible for most (69%) of the records lost. So not only were third-party breaches responsible for most of the records exposed, but these breaches tended to be larger than breaches that did not have third-parties involved.



69%

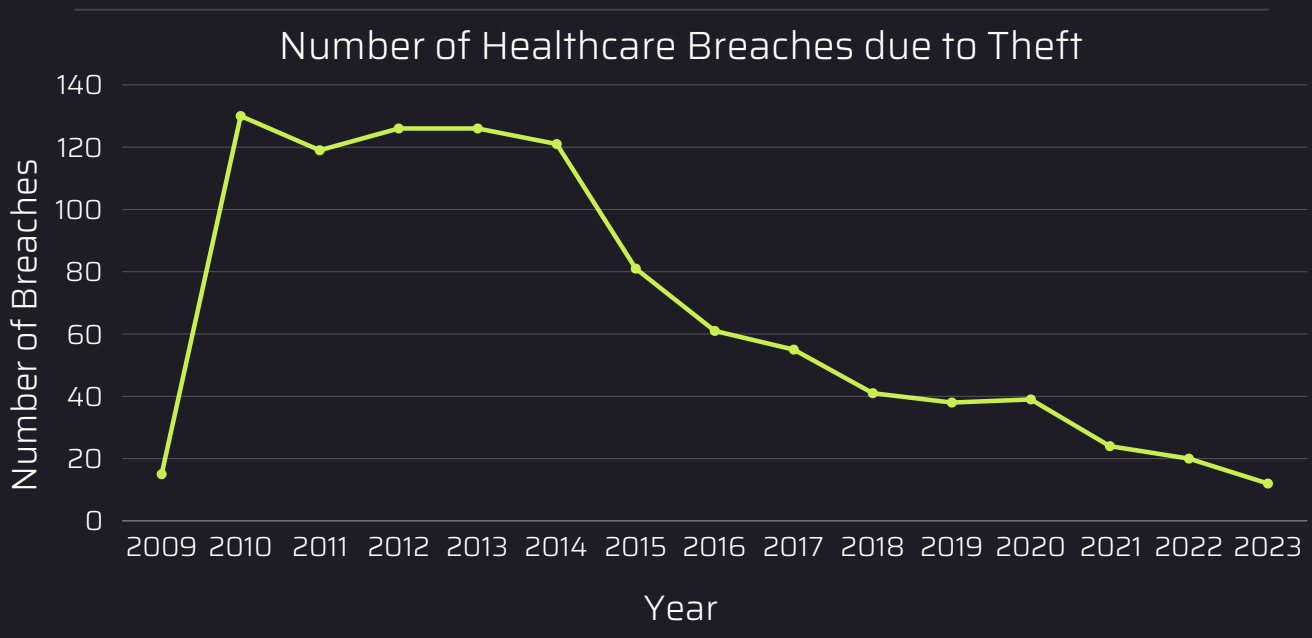
PHI RECORDS EXPOSED BY 3RD-PARTIES



Good News

While healthcare breaches and PHI records lost remain a serious concern which must be addressed, there is some good news:

Physical Theft Decline - Breaches due to physical theft have been on a steady decline. Examples include stolen laptops and filing cabinets that contain PHI. This decline could be because of an increased use of full disk encryption on devices combined with less use of paper records.



Good Breach News

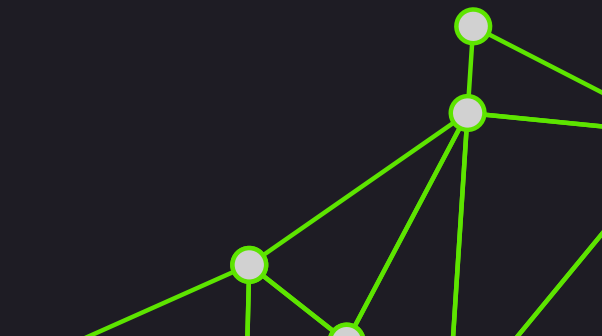
Healthcare Breaches due to theft have been on a steady decline.

