Securing Healthcare: 10 Years of U.S. Cyber Incident Insights and Defense Lessons

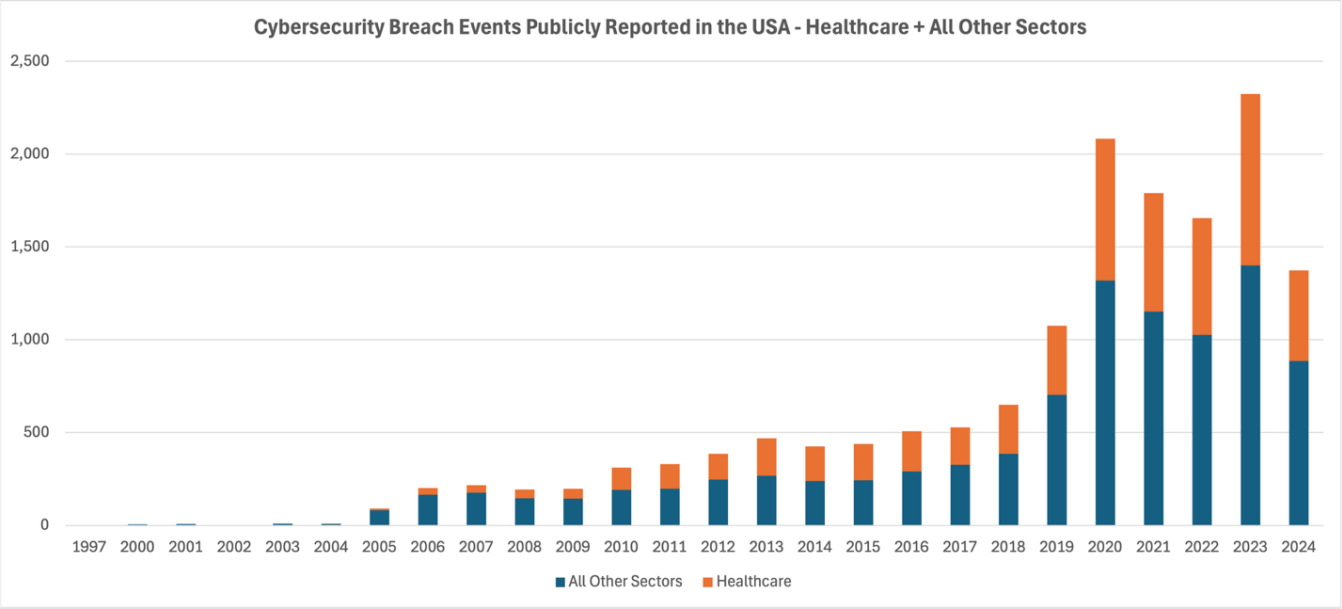
THOUGHT LEADERSHIP PAPER

JUNE 2025

Contents

Introduction

The earliest publicly reported information security breach event in the RiskRecon database dates to 1997 when a large US-based healthcare organization left several boxes of printed medical records by a dumpster during the process of vacating a facility. Since then, RiskRecon has cataloged 15,288 publicly reported breach events occurring in the United States through 2024. Of those 15,288 events, 37% were reported by healthcare organizations.



In this report we dive into the 4,692 breach events of US-based healthcare organizations that RiskRecon cataloged between January 2015 and December 2024. The data is based on RiskRecon's global monitoring of publicly reported breach events as a leading provider of cybersecurity ratings that are relied on by thousands of organizations worldwide to better manage the cybersecurity risks of their own organizations and that of their supply chain.

As individuals and as societies we have a vested interest in the safety and soundness of the healthcare sector. It is perhaps the one sector that if it isn't always immediately available that lives are really at risk. In striving to meet this expectation, healthcare faces unique challenges in its inherently large and complex operational and technology attack surface. While this report details the breach events of the US healthcare sector, it is by no means a criticism of its practices or performance. If anything, it is to raise awareness of the challenges and garner broader support for the industry.

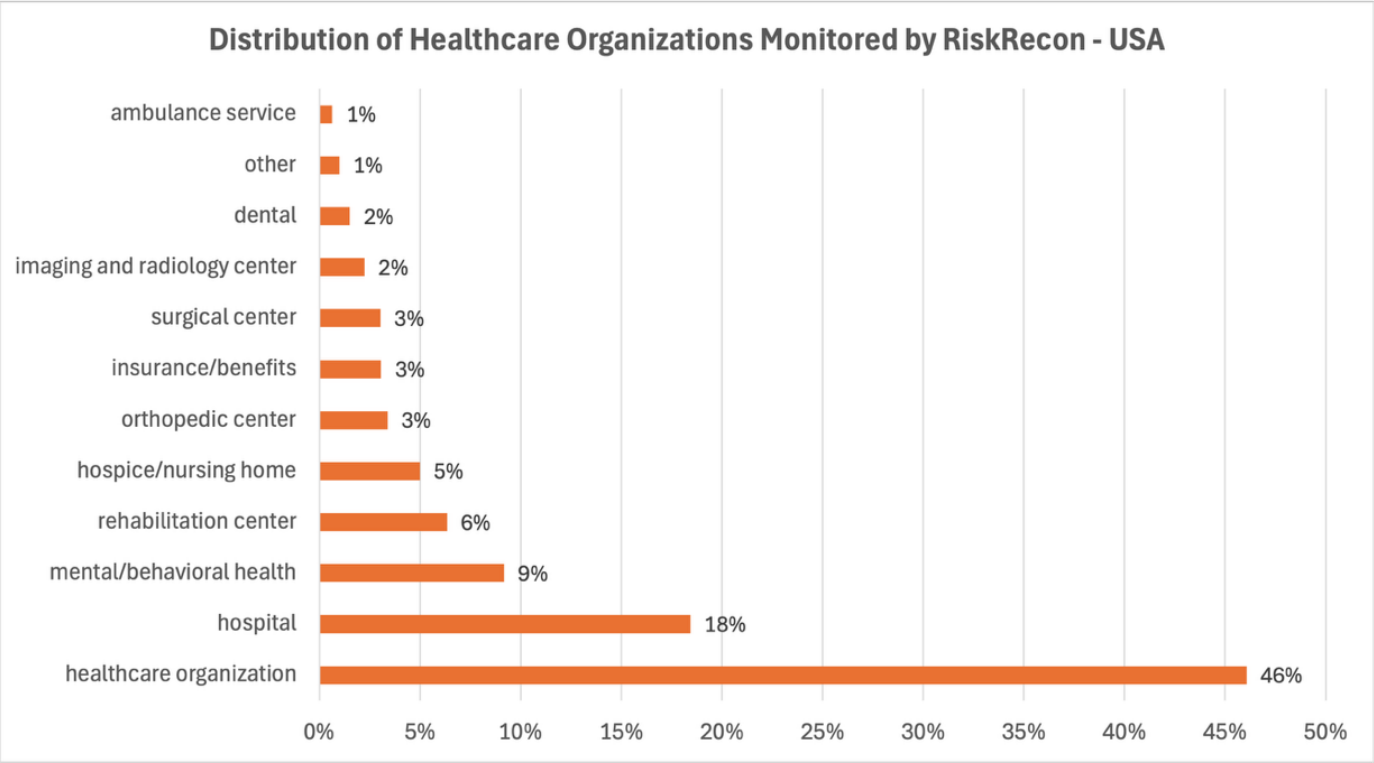
While much of this study is dedicated to cross examining the events, we also look at some good news – that healthcare organizations with good cybersecurity hygiene have much lower rates of breach events than those with poor hygiene. Perhaps the task of society is to understand how to better help healthcare organizations operate a higher state of defensibility necessary to resist the significant and unique threat level it faces.

