SOPHOS

THE STATE OF RANSOMWARE IN HEALTHCARE 2025

Findings from an independent survey of 292 IT and cybersecurity leaders in the healthcare sector across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. October 2025

Introduction

Welcome to the fifth edition of the annual Sophos State of Ransomware in Healthcare report, which reveals the reality of ransomware for healthcare providers in 2025.

This year's report unveils how healthcare providers' experiences of ransomware – both causes and consequences – have evolved over the last year. It also shines new light onto previously unexplored areas, including the operational factors that left healthcare providers exposed to attacks and the human impact of incidents on healthcare IT/cybersecurity teams.

Based on the real-world frontline experiences of 292 IT and cybersecurity leaders from the healthcare sector, across 17 countries whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why healthcare providers fall victim to ransomware
- What happens to the data
- Ransom demands and payments
- Business impact of ransomware
- Human impact of ransomware

A note on reporting dates

To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2025. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2024.

About the survey

The report is based on the findings from an independent, vendor-agnostic survey into organizational experiences of ransomware that was commissioned by Sophos and conducted by a third-party specialist between January and March 2025. All respondents work in organizations with between 100 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The 292 healthcare respondents the report is based on span 17 countries, ensuring that the survey results reflect a broad and diverse range of experiences. The report includes comparisons with the findings from our previous reports, enabling year-over-year juxtaposition. All financial data points are in U.S. dollars.

Key findings

Why healthcare providers fall victim to ransomware

- For the first time in three years, healthcare victims identified **exploited vulnerabilities** as the most common technical root cause of attack, used in 33% of incidents. This was followed by **malicious emails** and **compromised credentials** used in 22% and 18% of attacks respectively.
- Multiple operational factors contribute to healthcare providers falling victim to ransomware, with the most common being **a lack of people/capacity**, named by 42% of victims. It is followed in very close succession by both **known and unknown security** gaps, which were contributing factors in 41% and 40% of attacks respectively.

What happens to the data

- The **data encryption rate** in the healthcare sector is at its lowest level in five years, with 34% of attacks now resulting in data encryption, down from a 74% peak in 2024.
- 27% of healthcare providers that had data encrypted also experienced **data exfiltration**.
- 97% of healthcare providers that had data encrypted were able to recover it.
- The use of **backups** by healthcare providers to restore encrypted data is at the lowest rate in four years, used in 51% of incidents.
- 36% of healthcare victims **paid the ransom** to get their data back – among the lowest rates recorded in this year's survey.

Ransoms: Demands and payments

- The average (median) **ransom demand** made to healthcare providers has plummeted 91% over the last year, coming in at just $342K in 2025 compared to $4 million in 2024. The primary factor behind this significant decline is a 77% decrease in the percentage of ransom demands of $5M or more, down from 34% of demands in 2024 to just 8% in 2025.
- The average (median) **ransom paid** by healthcare providers has also dropped, coming in at $150K in 2025 compared to $1.47 million in 2024. The decline is largely driven by a 91% decrease in the percentage of ransom payments of $5M or more – however, it is important to note that there have been significant increases in sub $1M payments.
- The **proportion of the ransom demand** paid by healthcare providers dropped to 85% in 2025 from 111% in 2024.
- Looking closely at **demands vs. payments**, only 22% of healthcare providers said their payment matched the initial demand. 53% paid less than the initial ask, while 25% paid more.

Business impact of ransomware

- The average **cost for healthcare providers to recover** from a ransomware attack dropped by 60% over the last year, coming in at $1.02 million, down from $2.57 million in 2024. The sector reported among the lowest recovery costs recorded in this year's survey.
- Looking at **speed of recovery**, healthcare providers are recovering faster, with 58% recovered within a week in 2025, up from just 21% in 2024.

Human impact of ransomware

Every healthcare provider that had data encrypted reported that there were **direct repercussions** for the IT/cybersecurity team:

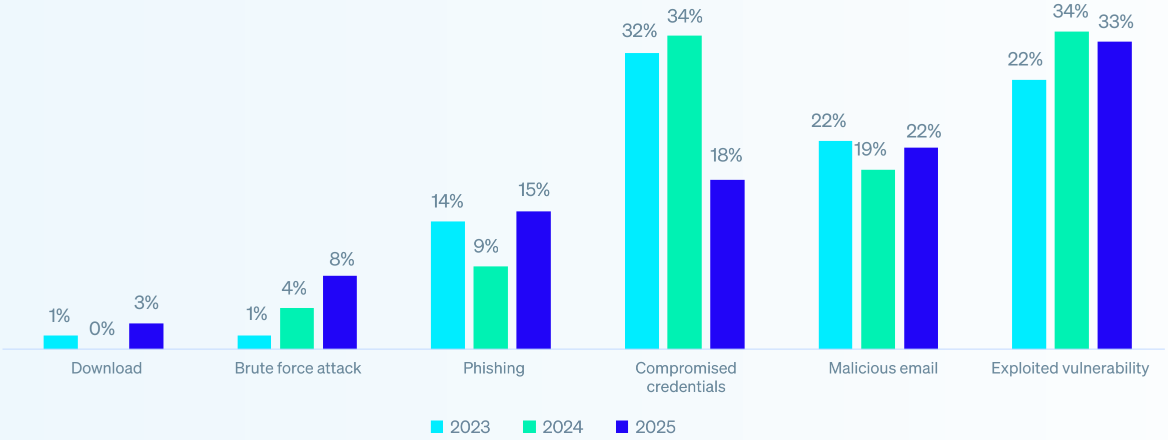
- 39% of healthcare IT/cybersecurity teams reported **increased pressure** from senior leaders, while 28% reported **increased recognition**.
- 37% of healthcare respondents cited increased anxiety or stress about future attacks as an impact on their IT/cybersecurity team.
- 35% reported a **change of team priorities/focus**.
- Close to a third of respondents (32%) cited both **feelings of guilt** that the attack was not stopped and **changes to team/organizational structure** as repercussions of the incident.
- 31% experienced an ongoing **increase in workload**.
- 24% of teams experienced **staff absence** due to **stress/mental health** issues related to the attack.
- In nearly one fifth of cases (19%), the team's **leadership was replaced** because of the attack.

Why healthcare providers fall victim to ransomware

Technical root cause of attacks in healthcare

For the first time in three years, healthcare providers identified **exploited vulnerabilities** as the leading root cause of ransomware attacks, responsible for 33% of incidents. **Malicious emails** ranked second, with their share rising from 19% in 2024 to 22% in 2025. **Credential-based attacks** continue to pose a significant risk, though reports dropped sharply—from 34% in 2024 to 18% in 2025.

Chart 1: Technical root cause of ransomware attacks in healthcare 2023 - 2025

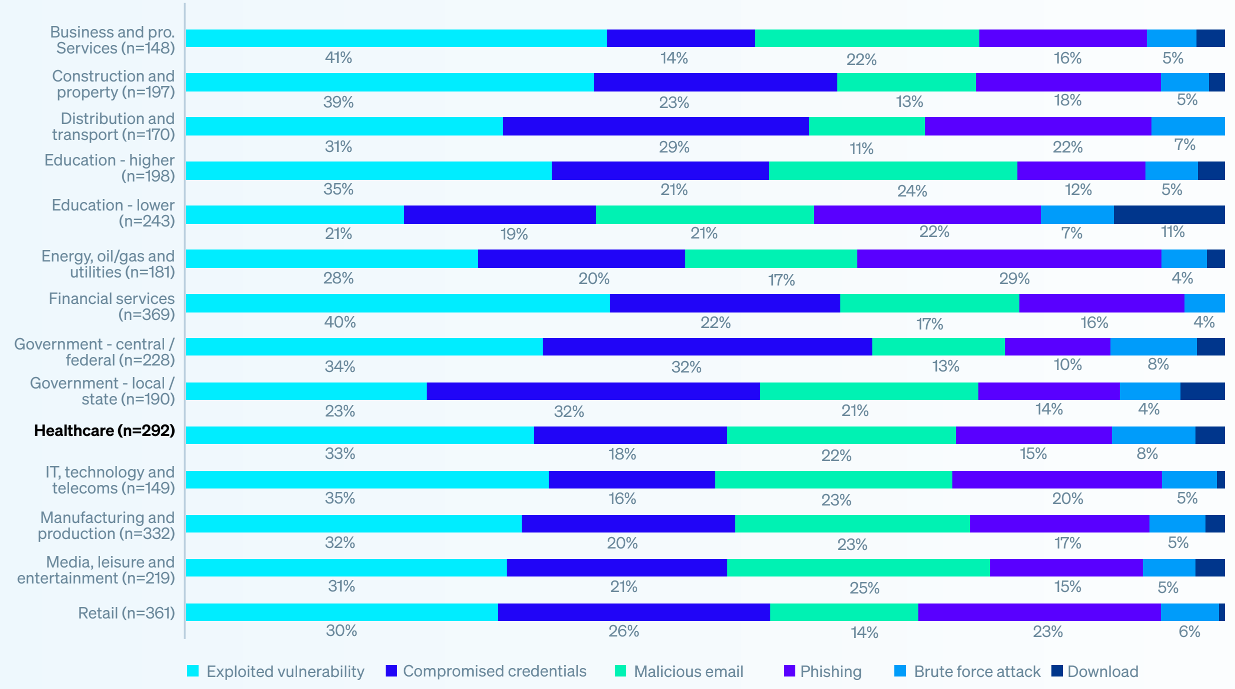


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=292 (2025), 271 (2024), 139 (2023).

The research reveals that while root causes vary by industry, exploited vulnerabilities are a major vector for most sectors. Notable exceptions:

- **Phishing** was the most common root cause cited by both **lower education** (22%) and **energy, oil/gas and utilities** (29%) providers.
- **Compromised credentials** were the most commonly perceived attack vector for **local/state government** organizations – accounting for nearly a third of incidents (32%).

Chart 2: Technical root cause of ransomware attacks split by industry

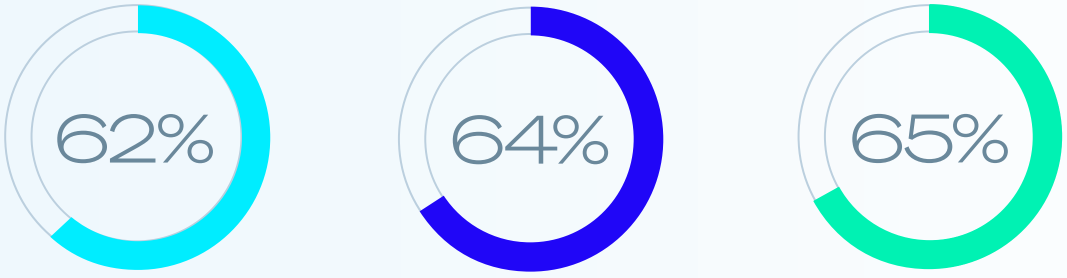


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

Organizational root cause of incidents in healthcare

This year's report explores for the first time the organizational factors that left healthcare providers exposed to attacks. The findings reveal that victims in the healthcare sector are typically facing multiple organizational challenges, with respondents citing 3 factors, on average, that contributed to them falling victim to the ransomware attack.

Overall, the organizational root causes are fairly evenly split across protection issues, resourcing challenges, and security gaps. However, healthcare providers are slightly more likely to cite a security gap (known and unknown) as the primary factor.



LACK OF/POOR QUALITY PROTECTION
Lack of protection or poor-quality protection solutions that could not stop the attack

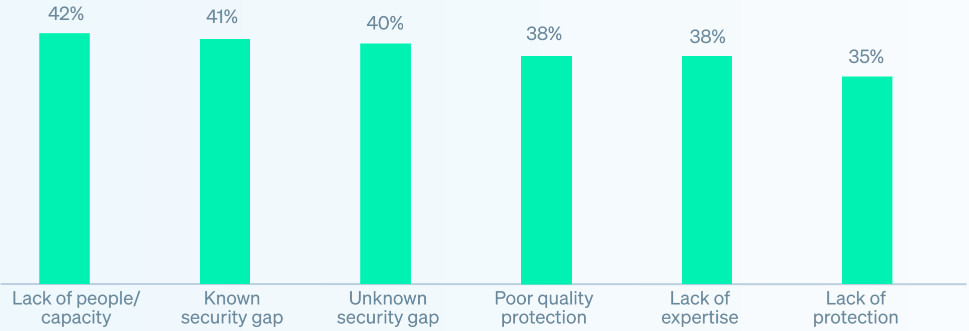
LACK OF PEOPLE/SKILLS
Lack of human expertise (skills or capacity) to detect and stop the attack in time

SECURITY GAP (KNOWN/UNKNOWN)
Had a known or unknown weakness in their defenses

Why do you think your organization fell victim to the ransomware attack? n=292. Consolidated responses.

A lack of people/capacity (i.e., an insufficient number of cybersecurity experts monitoring systems at the time of the attack) is the most common individual reason given, named by 42% of healthcare respondents. This is closely followed by **known security gaps** (i.e., weakness in defenses that respondents were aware of but had not addressed), which contributed to 41% of attacks. In third place was **unknown security gaps** (i.e., weakness in defenses that respondents were unaware of), which contributed to 40% of attacks.

Chart 3: Operational root cause of ransomware attacks on healthcare providers



Why do you think your organization fell victim to the ransomware attack? n=292

Organizational root cause by sector

The most common organizational root cause also varies by sector, reflecting the differing challenges businesses face. It's worth noting that no sector reported human error as the most common reason they fell victim to the ransomware attack.

Chart 4: Top operational root cause of ransomware attacks by sector (*denotes two joint top root causes)

LACK OF EXPERTISE	UNKNOWN SECURITY GAP	LACK OF PEOPLE/ CAPACITY	LACK OF PROTECTION	KNOWN SECURITY GAP	POOR QUALITY PROTECTION
We did not have the skills or knowledge available to detect and stop the attack in time	We had a weakness in our defenses that we were not aware of	We did not have sufficient cybersecurity experts monitoring our systems at the time of the attack	We did not have the necessary cybersecurity products and services in place	We had weakness(es) in our defenses that we were aware of but had not addressed	Our cybersecurity products and services were not able to stop the attack
Energy, oil/gas and utilities (43%) Lower education (K-12) (42%) * Manufacturing and production (42%) Construction and property (41%) *	Higher education (18 years+) (49%) Business & professional services (46%) Retail (46%) Financial service, incl. insurance (44%) *	Lower education (K-12) (42%) * **Healthcare (42%)**	Financial service, incl. insurance (44%) * Local/state government (40%)	Central/federal government (45%) IT, technology, telecoms (42%) Construction and property (41%) *	Media, leisure, & entertainment (44%) Distribution & transport (41%)

Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by industry.

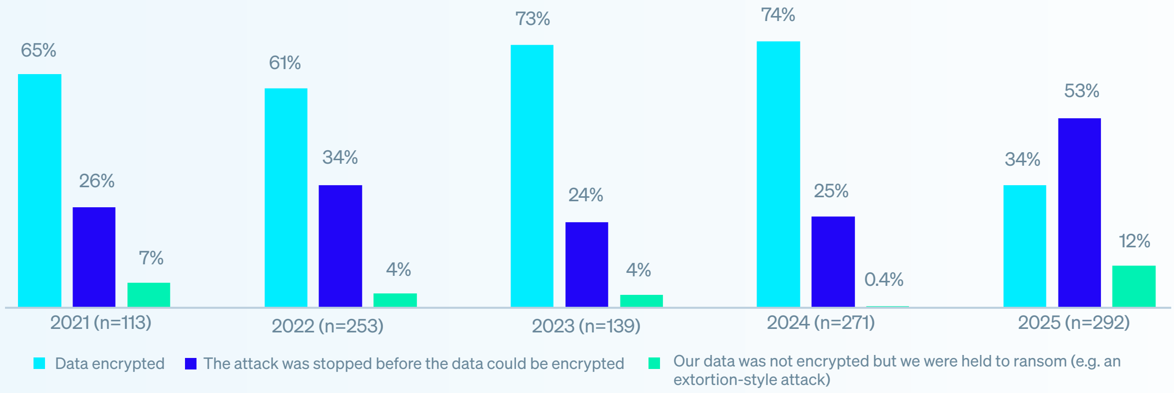
What happens to the data

Data encryption in healthcare

Encouragingly, data encryption in healthcare is at its lowest reported rate in the five years of our study, with only a third (34%) of attacks resulting in data being encrypted – the second lowest percentage recorded in this year's survey and less than half the 74% reported in 2024.

Meanwhile, the percentage of ransomware attacks that were stopped before data encryption has more than doubled over the past two years, climbing from 24% in 2023 to 53% in 2025. This suggests that healthcare providers are becoming more effective at halting attacks before they cause serious damage.

Chart 5: Data encryption rate in ransomware attacks on healthcare providers 2021 - 2025



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Data encryption rate by industry

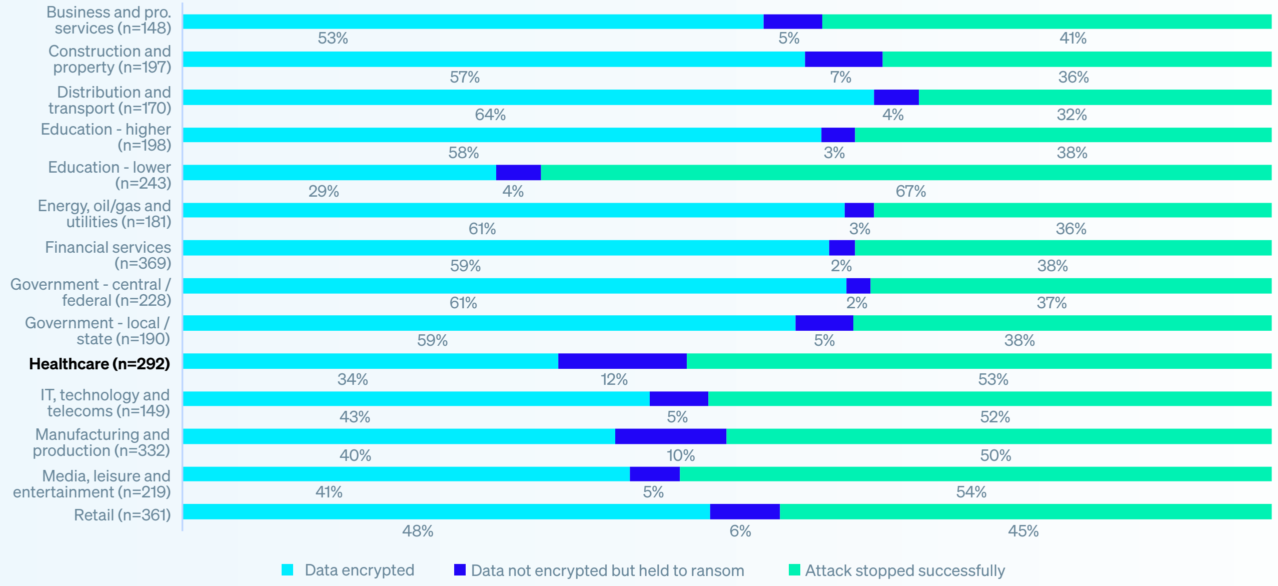
Organizations within the **distribution and transport** sector are most likely to have data encrypted (64%), indicating that organizations in this sector are less able to detect and stop the attack before encryption and/or are less able to block and roll back malicious encryption. In contrast, **lower education providers** reported the lowest data encryption rate, at just 29% - well below the 50% cross-sector average.

Data theft

Adversaries don't only encrypt data — they also steal it. Within the healthcare sector, 9% of all ransomware victims and 27% of those that had data encrypted experienced data theft. Breaking down the data by industry we see that:

- At the higher end, 42% of organizations in the **IT, technology, and telecoms** sector that experienced data encryption also had data stolen.
- By contrast, only 15% of organizations in both the **construction and property** and **energy, oil/gas, and utilities** sectors faced data theft alongside encryption.

Chart 6: Data encryption and theft by industry



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Extortion-style attacks

As shown in chart 5, the percentage of healthcare providers that did not have data encrypted but were held to ransom anyway (extortion) tripled to 12% of attacks in 2025 from just 4% in 2022/3 - the highest rate reported in this year's survey. This is likely due to the high sensitivity of medical data (patient records, etc.)

In contrast, both **financial service** providers and **central/federal government** organizations reported experiencing the fewest of these attacks, at just 2%.

Overall, **lower education** providers are most able to successfully prevent the repercussions of a ransomware attack, (i.e., to stop data being encrypted, to prevent data exfiltration, and to avoid being subject to extortion). This suggests that lower education providers are proving surprisingly effective at early detection and intervention - even with limited budgets.

Recovery of encrypted data in healthcare

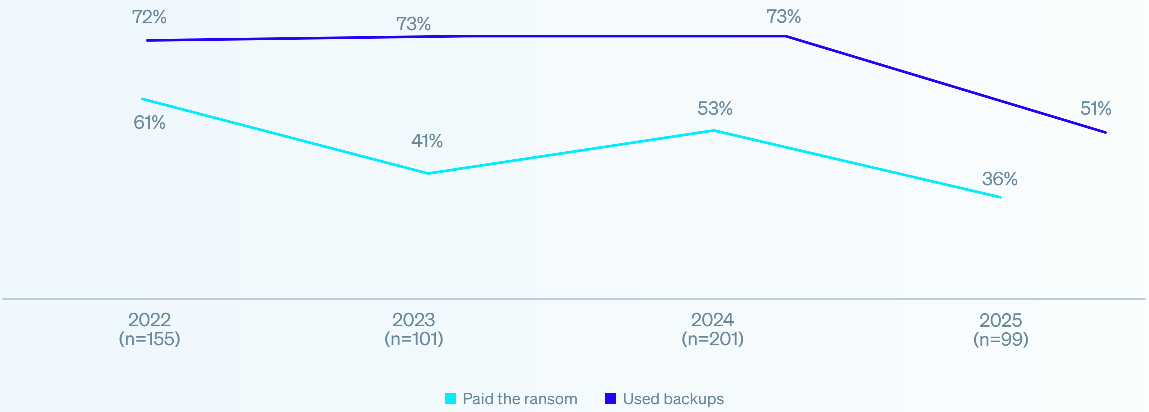
97% of healthcare providers that had data encrypted were able to recover it.

In 2025, just 36% of healthcare providers **paid the ransom**—down from 61% in 2022—placing the sector among the four least likely to recover data this way. At the same time, **backup use** has also fallen (51%, down from 72%). Collectively, these findings point to stronger resistance to demands but possible weaknesses or a lack of confidence in backup resilience.

Furthermore, the narrowing gap between healthcare providers paying the ransom to recover data and using backups to restore data suggests an increasing reliance on multiple/alternative recovery methods.

Evidencing this, we found that over a third (34%) of healthcare providers that had data encrypted said they **used other means to restore their data**.

Chart 7: Recovery of encrypted data in healthcare 2021 - 2025



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart.

Ransoms

Healthcare ransom demands

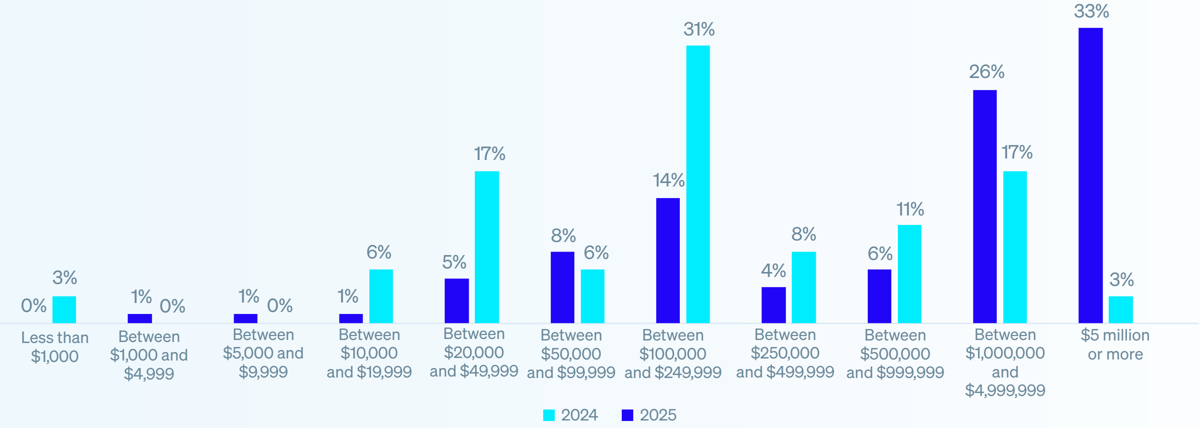
The average (median) ransom demand for healthcare providers plummeted 91% over the last year, coming in at $343K in 2025, down from $4 million in 2024. The decrease in ransom demands targeting healthcare providers is largely driven by a 77% decrease in demands of $5 million or more over the last year. However, it's important to note that there was a 13% increase in demands between $1M and $5M – accounting for 34% of demands – up from 30% in 2024.

Healthcare ransom payments

Following this trend, the average (median) ransom paid by healthcare providers also saw a sharp decline from $1.47 million in 2024 to just $150K in 2025 – the lowest payment reported across all industries surveyed. This is largely due to a 91% decrease in payments of $5 million or more over the last year. Sub $1 million payments, did however, show significant year-over-year increases – accounting for 81% of payments in 2025 – more than double the 40% recorded 2024.

These patterns suggest a potential shift: while attackers are still active in healthcare, their ability to demand or secure multimillion-dollar payouts appears to have diminished. The findings point to a sector becoming a tougher environment for cybercriminals, with both demands and payments now skewing toward smaller, lower-value cases.

Chart 8: Ransom payments in healthcare | Distribution banding

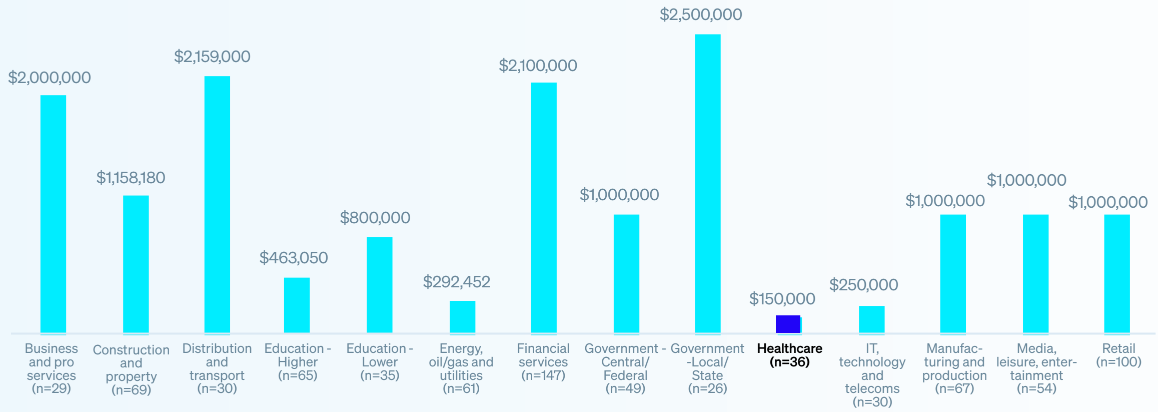


How much was the ransom payment that was paid to the attackers? n=36 (2025), 99 (2024)

Ransom payments by industry

Ransom payments varied considerably by industry, with state and local government organizations paying the highest average amount to attackers at $2.5 million. This may be due to critical service pressures, limited cyber resilience, and attackers exploiting their urgency to recover quickly. In contrast, and as already stated, healthcare providers paid the lowest at just $150,000.

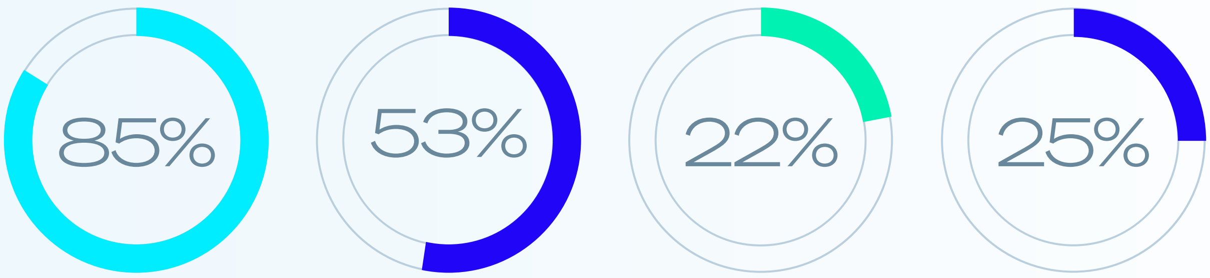
Chart 9: Ransom payments by industry



How much was the ransom payment that was paid to the attackers? Base numbers in chart. Note: Business and pro services and Government – Local/State have low base numbers, so findings should be considered indicative only.

How actual payments made by healthcare providers stack up with the initial demand

36 healthcare providers that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 85% of the initial ransom demand – a welcome drop from the 111% recorded in 2024. Overall, 53% paid less than the initial ask, a quarter (25%) paid more, and 22% matched the initial demand.



of the ransom demand **was paid**, on average

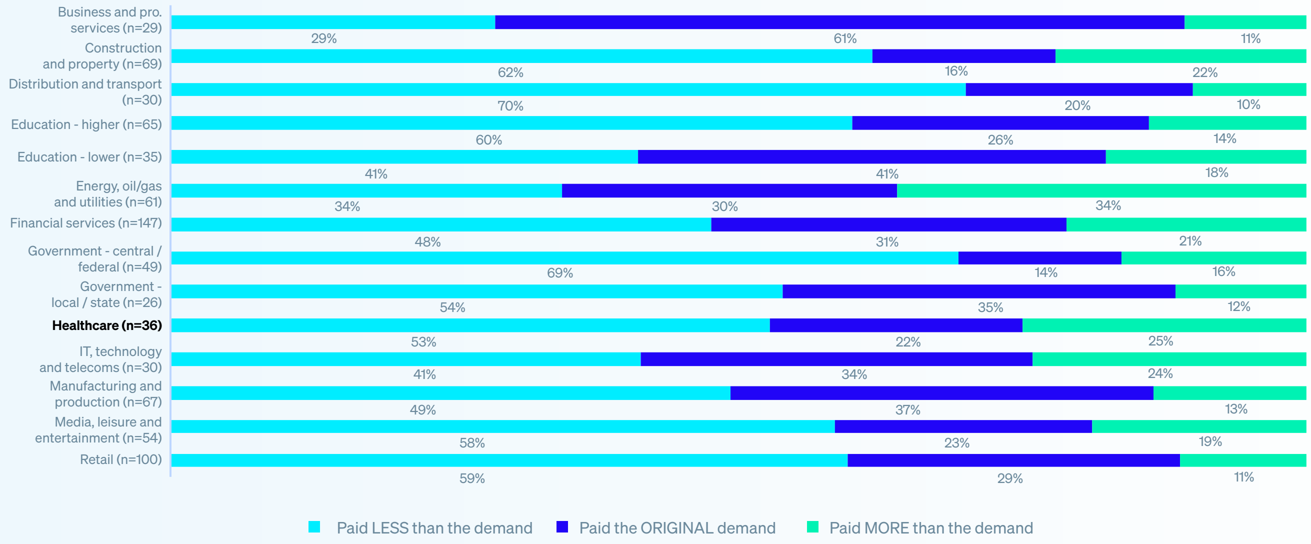
of payments were for **less** than the initial ransom demand

of payments **matched** the initial ransom demand

of payments were for **more** than the initial ransom demand

Splitting the data by industry, we see that, encouragingly, in the majority of sectors, paying less than the original ransom demand is the most common outcome. Organizations in the **distribution and transport** sector were by far the most likely to pay less than the original ransom demand (70%), suggesting a strong resistance to ransom demands. In contrast, **energy, oil/gas and utilities** providers were the most likely to pay more than what was initially demanded (36%), while **business and professional services** were most likely to match the initial ransom demand (61%).

Chart 10: How organizations respond to demands by industry



How much was the ransom payment that was paid to the attackers? Note: Business and pro services and Government – Local/State have low base numbers, so findings should be considered indicative only. Base numbers in chart.

Business consequences of ransomware

Recovery costs in healthcare

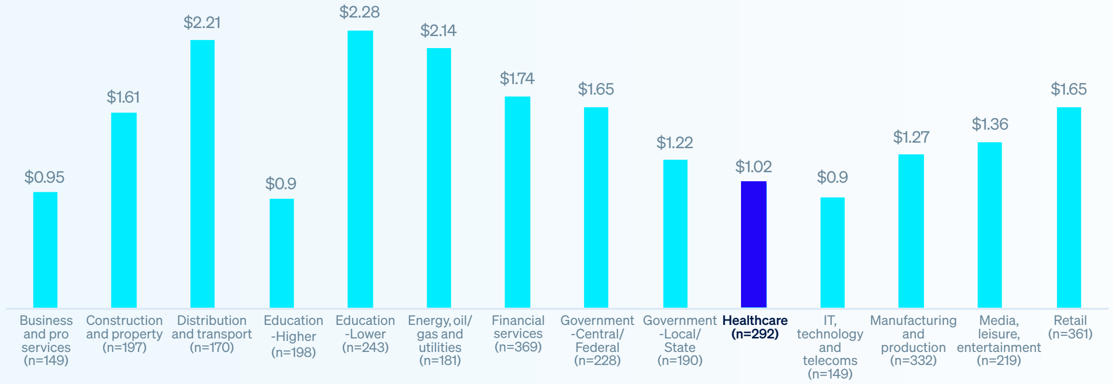
The average (mean) cost for healthcare providers to recover from a ransomware attack (excluding any ransom payment) has fallen to its lowest point in three years, dropping by 60% over the past year to $1.02 million, down from $2.57 million in 2024. It is also $1.18 million. lower than the sum reported in 2023.

2023	2024	2025
$2.20M	$2.57M	$1.02M

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? n=292 (2025), 271 (2024), 139 (2023)

When looking at an industry split, recovery varies considerably. **Lower education** providers reported the highest average cost to rectify incidents at $2.28 million. In contrast, both **higher education** providers and organizations within the **IT, technology and telecoms sector** equally reported the lowest cost at $0.90 million.

Chart 11: Ransomware recovery cost split by industry (USD, millions)

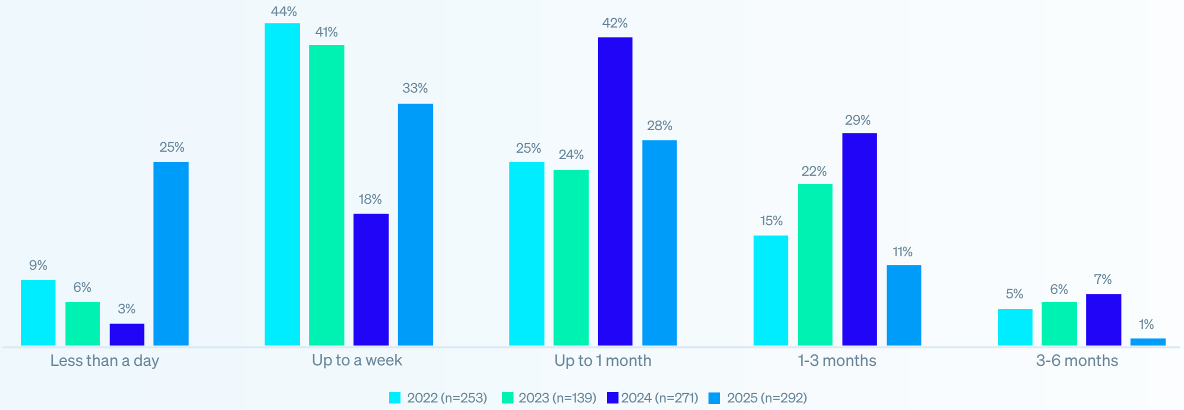


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

Recovery time in healthcare

The data reveals that, in 2025, healthcare providers are getting faster at recovering from ransomware attacks. 58% recovered within a week, nearly triple the 21% reported in 2024. At the same time, the proportion taking one to six months to recover fell sharply to 12%, down from 36% in 2024. Overall, 97% of healthcare victims fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

Chart 12: Recovery time for healthcare providers from ransomware attacks 2022 - 2025



How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Somewhat unsurprisingly, healthcare providers that had data encrypted typically were slower to recover than those that were able to stop the encryption: 9% that had data encrypted were fully recovered in a day, compared to 35% of those where the adversaries were unsuccessful in encrypting the data.

Human consequences of ransomware

The survey makes clear that having data encrypted in a ransomware attack has significant repercussions for IT/cybersecurity teams in the healthcare sector, with all respondents saying their team has been impacted in some way.

Chart 13: The consequences on IT/cybersecurity teams of having data encrypted

Cross-sector average	Healthcare	
40%	39%	Increased **pressure** from senior leaders
41%	37%	Increased **anxiety or stress** about future attacks
38%	35%	Change of **team priorities / focus**
34%	32%	Feelings of **guilt** that the attack was not stopped
37%	32%	Changes to team/ organizational **structure**
38%	31%	Ongoing **increase in workload**
31%	28%	Increased **recognition** from senior leaders
31%	28%	Staff absence due to **stress / mental health** issues
25%	19%	Our team's leadership was **replaced**

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team, if any? n=99.

Recommendations

Although healthcare providers have experienced several changes in their encounters with ransomware over the last year, it remains a significant threat. As adversaries continue to iterate and evolve their attacks, it’s essential that defenders and their cyber defenses keep pace with ransomware and other threats. Leverage the insights in this report to fortify your defenses, sharpen your threat response, and limit ransomware's impact on your business and people. Focus on these four key areas to stay ahead of attacks:

- **Prevention**. The most successful defense against ransomware is one where the attack never happens because adversaries couldn't breach your organization. Take steps to eliminate the technical and operational root causes highlighted in this report.
- **Protection**. Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- **Detection and response.** The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in-house, look to work with a trusted managed detection and response (MDR) provider.
- **Planning and preparation.** Having an incident response plan that you are well-versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to make quality backups and regularly practice restoring data from them to accelerate recovery if you do get hit.

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor, or visit www.sophos.com.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2025-10-03 WP (MP)