

REPORT

The State of Ransomware in Financial Services 2026

Findings from an independent survey of 177 IT and cybersecurity leaders in the financial services sector across 17 countries whose organizations were hit by ransomware in the last year.

SOPHOS

Introduction

Welcome to the sixth edition of the annual Sophos State of Ransomware in Financial Services report, which reveals the reality of ransomware for financial services organizations in 2026. Throughout this report, "financial services" refers to a combined respondent group including general financial services, banking, and insurance.

This year's report shines new light on previously unexplored areas, including where attacks start in the environment, the defensive role of multi-factor authentication (MFA) and firewalls, and the connection between identity attacks and ransomware.

Drawing on the real-world experiences of 177 IT and cybersecurity leaders in financial services organizations hit by ransomware in the past year, this report offers unique insights into:

- Attack and defense methods
- Data encryption and recovery
- Ransom demands and payments
- Business and human impact

Note: The 177 financial services sector respondents are part of a broader cohort of 2,158 respondents across 15 industry sectors.

Throughout this report, "cross-sector average" refers to combined answers from respondents across all sectors surveyed. Percentages are rounded to the nearest whole number after summary combinations.

About the survey

This report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos. The survey asked questions about the organizational experiences of ransomware attacks and identity-based intrusions, tracking ransom payment rates, recovery costs, recovery times, and many other metrics year-over-year. Answers were gathered from January to March of 2026 and are based on respondents' experiences from the previous 12 months.

Participants came from 17 countries and 15 economic sectors, a wide range of industries across public and private sectors, and a bell-curve sampling of company sizes between 100 and 5,000 employees that has remained proportionally consistent over the survey's six-year history. All financial data points are in U.S. dollars.

Key findings

- **Identity-based approaches dominated how attacks began.**
  - Identity-based vectors (e.g., malicious email, phishing, compromised credentials, and brute-force attacks) initiated 85% of attacks against financial services, one of the highest rates above the 79% cross-sector average.
  - Financial services was the most likely sector to be breached by a brute-force attack (10%, versus 6% across all sectors).
  - However, it was among the least likely to be breached through an exploited vulnerability (12% of attacks, behind only energy, oil/gas, and utilities at 11%).
- **Financial services' ransomware attacks and most significant identity attacks were the same incident over half of the time.**
  - 58% of financial services victims said their ransomware attack was also their most significant identity attack, the lowest share of any sector and still a clear majority.
- **Known security gaps were the sector's defining operational root cause.**
  - 44% of financial services organizations attributed their breach to a known security gap they were aware of but had not addressed, the highest of any sector.
  - Combining known and unknown gaps, roughly 69% cited a security gap of some kind.
- **Double extortion is climbing in financial services.**
  - 21% of attacks encrypted data and also stole it, up from 18% in 2025 and 16% in 2024.
  - 59% of attacks succeeded in encrypting data.
- **Financial services negotiated the largest absolute reduction in ransom payments yet still paid more when compared to respondents across all sectors.**
  - Financial services victims negotiated ransom payment amounts down by a median of $64,000, the largest dollar reduction of any sector.*
  - The median ransom payment in financial services was 79% of the original demand, the third-deepest reduction of any sector.*
  - The median ransom demand for financial services was $1 million versus the $698,000 cross-sector median.
  - The median ransom payment was $1.07 million versus the $769,000 cross-sector median.
- **Recovery costs are down YoY, but the cost floor is higher than most sectors.**
  - Year-over-year, the average (mean) recovery cost for financial services eased from $1.74 million in 2025 to $1.5 million in 2026.
  - Financial services had a lower mean recovery cost than the cross-sector average, but a higher median, meaning this sector is more likely to face a costly recovery than other sectors, but less likely to face a ruinous one.
- **Financial services took a week longer to recover compared to last year's survey.**
  - The mean recovery time for financial services was 3.79 weeks (up from 2.72 in 2025) and was the second slowest among all sectors.
  - Just 42% recovered within a week, compared to the 55% all-sector average.
- **The anxiety for IT and security teams was the highest in the study.**
  - 52% of financial services teams reported increased anxiety or stress about future attacks, the highest percentage among all sectors.