The Study

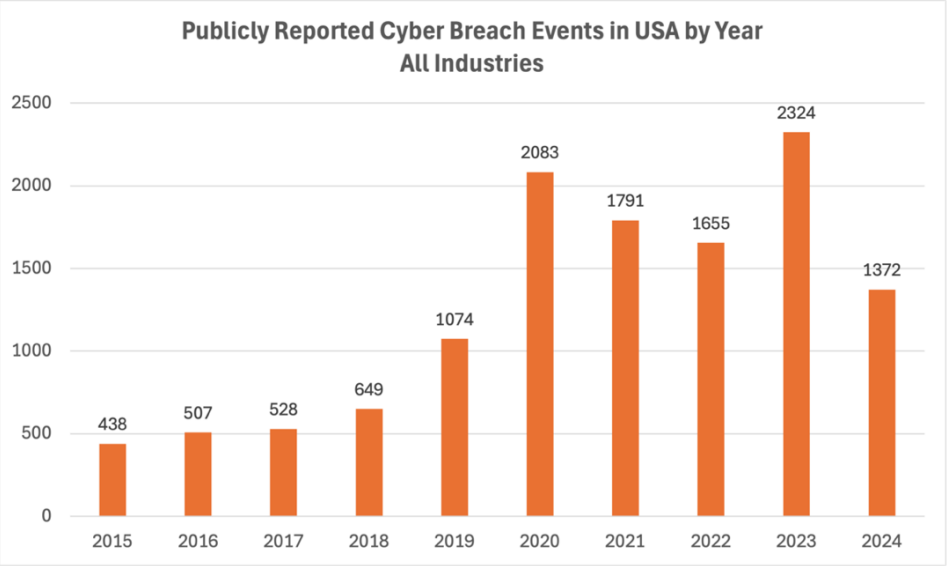
RiskRecon continuously monitors the cybersecurity hygiene of over five million organizations, passively assessing performance against nine security domains and 33 security criteria spanning tens of thousands of security checks. RiskRecon's assessments cover software patching, application security, web encryption, network filtering, breach events and so forth. RiskRecon distills each assessment, detailing the IT profile, the security issues, and related severities, into a simple cybersecurity rating of A to F.

This study is based on the subset of 196,000 organizations whose assessments are human-supervised, providing expansive, accurate visibility into each organization's attack surface, their cybersecurity conditions, and breach events impacting the organization. The breach events accounted for in this study are limited to those that are publicly reported events of unauthorized access to systems and services. Reports of events which were confirmed to contain the breach such that there was no impact to data or operations were not included.

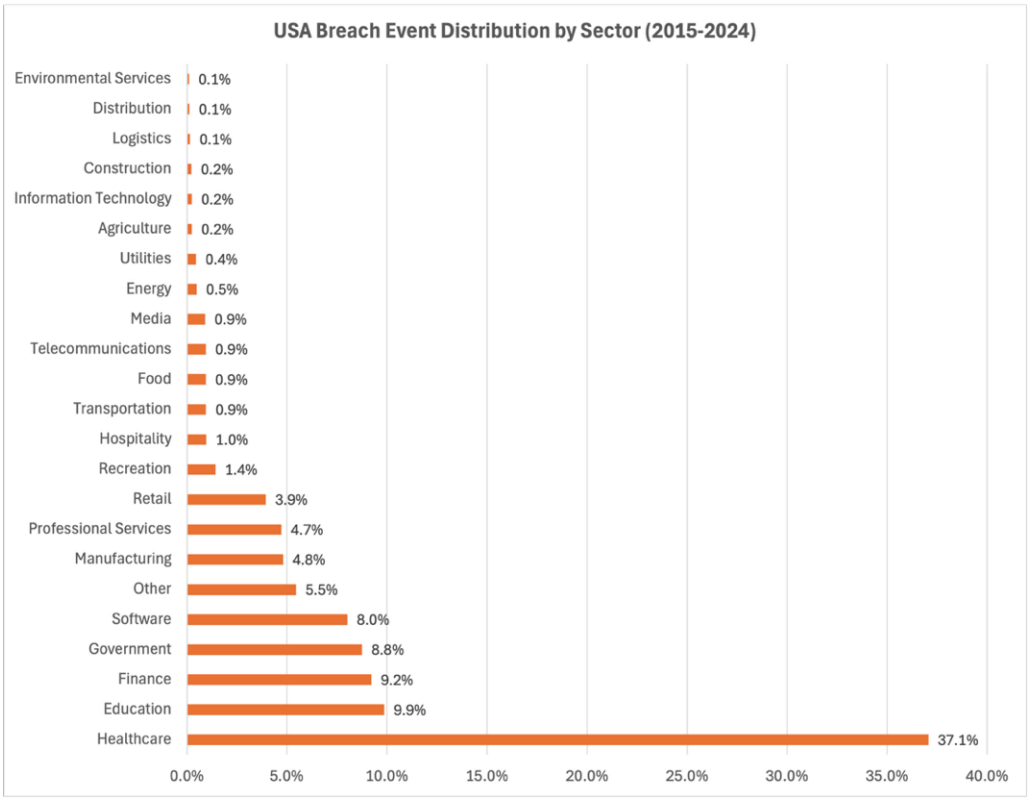
Among these 196,000 organizations, RiskRecon monitors 14,583 US-based healthcare organizations. RiskRecon divides these organizations into twelve healthcare subsectors. The "healthcare organization" category is the largest, accounting for 46% of the total. This lumps in healthcare clinics, physician groups, and large healthcare organizations. Essentially, it contains all healthcare providers that are not primarily identified as a hospital or a specialist provider such as a surgical, radiology, or orthopedic center.



From 2015 to 2024, RiskRecon cataloged 12,421 publicly reported breach events of US-based organizations across all sectors. Ignoring the increasing severity of the breach events, the good news is that in 2024 publicly reported breach events in the US were down 40% from the peak in 2023 (1,372 compared with 2,324) and were at the lowest level since 2019.

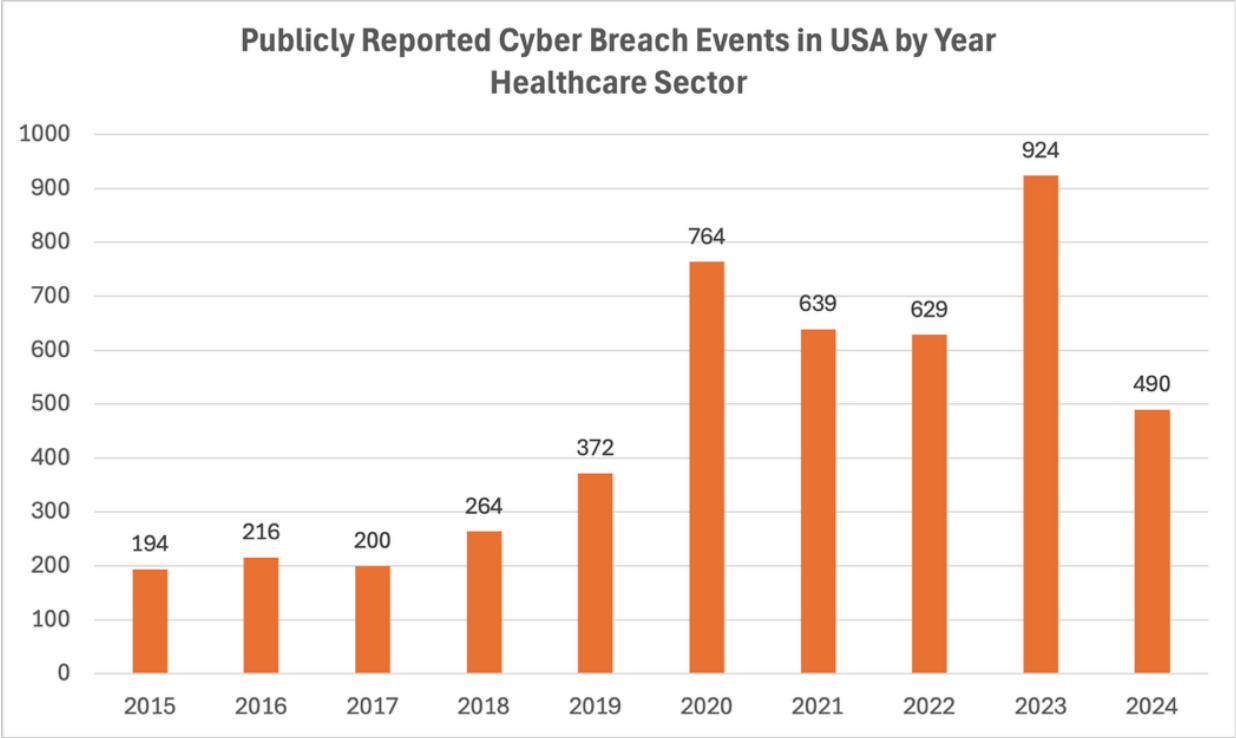


From 2015 through 2024, the healthcare sector has carried the heaviest breach event burden, accounting for 37% of all breach events in the United States (4,692). Healthcare was followed distantly by Education at 9.9% of all events and Finance at 9.2%.

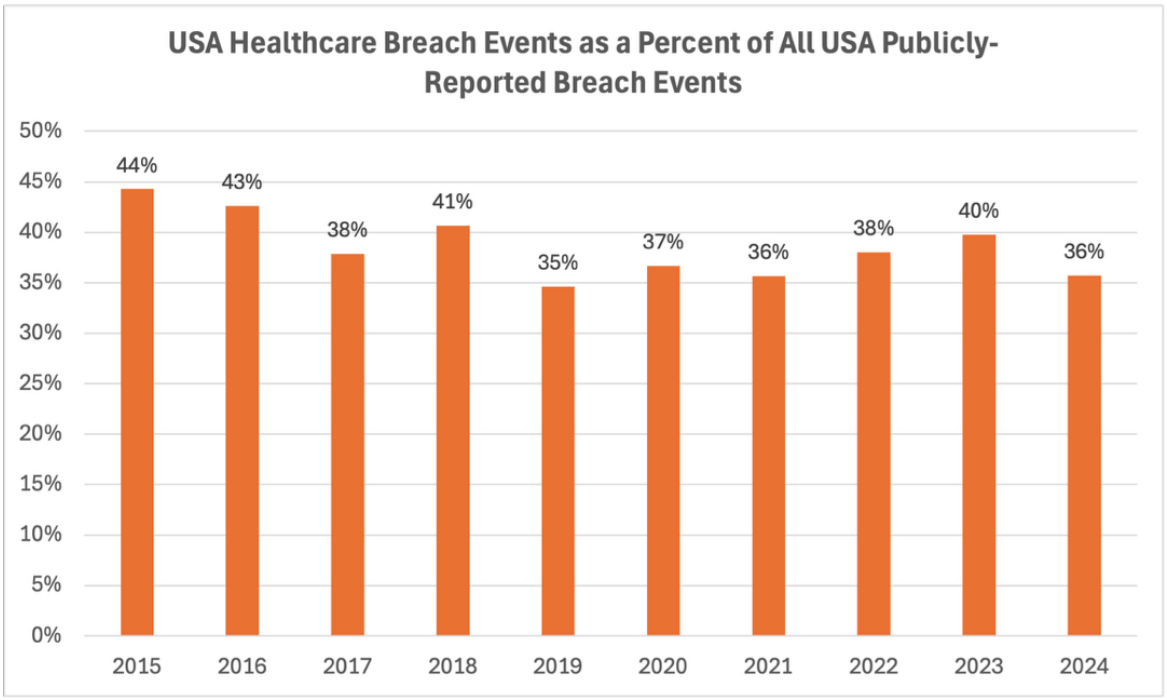


Examining the Healthcare Sector

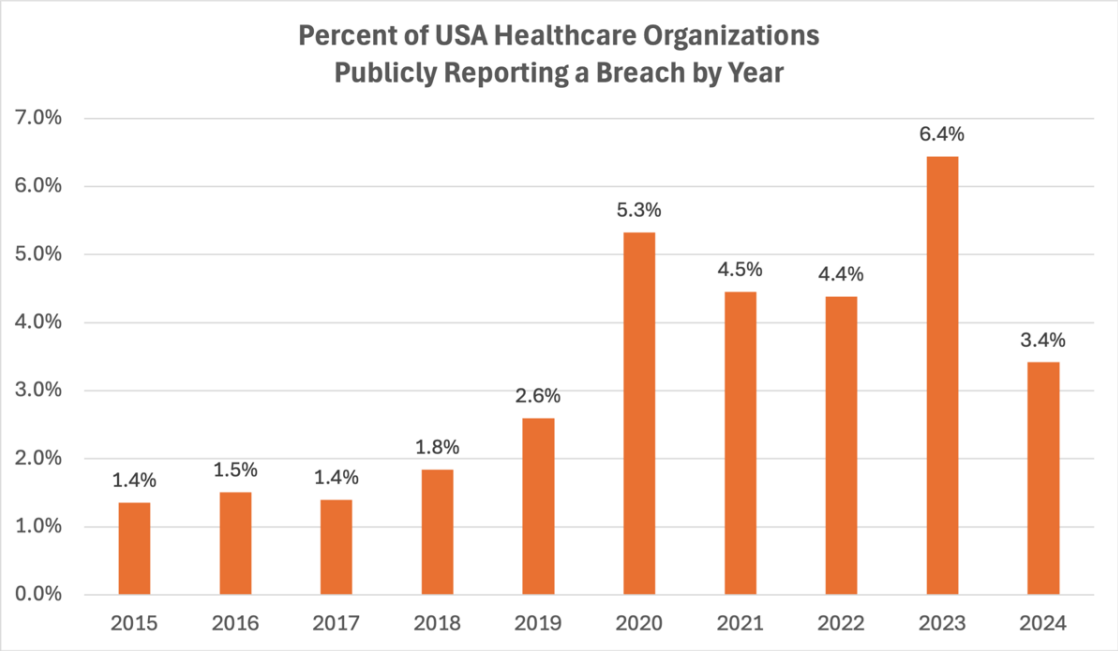
Of the 12,421 publicly reported cybersecurity breach events of US companies that RiskRecon has cataloged between 2015 and 2024, 37% (4,692) were reported by healthcare organizations. Mirroring the breach event trends for all sectors, publicly reported healthcare sector breach events are at a five-year low and down 47% from the 2023 peak and came in at the lowest level since 2019.



Healthcare's breach event burden has been consistently heavy over time, accounting for a high of 44% of all publicly reported US breach events reported in 2015 and a low of 35% in 2019. In 2024, healthcare represented 36% of events.

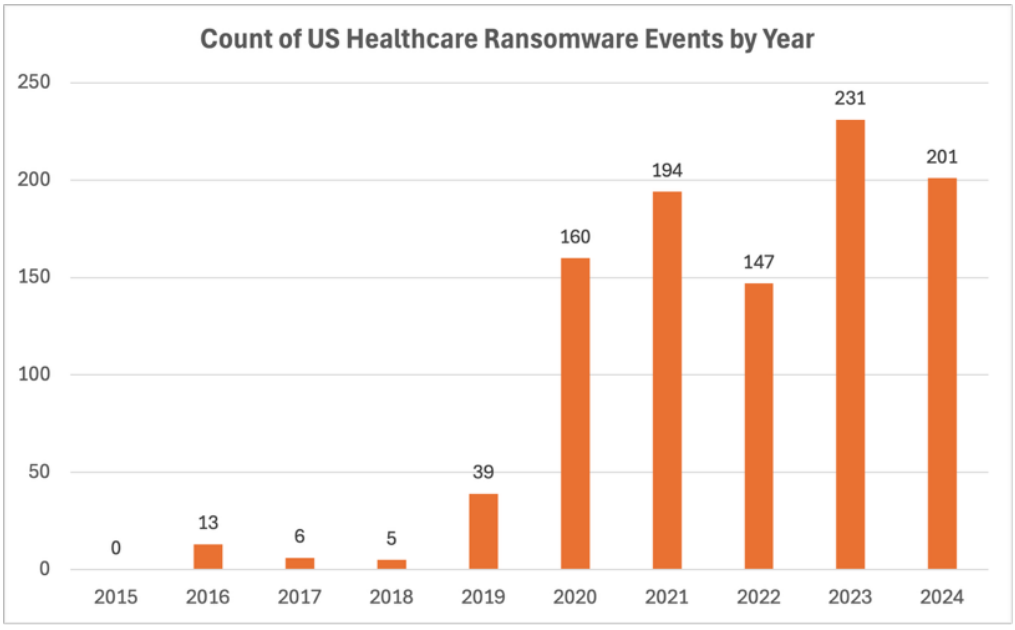


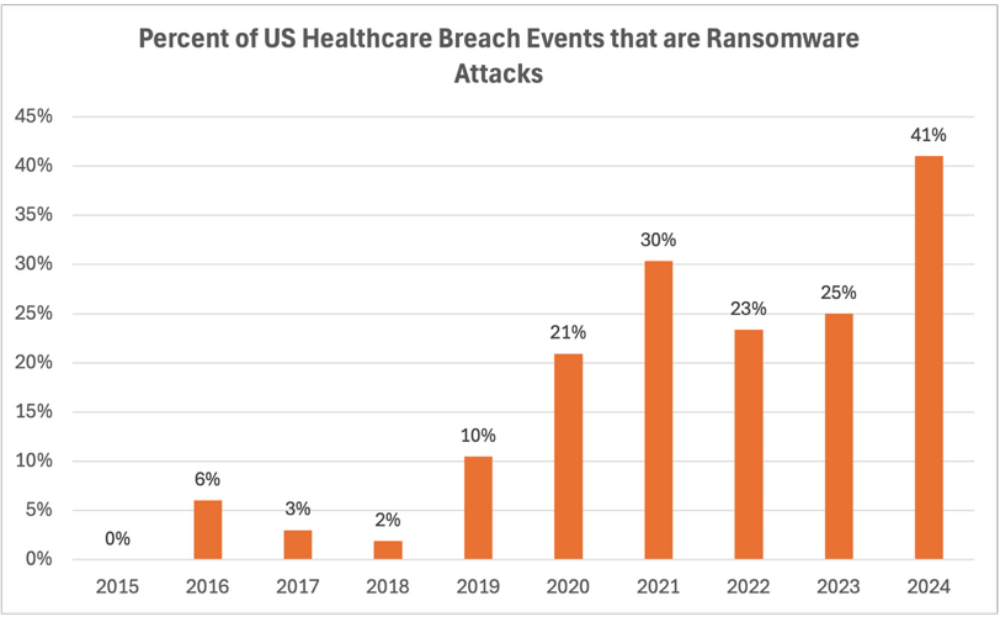
Twenty-eight percent of the 14,583 US-based healthcare organizations in this study (4,042) publicly reported one or more breach events between 2015 and 2024. Looking at the 10-year average, 3.3% of healthcare organizations publicly reported a breach per year.



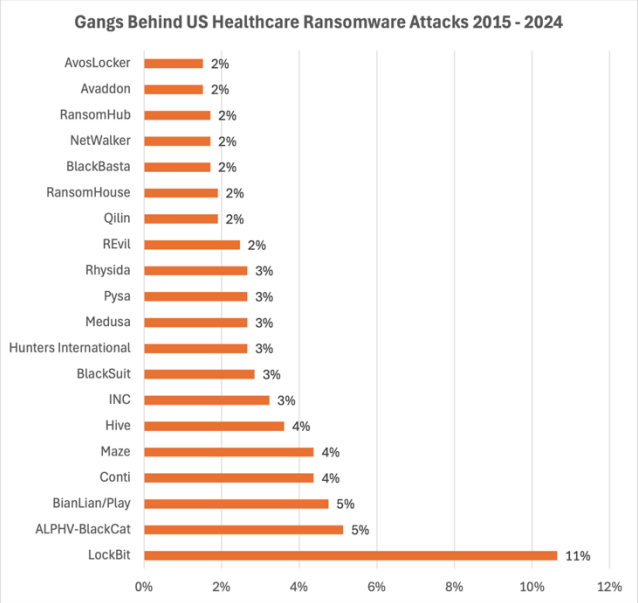
RANSOMWARE

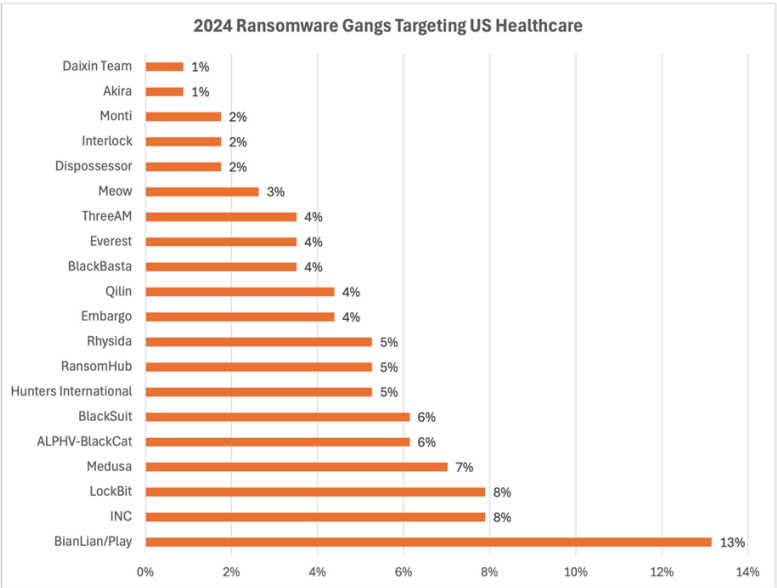
Ransomware attacks stand out from all other breach events in the severity of their impact, aggressively holding hostage the operational capability of victim systems and the confidentiality of sensitive data until financial demands are met. The volume of publicly disclosed ransomware attacks against US healthcare entities has grown from zero in 2015 to 201 in 2024. During that time ransomware attacks made up 21% of the events. With ransomware being the driver behind 41% of breach events in 2024 the trajectory is clear – if your organization is breached, it is likely that it is going to be a ransomware attack. Make sure that response playbook is solid and well-rehearsed.





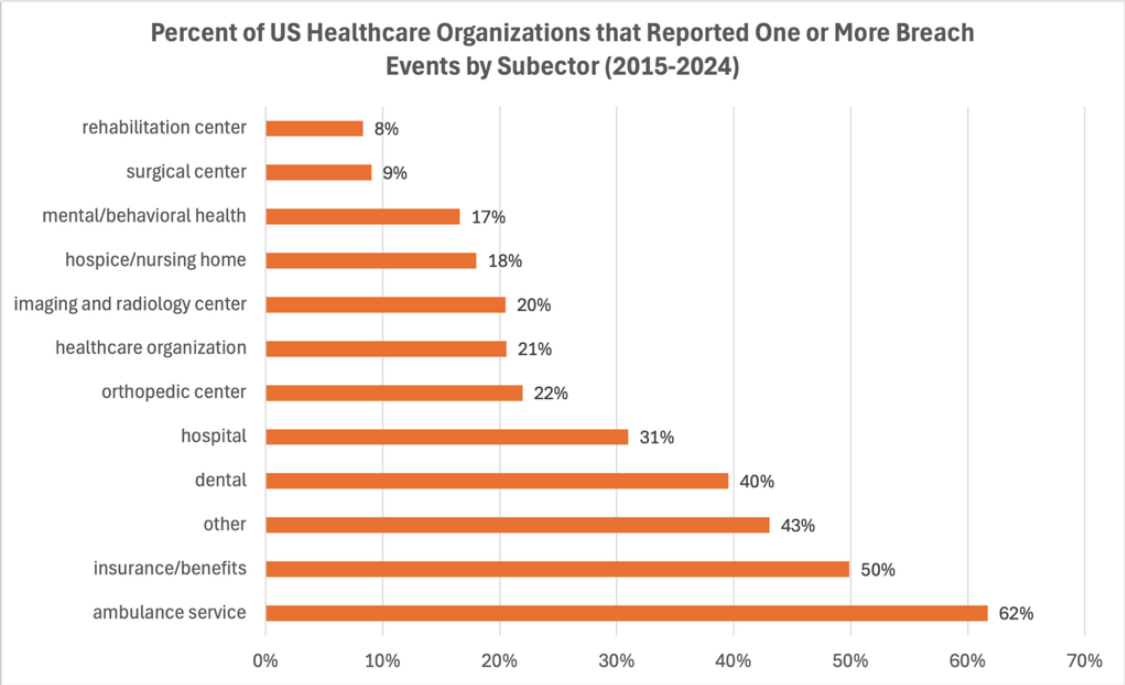
The drivers behind these attacks are ransomware gangs that are financially motivated to compromise organizations and make them pay for restoration of services and promises of deleting stolen data. Since 2015, RiskRecon has identified 99 different gangs behind the healthcare ransomware attacks, with LockBit being the most prolific from 2015 – 2024. In 2024 the BianLian and Play ransomware gangs combined for 13% of all US healthcare ransomware attacks.



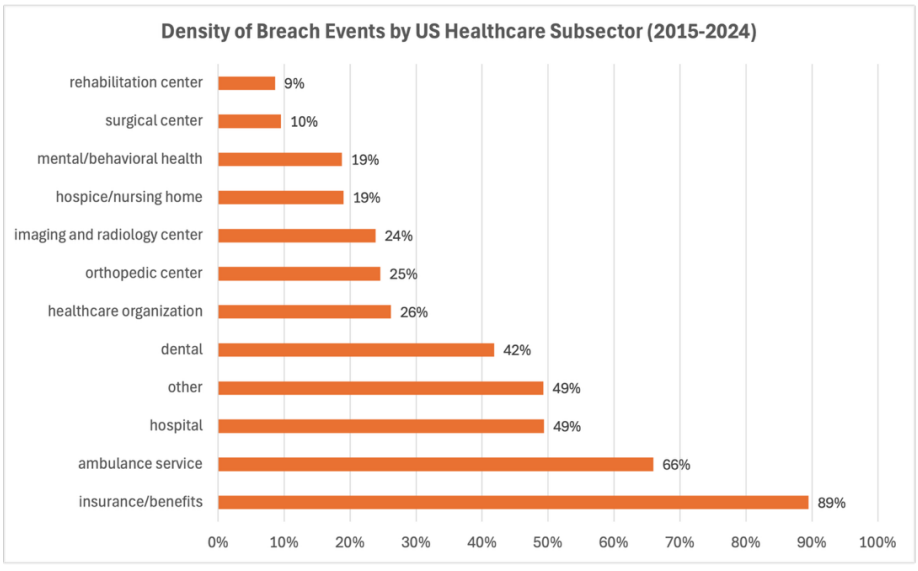


Studying Healthcare Subsectors

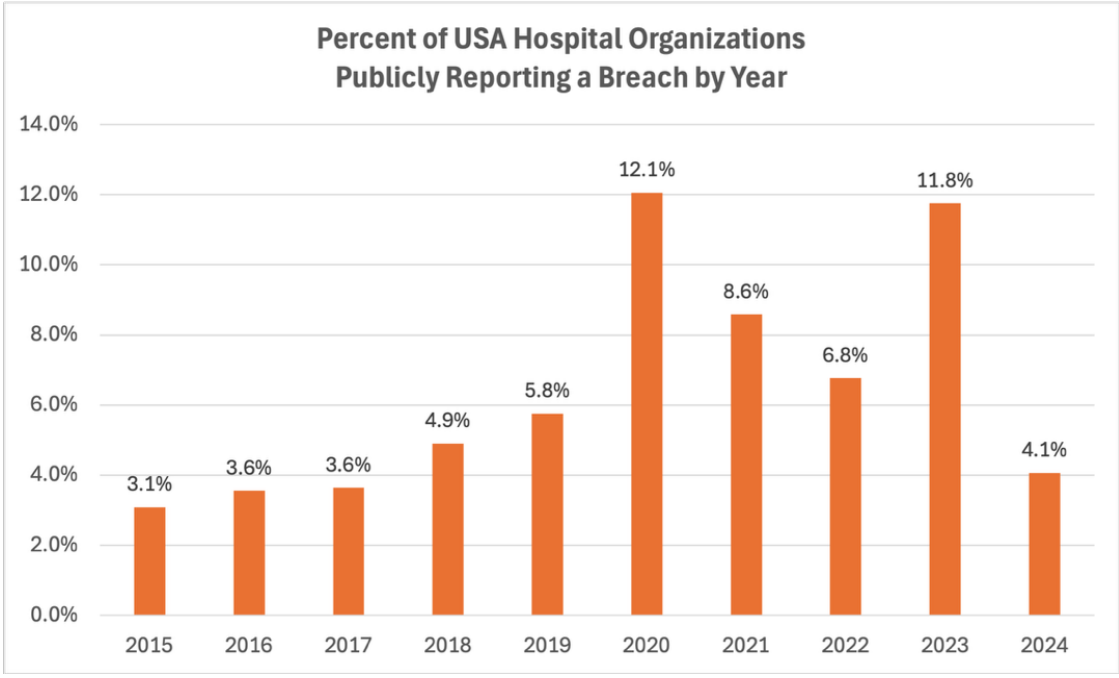
Splitting out the industry into subsectors reveals which areas of healthcare are reporting compromise most frequently. Ambulance services came in the highest with an amazing 62% reporting at least one breach between 2015 and 2024. That was followed by insurance/benefits at 50%. Thirty-one percent of hospitals reported experiencing one or more breach event from 2015 to 2024.



Taking another angle on the data, let's look at how frequently breach events occur within the sector. In insurance/benefits from 2015 – 2024 for every 10 organizations in the subsector there were almost nine publicly reported breach events (89% breach event frequency rate). Ambulance services had a very concerning 66% breach event frequency and hospitals 49%.



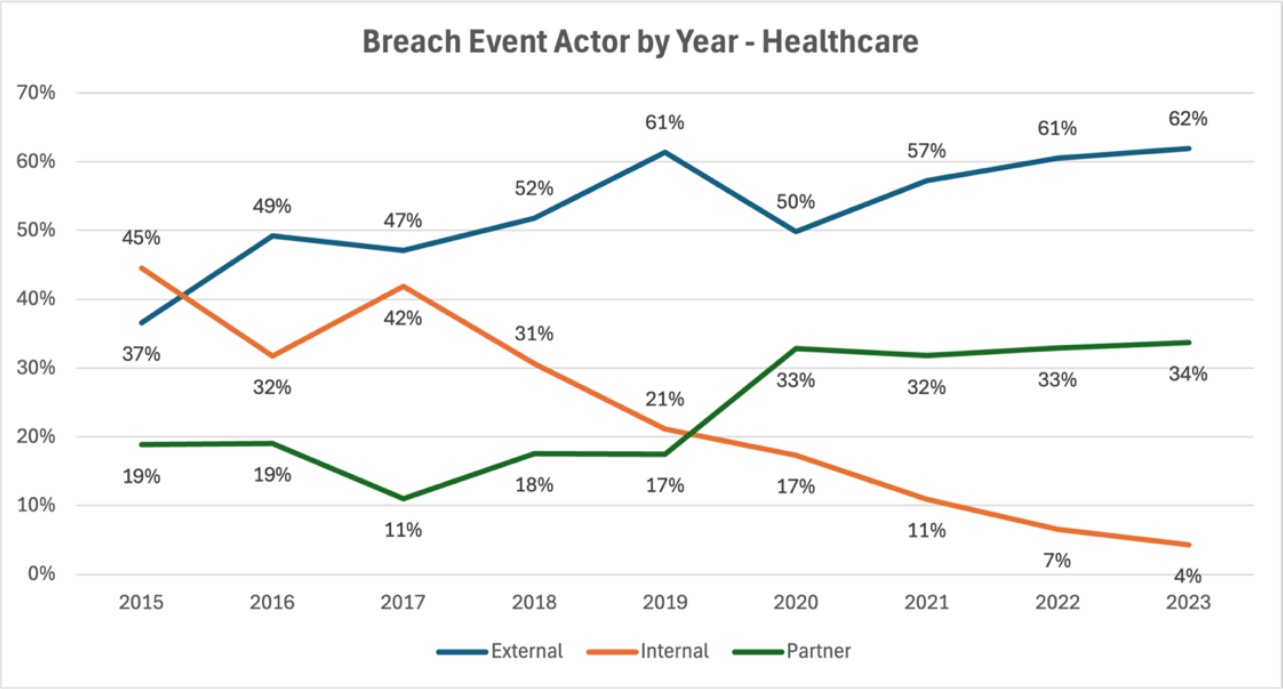
Digging down into the year-by-year breach frequency for hospitals, we see that the frequency within a given year has gone as high as 12.1% in 2020, with twelve publicly reported hospital breach events for every 100 hospitals. Fortunately, though still concerning, in 2024 there were just over four publicly reported breach events for every 100 US hospitals, nearly one third that of 2023.



Breach Event Analysis

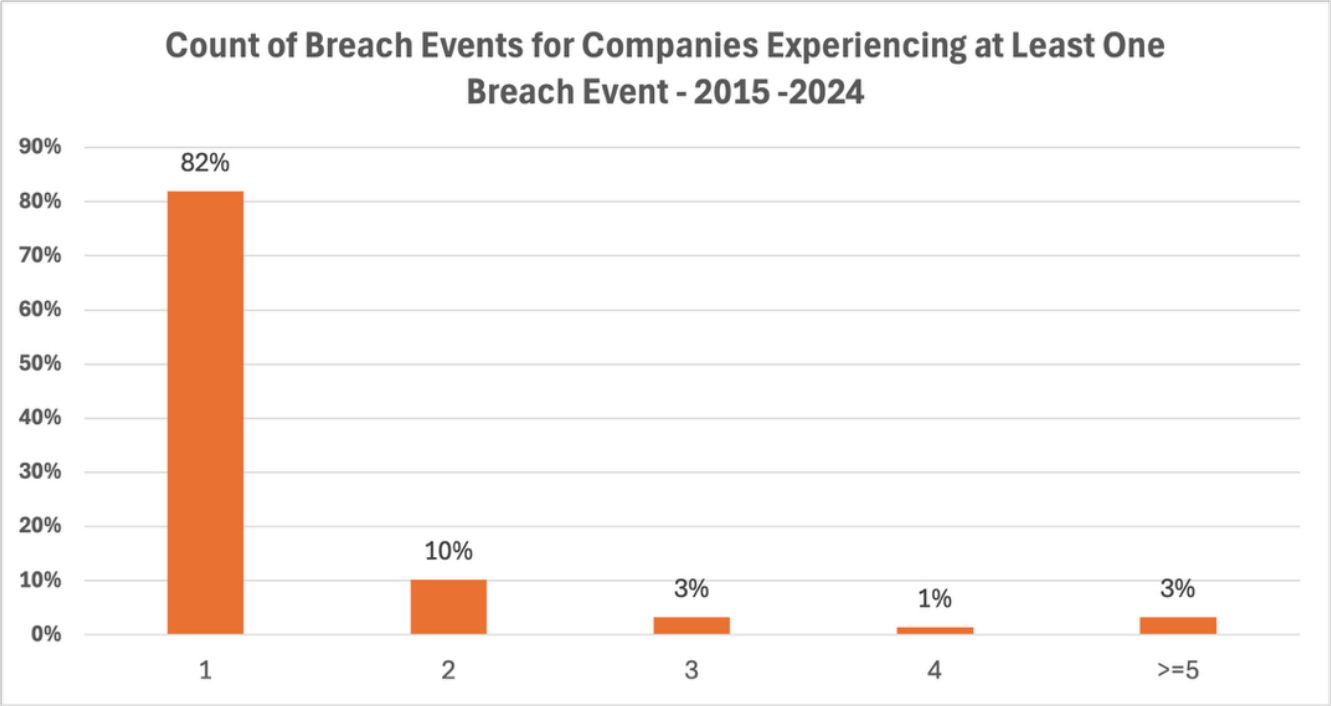
BREACH EVENT ACTORS

External actors directly compromising the systems of the victim organization accounted for 62% of all healthcare breach events in 2023, up significantly from 37% of all events in 2015. Breach of systems and data under the stewardship and administration of vendors accounted for 34% of all publicly reported breach events in 2023, growing from 19% in 2015. In comparison, insider sourced breach events have taken the opposite course, falling from the top spot in 2015 at 45% all the way to 4% in 2023.



BREACH RECURRENCE

If you are responsible for managing third-party risk, you will be keenly interested in this stat. For those organizations publicly reporting a breach event during the study period, 17% reported at least one more breach event with the next event being disclosed within an average of 2.7 years. So, if you were to guess which vendor is going to be the source of your next breach event, you'd be wise to look at those that were most recently compromised – nearly one in five of those will have another breach event and that event will occur within average of less than three years.



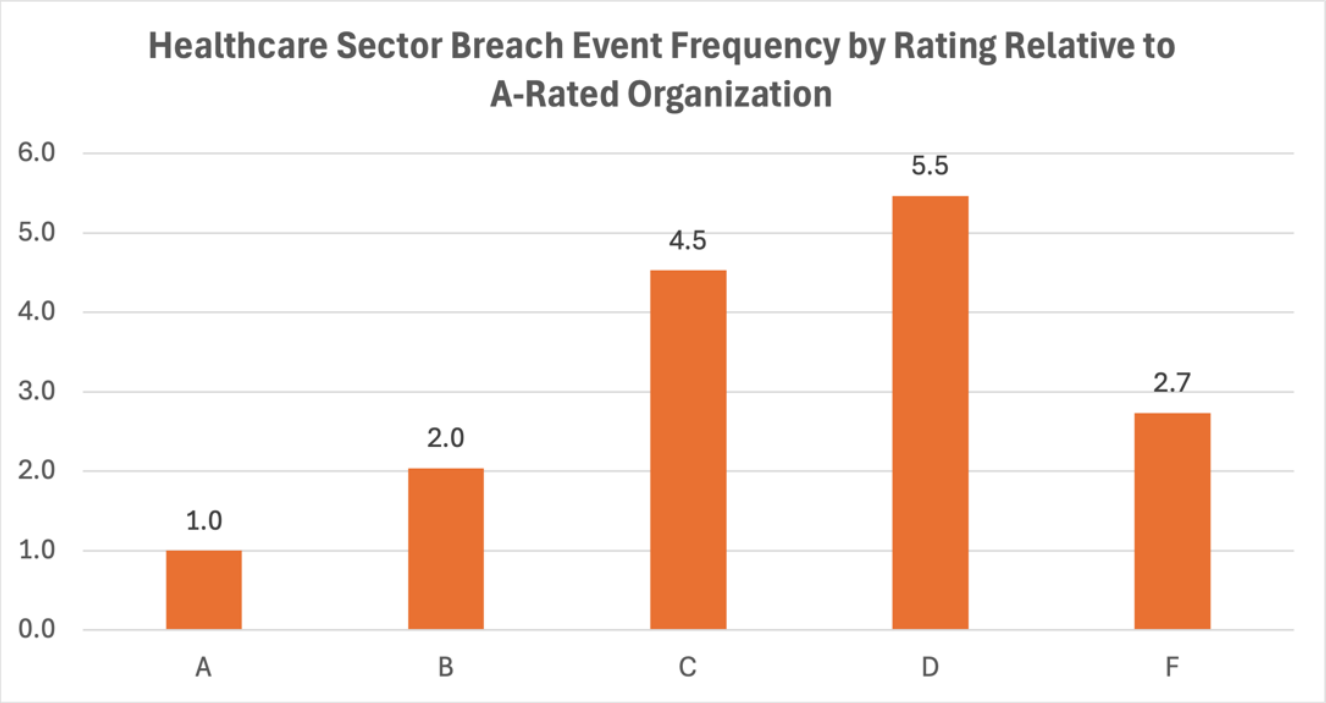
Cybersecurity Hygiene

In the face of this terrible threat pressure, there is positive news. Good cybersecurity hygiene pays great returns! US healthcare organizations with good cybersecurity hygiene have over four times lower breach event frequency compared to those with poor or very poor hygiene. Certainly, organizations with good hygiene still get compromised, but at a much lower rate.

CYBERSECURITY HYGIENE AND BREACH EVENT FREQUENCY

As a leading provider of cybersecurity ratings, RiskRecon continuously assesses the passively observable cybersecurity practices of organizations against nine security domains and 33 security criteria spanning tens of thousands of security checks.

Looking across RiskRecon's population of 14,583 US-based healthcare organizations, those with poor or very poor cybersecurity hygiene (those rated C, D or F) experienced a combined 4.4x higher frequency of breach events compared to A rated organizations, which RiskRecon observes as having very clean hygiene. As a group, forty-six percent of C, D and F rated companies have had a breach event since 2015. In comparison, only 10% of A rated companies and 21% of B rated companies have publicly reported a breach.



Why do US healthcare organizations rated as F, RiskRecon's lowest rating, have a lower frequency of breach events than C and D rated organizations? While the RiskRecon ratings model does strongly correlate between hygiene and breach event rates, the model is not explicitly designed to predict breach events. Rather, RiskRecon's rating model is designed to reflect real-world risk management practices, where A rated organizations have an observable external hygiene posture like financial institutions and F rated organizations look more like universities.

The cybersecurity conditions underlying the RiskRecon rating reveal just how poor the cybersecurity hygiene is of companies, on average, at the time of the breach event. In comparison with the larger US healthcare population, those that experience a breach event, on average, have:

- ✓ Twelve times more high and critical severity issues in their internet facing systems.
- ✓ Seven times more unsafe network services exposed to the internet, such as RDP, telnet, database listeners, NetBIOS, and SMB.
- ✓ Six times higher frequency of application security issues such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet with single-factor authentication.
- ✓ Fifteen times higher frequency of encryption configuration issues in high value systems that collect and transmit sensitive data.

Table: Comparison of count of security issues in internet-facing systems surrounding the date of the breach event.

Security Issue	Percent with at Least one Issue		
	Victim Hygiene at Time of Breach Event	All US Healthcare Organizations	Difference
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	3.5	0.3	12x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	2.8	0.4	7x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	7.5	1.2	6x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	20.8	1.4	15x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	5.8	0.3	19x higher

Ignoring issue counts and just looking at the percent of companies with one or more significant issues across the RiskRecon cybersecurity domains, the material breach event victim group again stands out as having very poor hygiene in comparison to the general population.

- ✓ 28 times more organizations with at least one high or critical severity software vulnerability in their internet facing systems.
- ✓ 17 times more organizations with at least one unsafe network service exposed to the internet.
- ✓ 11 times more organizations with at least one application security issues such as not implementing encryption in systems that collect sensitive data and application platform administration interfaces exposed to the internet with single-factor authentication.
- ✓ 21 times more companies with at with at least one web application that transmits sensitive data that has HTTP encryption issues such as expired certificates, weak encryption algorithms, or invalid certificate subjects.

Table: Comparison of percent of organizations with at least one issue in their internet-facing systems

	Average Issue Count		
	Victim Hygiene at Time of Breach Event	**All US Healthcare Organizations**	**Difference**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	39%	1.4%	28x higher
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	40%	2.4%	17x higher
Application Security Issues Missing common security practices in applications that collect sensitive data	55%	5.1%	11x higher
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	62%	3%	21x higher
Email Security Issues Security issues in active email servers and domains that increase susceptibility to phishing and data theft	40%	2%	20x higher

Why such a strong correlation? Organizations that have poor cybersecurity hygiene in their external surface not only provide easy initial entry vectors, but they are also unlikely to have strong internal defenses that reduce the risk of ransomware detonation. Conversely, organizations that demonstrate very clean hygiene in their externally observable systems and signals don't offer as many initial entry vectors and are more likely to have strong internal defenses.

CHANGE IN HYGIENE AFTER BREACH

As it turns out, the data shows that a breach event must be a strong motivator for improving cybersecurity hygiene. Comparing the cybersecurity hygiene of victim organizations at the time breach with their hygiene as of Q1 2025, the organizations have dramatically lower counts of critical software vulnerabilities, unsafe network services, application security issues, and web encryption issues. Their current issue rate isn't as good as that of the overall US healthcare general population, shown in the previous table, but it is still materially better.

	Average Issue Count		
	Victim Hygiene at Time of Breach Event	**Victim Hygiene Current (Q1 2025)**	**Change**
Software Patching Issues Software vulnerabilities with CVSS rating of High or Critical (7.0 – 10)	3.5	1.1	3.2x lower
Unsafe Network Services Internet-exposed unsafe services such as databases and remote administration	2.8	1.2	2.3x lower
Application Security Issues Missing common security practices in applications that collect sensitive data	7.5	3.2	2.3x lower
Web Encryption Issues Errors in encryption configuration in systems that collect and transmit sensitive data	20.8	5.4	3.8x lower

CONCLUSION: STRENGTHENING HEALTHCARE WITH DATA-DRIVEN DEFENSE

The healthcare sector has consistently been one of the most targeted industries, responsible for 37% of all publicly reported U.S. breach events over the past decade. That's not surprising, given the vital role healthcare plays and the complexity of its digital infrastructure. The good news? There's a clear path forward.

RiskRecon's analysis shows that strong cybersecurity hygiene significantly reduces breach frequency—by a factor of more than four. Organizations that proactively manage and monitor their external risk posture are far less likely to suffer a publicly reported breach. And for those that have been impacted, the data reveals meaningful improvement when organizations take action.

RiskRecon empowers healthcare providers to assess, monitor, and continuously improve their security hygiene with precision. Our ratings, built on real-world data from millions of organizations, give you the visibility to defend your systems, the insights to prioritize action, and the tools to strengthen your third-party ecosystem.

Contact us to learn how Mastercard's Enterprise Cybersecurity Platforms supports the full ecosystem resilience cycle with RiskRecon, Cyber Quant, Threat Protection and more!

Contributors

Kelly White
SVP, Cybersecurity Solutions
Mastercard
kelly.white@mastercard.com

Johnathan Beifuss
Director, Cybersecurity Solutions
Mastercard
johnathan.beifuss@mastercard.com