Solutions

All is far from lost and there are measures that organizations can do to improve their security and reduce risk:

1. Asset Management - One of the first steps to protecting an organization is simply knowing all of your systems. When a documented asset inventory is in place, then it is much easier to analyze, patch, and protect systems.
2. Patch Schedule - Critical vulnerabilities should be patched quickly, especially for publicly accessible systems. With respect to the MOVEit exploit, healthcare organizations were still announcing breaches many months after a patch was released. It is unclear whether this lengthy timeline is because of the time it took to patch the vulnerability, or the time to discover a compromise.
3. Minimize Data - If possible, organizations should minimize the data that is requested and stored. Breaches are growing in size and one way to combat larger breaches is to reduce the amount of data stored. For example, if an organizations don't need a particular data field such as social security number, then they shouldn't collect it. If data is no longer being used then encrypt and archive it, or securely dispose if archival is not required or if archival time has expired. In the case of publicly accessible file transfer systems like MOVEit, once data is transferred, remove it from the system if no longer needed.
4. Limit Access to Systems - External file transfer systems like MOVEit may not always need to be open to the entire internet. Try implementing an "allow-list" process instead of a "deny-list" to only allow access to authorized sources and destinations.

5. Third-Party Risk Management - Business Associates were responsible for most of the PHI exposed in 2023. It is essential to perform security due diligence reviews on third-parties in addition to having them sign Business Associates Agreements before commencing work. Also limit the amount of data shared to the minimum necessary to complete the task.
6. Risk Analysis - The HIPAA Security Rule requires covered entities and business associates to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI). This process is referred to as a "Risk Analysis." A penetration test should be conducted as part of this process.



Conclusion

Several healthcare breach records were broken in 2023 including the most records lost by business associates and total breaches. The MOVEit zero-day vulnerability had a major impact on the healthcare industry as over 25% of the PHI exposed was due to this issue.

On a positive note, healthcare breaches due to physical theft continues to decline. Additionally, there are numerous solutions for decreasing risk including, but not limited to, asset management, minimizing data, limiting access, patch management, third-party risk management, and completing an accurate and thorough risk analysis.

Resources

Health and Human Services (HHS) publishes a list of breaches of Protected Health Information (PHI) affecting 500 or more individuals per section 13402(3)(4) of the HITECH Act. Stern Security utilized the information posted by HHS combined with our own research into the listed breaches to create both HealthcareBreaches.com and this 2024 Healthcare Breach Report.

Company

Stern Security is a leading cybersecurity company and the creator of the HealthcareBreaches.com Executive Dashboard.

Stern Security developed the cyber risk quantification SaaS platform Velocity (https://www.sternsecurity.com/velocity/). Based on the most accurate internal and third-party risk information, Velocity creates actionable plans to help organizations reduce risk, increase security posture, select cybersecurity products, optimize costs, and show ROI.

Stern Security's services division conducts comprehensive penetration testing, threat emulation, and Virtual CISO (Chief Information Security Officer) engagements. Stern Security's vision is to "Secure the Planet" and we believe that every organization can reduce risk.

If you appreciated the report and would like to hear more about our products and services (or just want to say thank you), contact us!

Contact form: https://www.sternsecurity.com/contact/
LinkedIn: https://www.linkedin.com/company/sternsecurity
Twitter: https://twitter.com/stern_security
Instagram: https://www.instagram.com/sternsec/
Vimeo: https://vimeo.com/sternsecurity
Facebook: https://www.facebook.com/sternsec

Velocity Cybersecurity Risk Quantification Platform:
https://www.sternsecurity.com/velocity/

Stern Security

Sponsors

A very special thanks to our sponsors, whose support makes it possible to continue this valuable research and distribute the report freely. Our sponsors are helping in our vision to secure the planet!

Premium

Community

Works Cited

NIST. (2024, 08 14). CVE-2023-23397 Detail . Retrieved from NIST National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2023-23397

Rapid7. (2023, June 14). CVE-2023-34362: MOVEit Vulnerability Timeline of Events. Retrieved from Rapid7: https://www.rapid7.com/blog/post/2023/06/14/etr-cve-2023-34362-moveit-vulnerability-timeline-of-events/

U.S. Department of Health & Human Services. (2024, August 20). U.S. Department of Health and Human Services Office for Civil Rights. Retrieved from Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information : https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf