SOPHOS

THE STATE OF RANSOMWARE IN FINANCIAL SERVICES 2025

Findings from an independent survey of 369 IT and cybersecurity leaders in the financial services sector across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. November 2025

Introduction

Welcome to the fifth edition of the annual Sophos State of Ransomware in Financial Services report, which reveals the reality of ransomware for financial services providers in 2025.

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

Based on the real-world frontline experiences of 369 IT and cybersecurity leaders from the financial services sector, across 17 countries whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why financial services 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 369 financial services 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 financial services providers fall victim to ransomware

- **Exploited vulnerabilities** are the leading root cause of ransomware attacks on financial services providers, accounting for 40% of incidents. **Malicious emails** rank second (22%), while **credential-based attacks** follow in third, used in 17% of cases.
- Multiple operational factors contribute to financial services providers falling victim to ransomware. The most common factors are a **lack of protection** and **unknown security gaps**, cited by 44% of victims. They are followed in very close succession by both **poor-quality protection** and a **lack of expertis**e, which were contributing factors in 40% of attacks.

What happens to the data

- The **data encryption rate** in the financial services sector is at its second highest in five years, with 59% of attacks now resulting in data encryption, up from 49% in 2024.
- 31% of financial services providers that had data encrypted also experienced **data exfiltration**.
- 97% of financial services providers that had data encrypted were able to recover it.
- The use of **backups** by financial services providers to restore encrypted data is at its lowest rate in four years, used in 44% of incidents.
- 67% of financial services victims **paid the ransom** to get their data back–the highest rate recorded in this year's survey.

Ransoms: Demands and payments

- The **median ransom demanded** from financial services providers increased 50% over the past year to $3 million from $2 million in 2024, with the sector recording the highest demand across all industries surveyed. The primary factor behind this significant is a is largely driven by a 68% increase in demands between $1M and $5M over the last year, up from 19% of demands in 2024 to 32% in 2025.
- The **median ransom paid** by financial services providers increased by only 5%, rising from $2 million in 2024 to $2.1 million. Nevertheless, it is one of the highest fees reported in this year's survey.
- The **proportion of the ransom demand paid** by financial services providers increased to 92% in 2025 from 75% in 2024.
- Looking closely at **demands vs. payments**, close to a third (31%) of financial services providers said their payment matched the initial demand. 48% paid less than the initial ask, while 21% paid more.

Business impact of ransomware

- The average **cost for financial services providers to recover** from a ransomware attack dropped by a third (33%) over the last year, coming in at $1.74 million, down from $2.58 million in 2024 and $2.23 million in 2023.
- Looking at **speed of recovery**, financial services providers are recovering faster, with 57% recovered within a week in 2025, up from 46% in 2024.

Human impact of ransomware

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

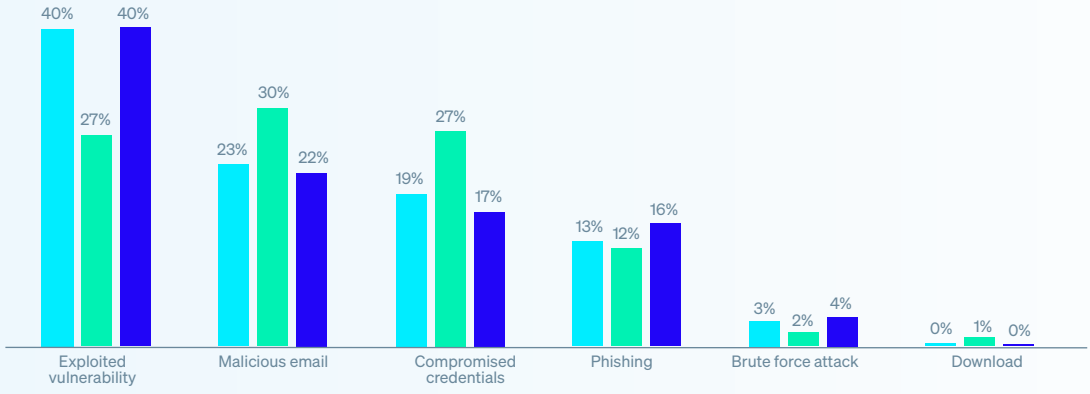
- 55% of providers reported a **change of team priorities/focus**.
- 51% of respondents cited **increased anxiety or stress** about future attacks as an impact on their IT/cybersecurity team.
- 43% experienced an ongoing **increase in workload**.
- 42% of IT/cybersecurity teams reported **increased pressure** from senior leaders, while 28% reported **increased recognition**.
- 40% reported changes to their **team/organizational structure**.
- Close to a third of respondents (31%) cited **feelings of guilt** that the attack was not stopped as a repercussion of the incident.
- 28% of teams experienced **staff absence** due to **stress/mental health** issues related to the attack.
- In nearly a quarter of cases (24%), the team's **leadership was replaced** because of the attack.

Why financial services providers fall victim to ransomware

Technical root cause of attacks in financial services

Financial services providers identified **exploited vulnerabilities** as the leading root cause of ransomware attacks, responsible for 40% of incidents. Malicious emails ranked second, with their share dropping from 30% in 2024 to 22% in 2025. **Credential-based attacks** continue to pose a significant risk, though reports dropped from 27% in 2024 to 17% in 2025.

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

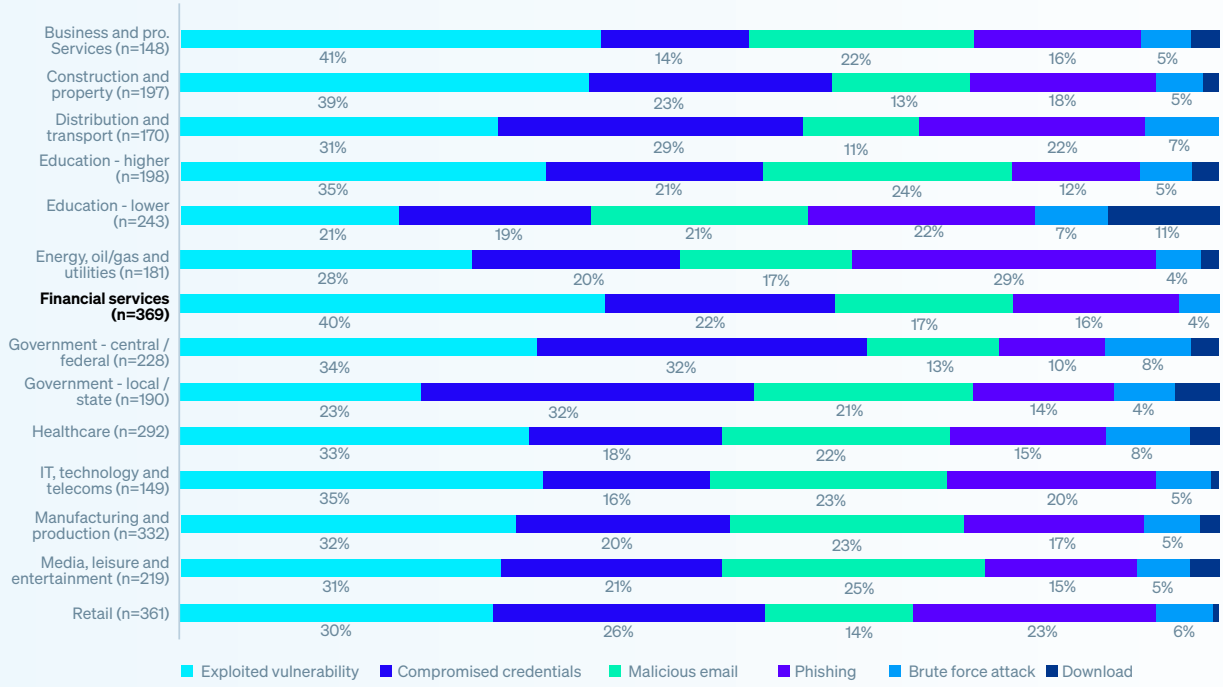


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=369 (2025), 387 (2024), 216 (2023).

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

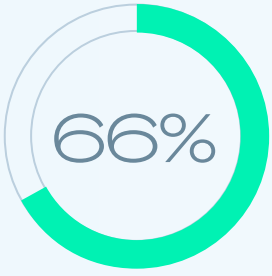


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

Organizational root cause of incidents in financial services

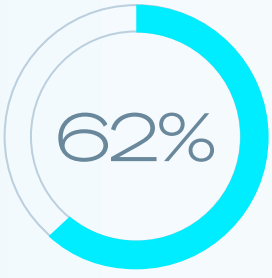
This year's report explores that, for the first time, the organizational factors that left financial services providers exposed to attacks. The findings reveal that victims in the financial services sector are typically facing multiple organizational challenges, with respondents citing three factors,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

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



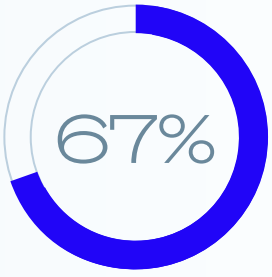
LACK OF/POOR QUALITY PROTECTION

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



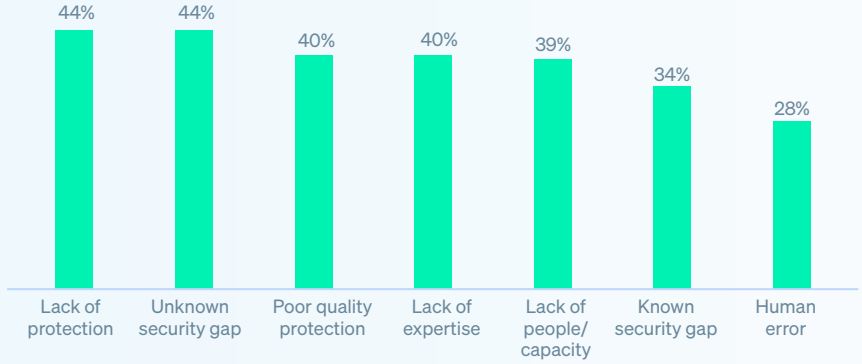
SECURITY GAP (KNOWN/UNKNOWN)

Had a known or unknown weakness in their defenses

Why do you think your organization fell victim to the ransomware attack? n=369. Consolidated responses.

Both a **lack of protection** (i.e., not having the necessary cybersecurity products and services in place) and **unknown security gaps** (i.e., a weakness in defenses that the organization were not aware of) were the joint most common individual reasons given, named by 44% of financial services respondents. These were closely followed by both **poor quality protection** (i.e. the cybersecurity products and services in place were not able to stop the attack) and a **lack of expertise** (i.e., insufficient skills or knowledge available to detect and stop the attack in time), which contributed to 40% of attacks.

Chart 3: Operational root cause of ransomware attacks on financial services providers

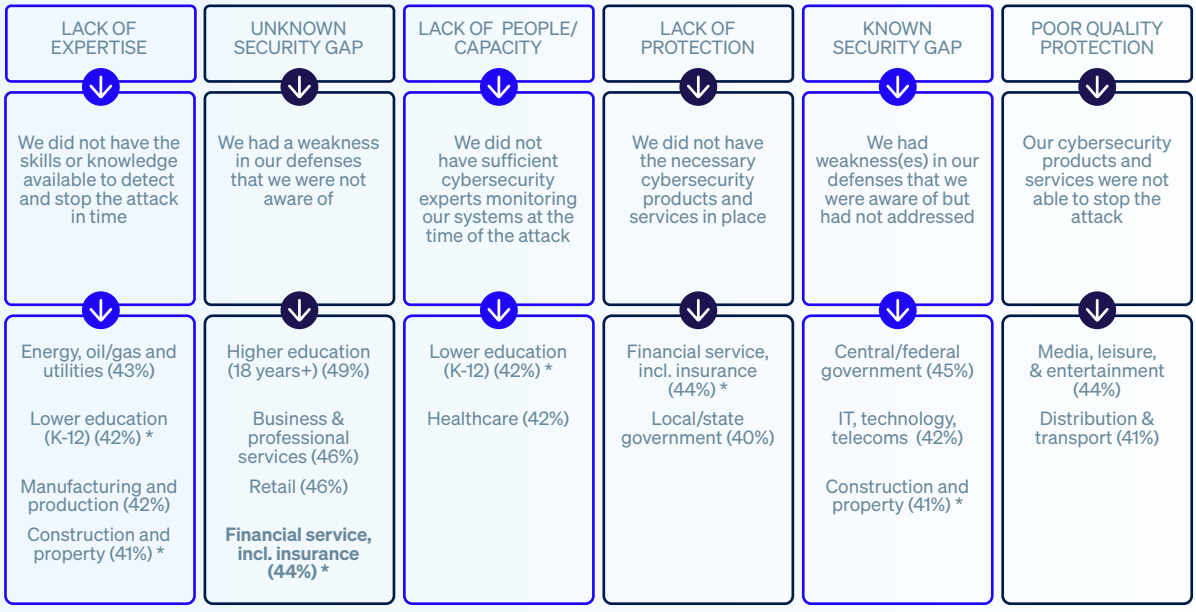


Why do you think your organization fell victim to the ransomware attack? n=369.

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



Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by industry. (* denotes two joint top root causes)

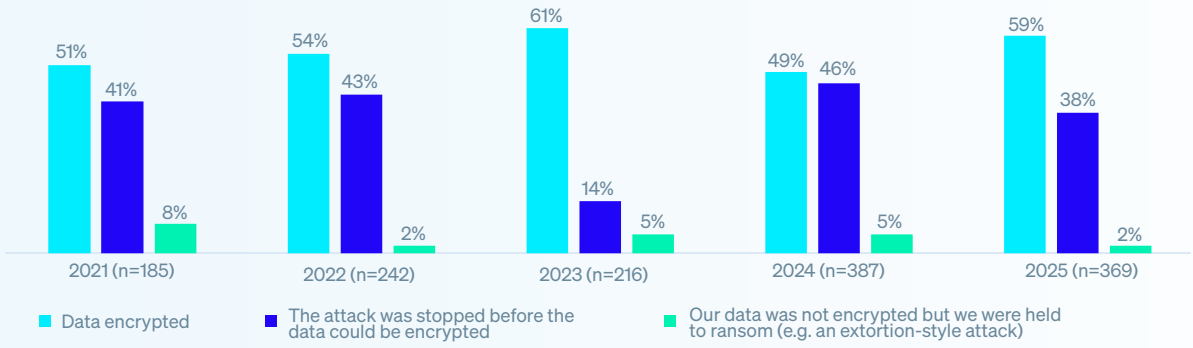
What happens to the data

Data encryption in financial services

Alarmingly, data encryption in the financial services sector has reached its second-highest level in five years, with 59% of ransomware attacks resulting in encrypted data — up from 49% in 2024.

At the same time, the proportion of attacks stopped before encryption could occur has declined to 38% from 46% last year, pointing to weakening ransomware defenses in the sector.

Chart 5: Data encryption rate in ransomware attacks on financial services 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

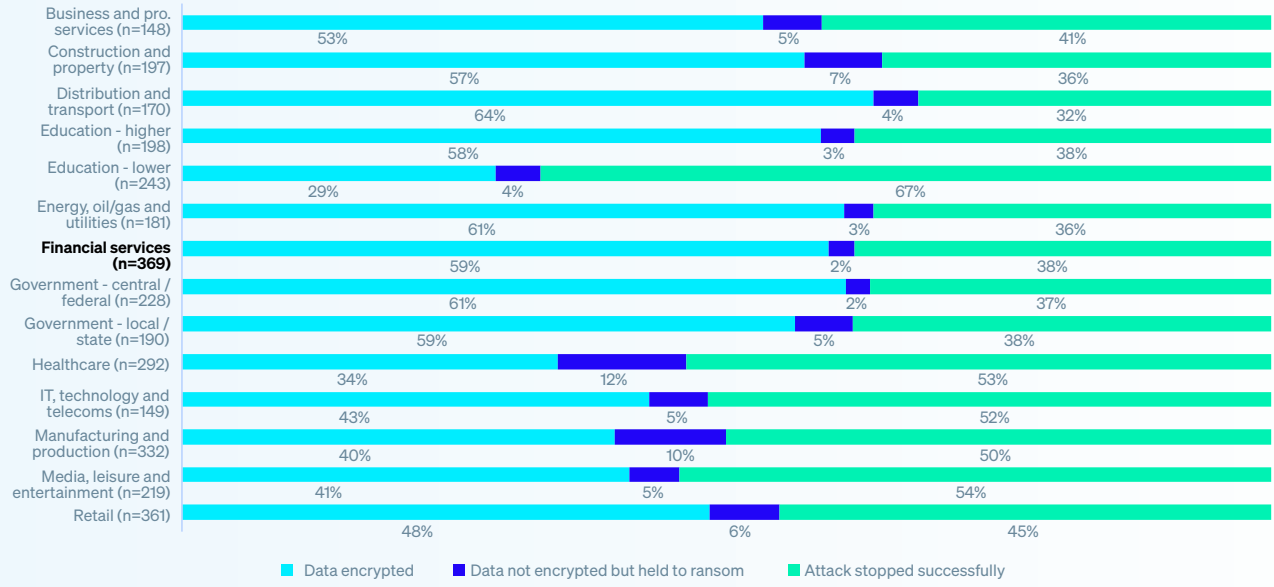
Organizations within the **distribution and transport** sector are most likely to have data encrypted (64%), indicating that organizations in this sector are less able to detect and stop the attack before encryption and/or are less able to block and roll back malicious encryption. In contrast, **lower 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 financial services sector, 18% of all ransomware victims and 31% of those that had data encrypted experienced data theft.

- 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 financial services providers that did not have data encrypted but were held to ransom anyway (extortion) fell to just 2% of attacks in 2025 from just 5% in 2023-24. While positive, this decline likely reflects the growing effectiveness of ransomware actors in successfully encrypting the data of organizations within the sector.

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.

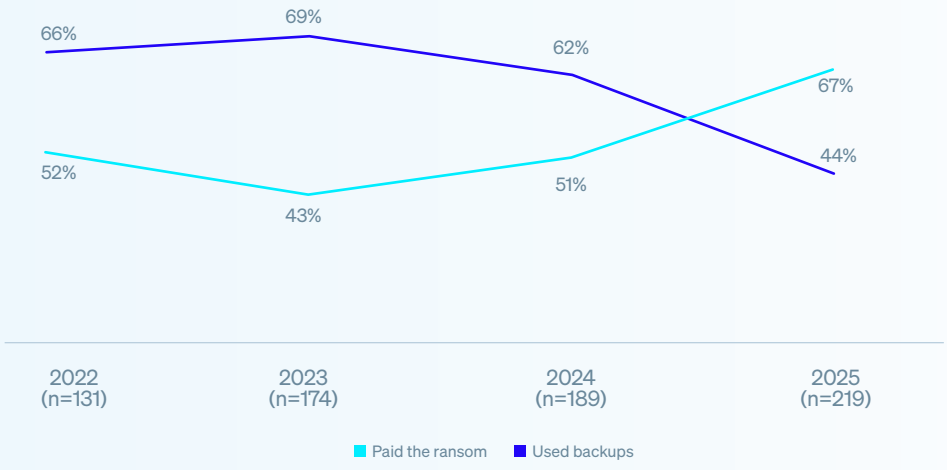
Recovery of encrypted data in financial services

97% of financial services providers that had data encrypted eventually recovered it.

In 2025, the proportion of financial services providers who **paid the ransom** to recover encrypted data increased significantly from 51% in 2024 to 67%, marking the highest rate reported in this year's survey. Meanwhile, **backup use** fell to a four-year low (44%, down from 62% in 2024).

For the first time in four years, more financial services organizations paid the ransom than recovered data using backups. This reversal highlights weakening resilience and a growing dependence on ransom payments for data recovery — likely driven by operational urgency, the high costs of disruption, and declining confidence in backup reliability.

Chart 7: Recovery of encrypted data in financial services 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

Financial services ransom demands

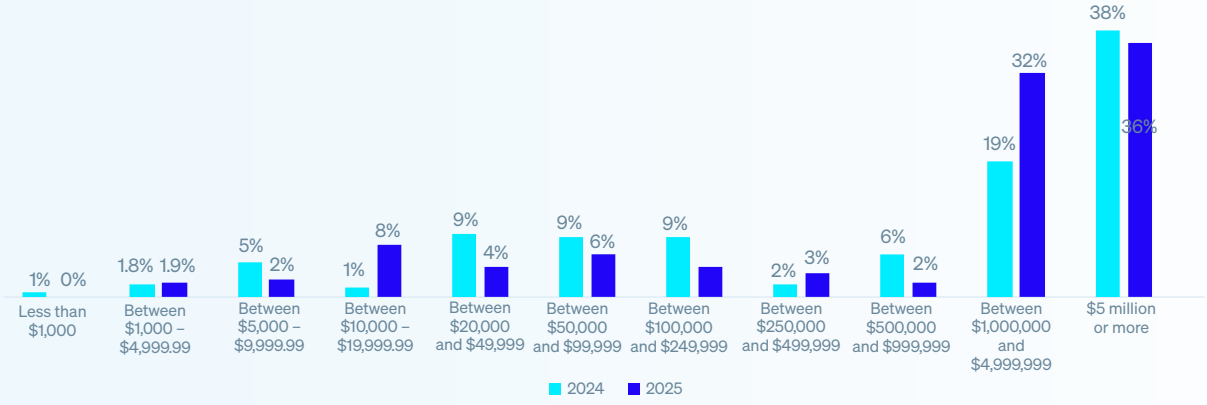
The average (median) ransom demand for financial services providers surged 50% over the last year, coming in at $3 million in 2025, up from $2 million in 2024. The increase is primarily driven by a 68% rise in demands between $1 million and $5 million over the past year, accounting for close to a third (32%) of demands in 2025, up from 19% in 2024.

Financial services ransom payments

Despite the surge in demands, the average (median) ransom paid by financial services providers rose just 5% from $2.0 million in 2024 to just $2.1 million in 2025, suggesting stronger resistance to pressure. However, the $2.1 million fee is among the highest reported in this year's survey.

Collectively, these findings suggest that while financial services organizations remain a prime target for high-value ransom demands, firms are showing greater resilience and resisting pressure. Yet, the persistently high payments highlight the sector's continued appeal to attackers and the need for stronger prevention and response capabilities.

Chart 8: Ransom payments in financial services | Distribution banding

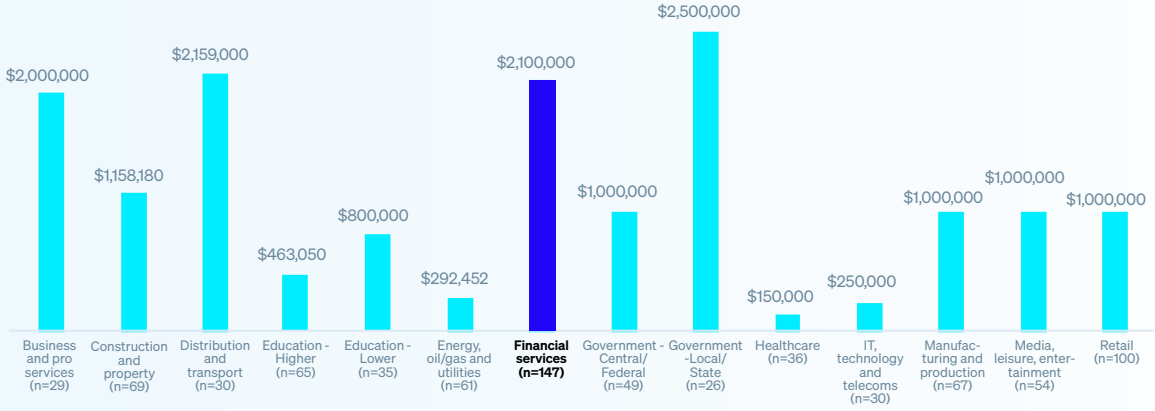


How much was the ransom payment that was paid to the attackers? n=147 (2025), 90 (2024)

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, **healthcare** providers paid the lowest, at just $150,000.

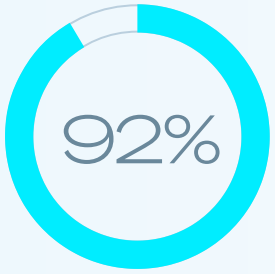
Chart 9: Ransom payments by industry



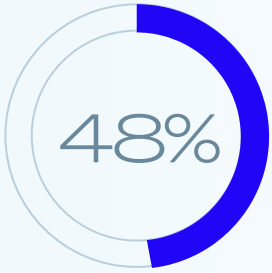
How much was the ransom payment that was paid to the attackers? Base numbers in chart. Note: Business and pro services and Government — Local/State have low base numbers, so findings should be considered indicative only.

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

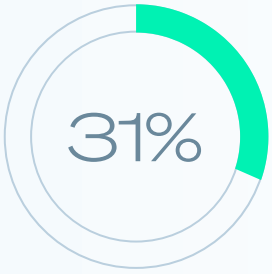
147 financial services providers that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 92% of the initial ransom demand — a notable increase from the 75% recorded in 2024. Overall, just under half (48%) paid less than the initial ask, 21% paid more, and 31% matched the initial demand.



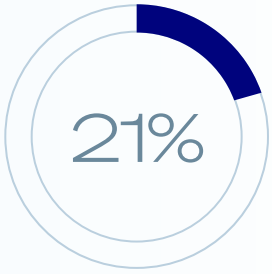
of the ransom demand **was paid**, on average



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

Why most ransom payments made by financial services providers differ from the amount initially demanded

This year, for the first time, we have explored why some financial services providers pay more than the initial demand and others pay less, shining new light on an important area when dealing with a ransomware attack.

31 financial services providers that **paid more** than the initial demand revealed that:

- 52%: The attackers got frustrated and increased the price.
- 48%: The attackers realized we are a high value target.
- 45%: Our backups failed or were malfunctioning.
- 42%: The attackers believed we could afford to pay more.
- 32%: We did not pay quickly enough, so the price went up.

Financial services providers typically cited two factors behind the decision to pay more, revealing the multiple challenges that victims face when trying to recover their data.

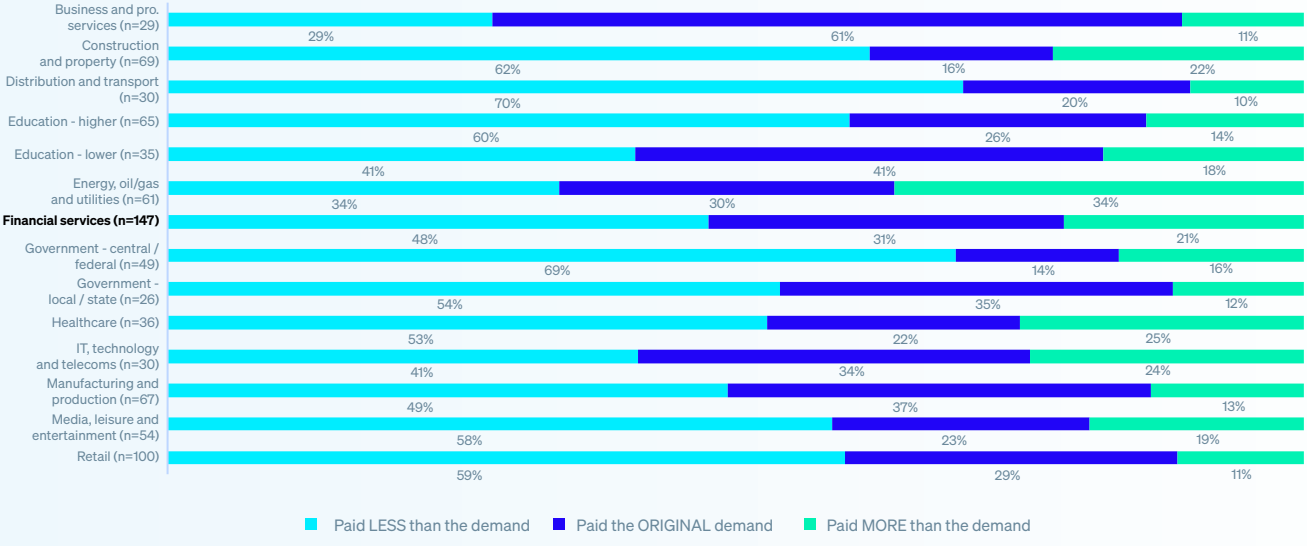
70 financial services providers that **paid less** than the initial demand explained how they were able to lower their payment:

- 49%: We paid the ransom quickly, so we got a discount.
- 47%: The attackers reduced their demand to encourage us to pay.
- 44%: We negotiated a lower amount with the attackers.
- 39%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement)
- 30%: A third party negotiated a lower amount with the attackers.

This cohort also reported, on average, two factors behind their lower ransom payment, further emphasizing the complex, multi-faceted situation that ransomware victims face.

Splitting the data by industry, we see that, encouragingly, in most 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 financial services

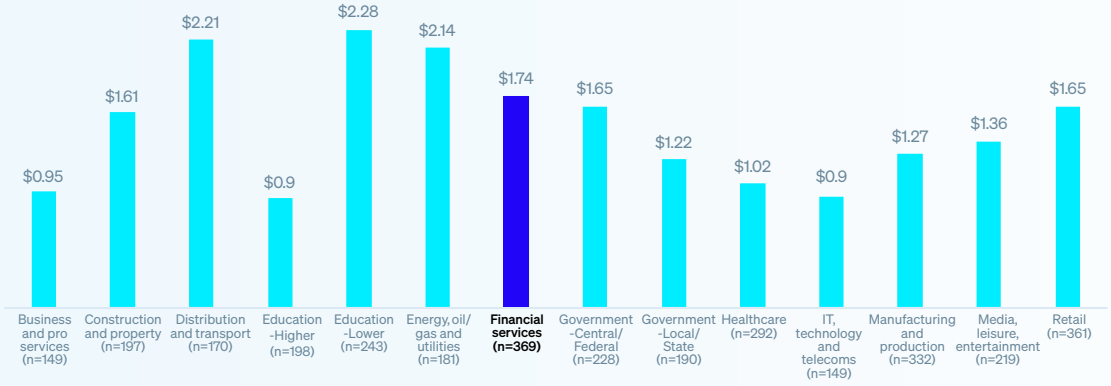
The average (mean) cost for financial services providers to recover from a ransomware attack (excluding any ransom payment) has fallen to its lowest point in three years, dropping by a third (33%) over the past year to $1.74 million, down from $2.58 million in 2024. It is also $0.49 million lower than the sum reported in 2023.

2023	2024	2025
$2.23M	$2.58M	$1.74M

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=369 (2025), 387 (2024), 216 (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

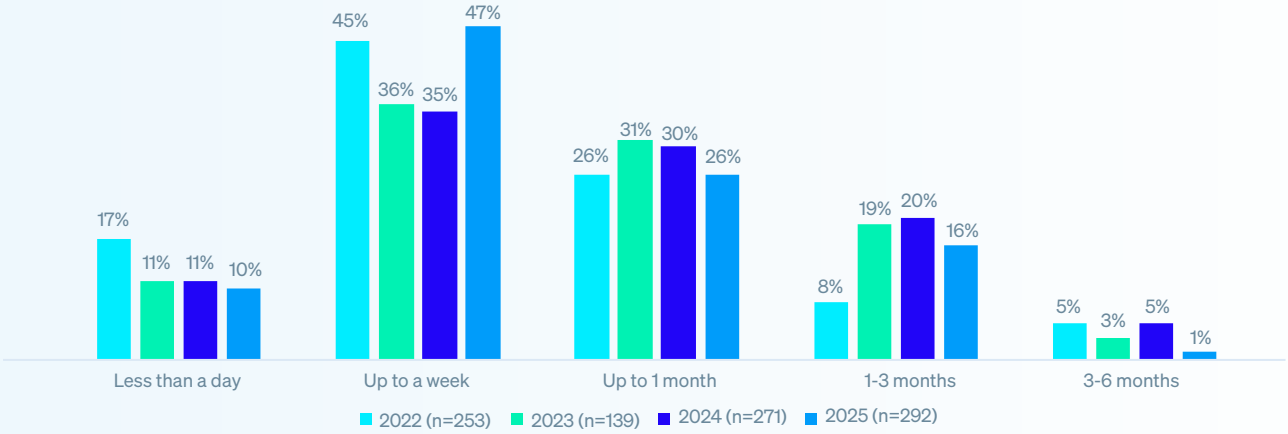


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

Recovery time in financial services

The data reveals that, in 2025, financial services providers are getting faster at recovering from ransomware attacks. 57% recovered within a week, up from the 46% reported in 2024. At the same time, the proportion taking one to three months to recover fell to 16%, down from 20% in 2024. Overall, 98% of financial services victims fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

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



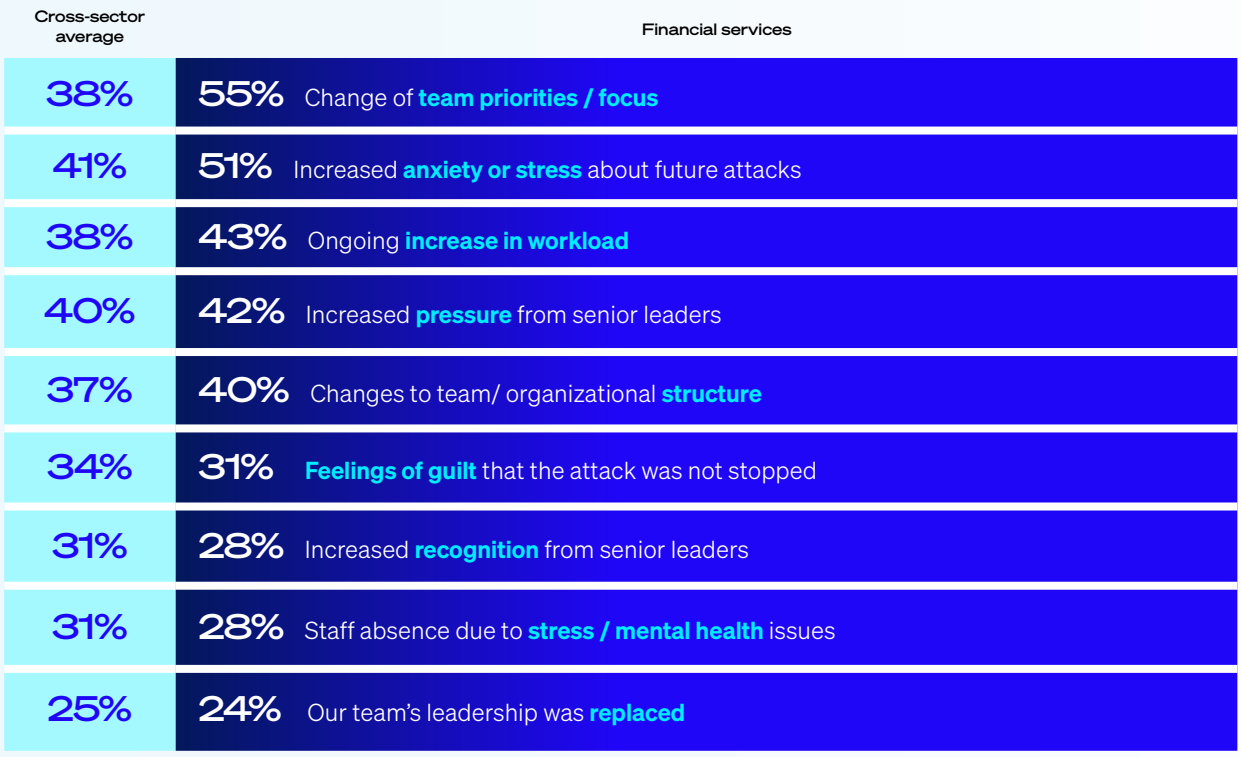
How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Somewhat unsurprisingly, financial services providers that had data encrypted typically were slower to recover than those that were able to stop the encryption: 6% that had data encrypted were fully recovered in a day, compared to 15% 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 financial services 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



What repercussions has the ransomware attack had on the people in your IT/cybersecurity team, if any? n=219.

Recommendations

Although financial services 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.

2025-11-18 WP (MP)

SOPHOS