** Sectors with fewer than 30 respondents that paid the ransom were excluded from comparisons.*

Attack and defense methods

Root causes of attacks

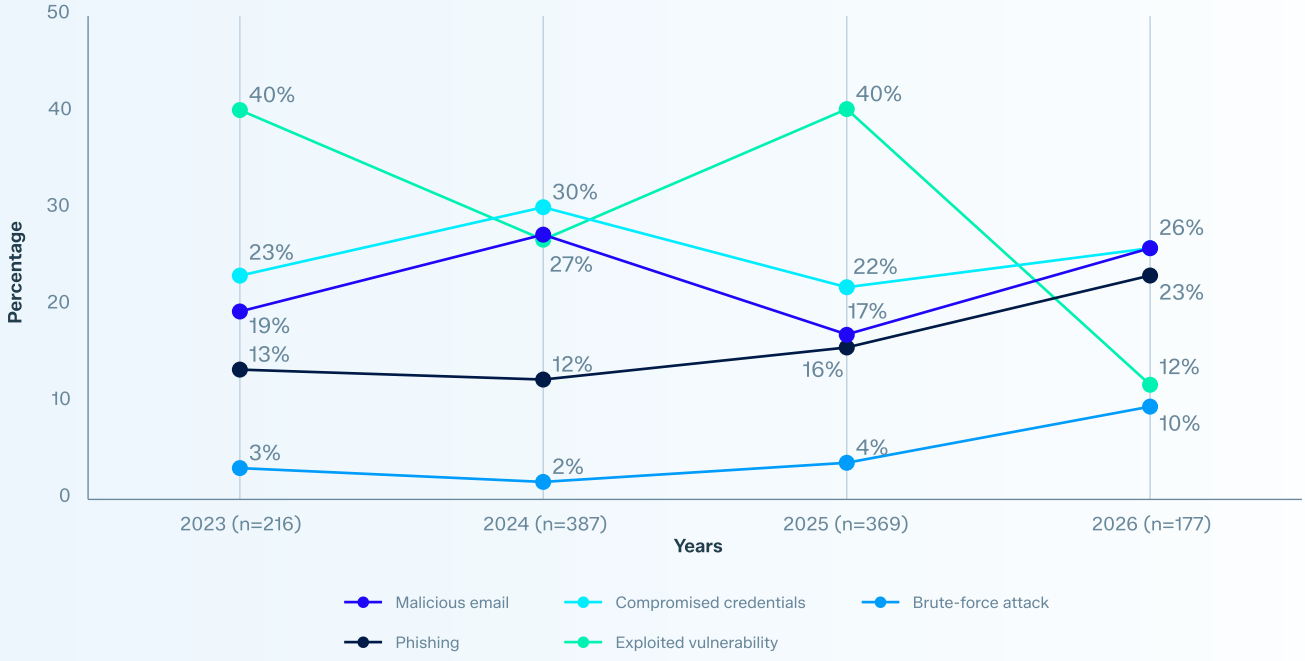
This year's financial services data reflects the same shift seen across all sectors: identity-based attacks are growing.

Malicious email and compromised credentials were the joint-leading technical root causes in financial services, each at 26%, with phishing close behind at 23%. Exploited vulnerabilities dropped sharply to 12%, down from 40% in the 2025 report, a steeper decline than the cross-sector trend from 32% (2025) to 18% (2026).

10%

The percentage of financial services attacks that began with a brute-force attempt, the highest of any sector surveyed.

Technical root cause over time: Financial services

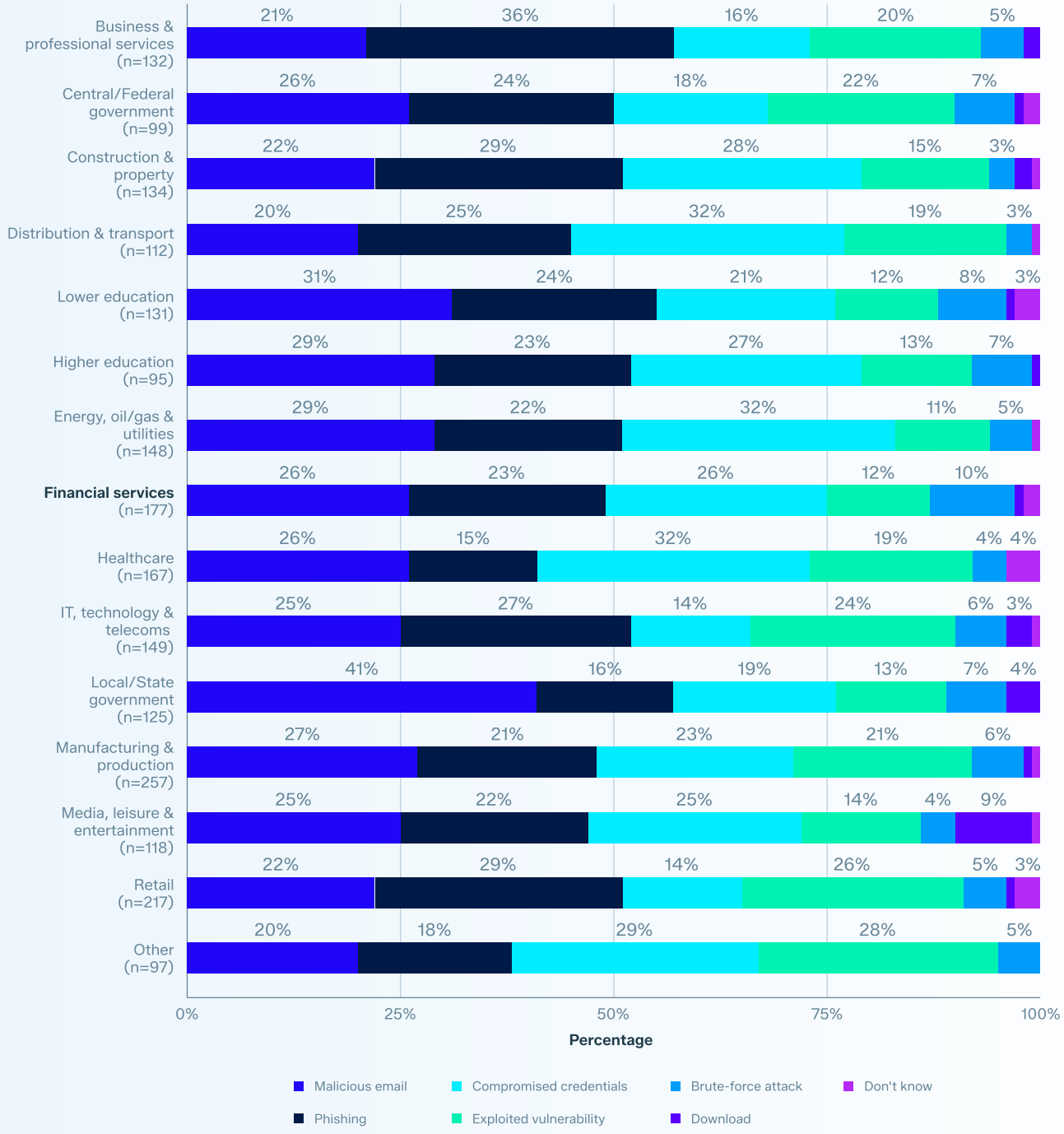


Do you know the root cause of the ransomware attack your organization experienced in the last year? "Downloads" and "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

One vector runs against the sector's otherwise low exploit profile. **Financial services was the most likely sector in the survey to be breached through a brute-force attack (10%, versus 6% across all sectors)**, but it sat near the bottom of the field
on exploited vulnerabilities (12%, the second lowest among all sectors).

Taken together, **identity-based vectors (e.g., malicious email, phishing, compromised credentials, and brute-force attacks) accounted for 85% of attacks on financial services**. In other words, roughly six in seven attacks against the financial services sector began with an identity-based approach, reinforcing why identity security is central to its defenses.

Technical root cause by industry (2026)

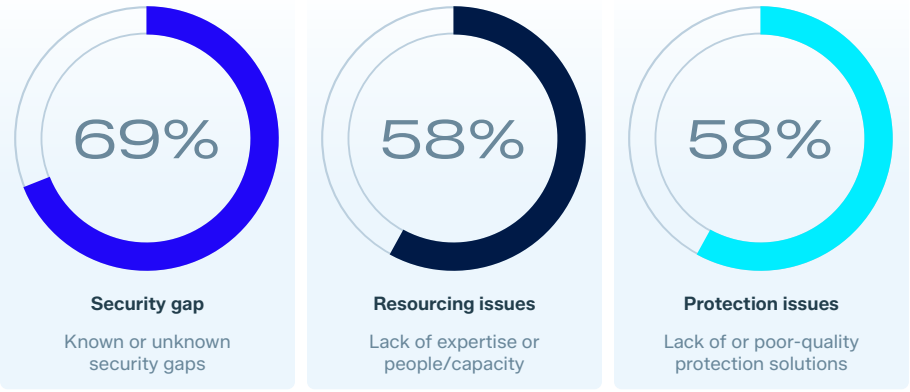


Do you know the root cause of the ransomware attack your organization experienced in the last year? Percentages in this chart rounded using the largest remainder method and may differ from percentages in the report text. Base numbers in chart.

Financial services reflects the broader cross-sector shift toward more email-borne attacks and fewer reports of exploited vulnerabilities. However, Sophos experts expect exploits to climb again as organizations struggle to keep up with patches for vulnerabilities found by frontier AI.

What made organizations vulnerable

Financial services providers cited a broad mix of challenges with protection, resourcing, and security gaps. Across the three consolidated categories, security gaps led at 69%, followed by resourcing issues (58%) and protection issues (58%).



Why do you think your organization fell victim to the ransomware attack? n=177. Consolidated responses.

The most common operational root cause for financial services was known security gaps: 44% attributed their breach to a known security gap that the organization had not closed. **Financial services had the highest known security gap percentage of any sector**, exceeding the 36% cross-sector average by eight percentage points.

The sector also struggled with unknown security gaps, attributing 41% of breaches to that operational root cause, versus the 36% cross-sector figure.

44%

The percentage of financial services victims who cited a known security gap (a weakness they were aware of but had not addressed), the highest of any sector surveyed.

Operational root causes: Financial services vs. all sectors

Operational root cause	Financial services (n=177)	All sectors (n=2,158)
Known security gap	44%	36%
Unknown security gap	41%	36%
Lack of protection	40%	36%
Lack of people/capacity	34%	35%
Poor quality protection	34%	33%
Human error	33%	35%
Lack of expertise	33%	35%

Why do you think your organization fell victim to the ransomware attack? Multiple responses permitted. Base numbers in chart.

Financial services' weaknesses clustered in security gaps, along with some shortfalls in having the necessary cybersecurity products and services in place. The sector didn't have any expertise or capacity gaps that were worse than respondents across all sectors.

The table below shows sectors placed in the column of the operational root cause they cited most.

Top operational root cause of ransomware attacks by sector



Why do you think your organization fell victim to the ransomware attack? Multiple responses permitted. Sectors tied across multiple causes are marked with an asterisk (*). n=2,158.

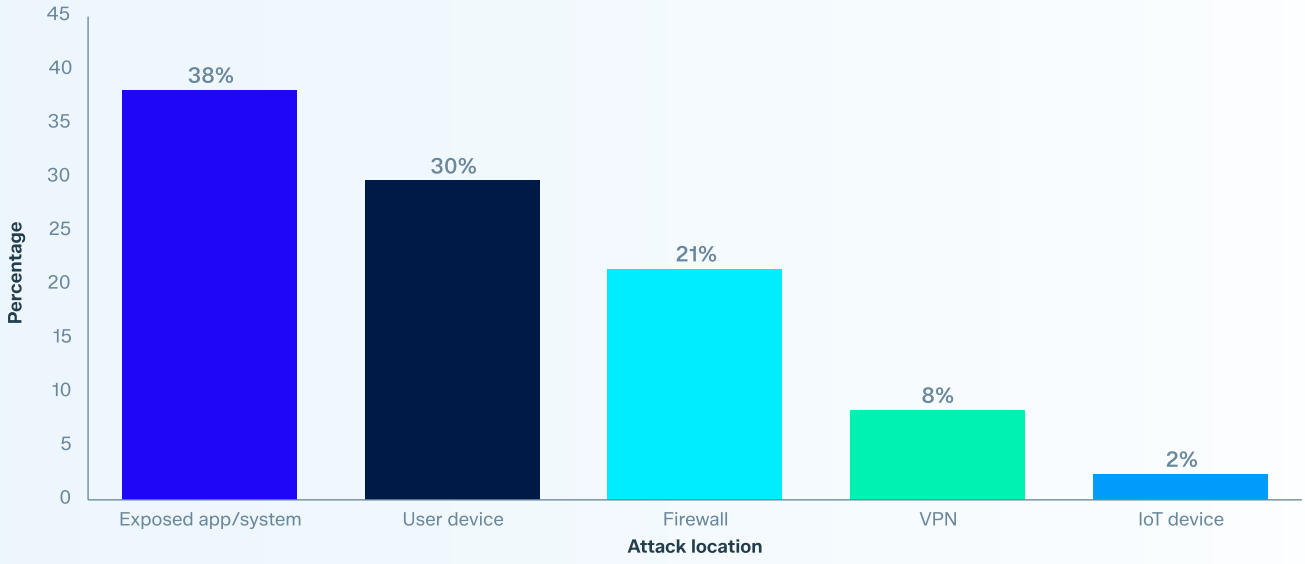
NEW RESEARCH

Where attacks start

New research this year dives into where in the environment attacks began, specifically among incidents that started with an exploited vulnerability, compromised credentials, or a brute-force attack.

For financial services, exposed applications and systems were the most common entry point (38%), followed by user devices (30%) and firewalls (21%).

Where ransomware attacks start: Financial services



You said the root cause was an exploited vulnerability, compromised credentials, or a brute-force attack. Where did this happen in your environment? n=84.

The prominence of exposed applications aligns with the broader shift toward cloud and SaaS environments, where internet-facing systems present a large and growing attack surface.

NEW RESEARCH

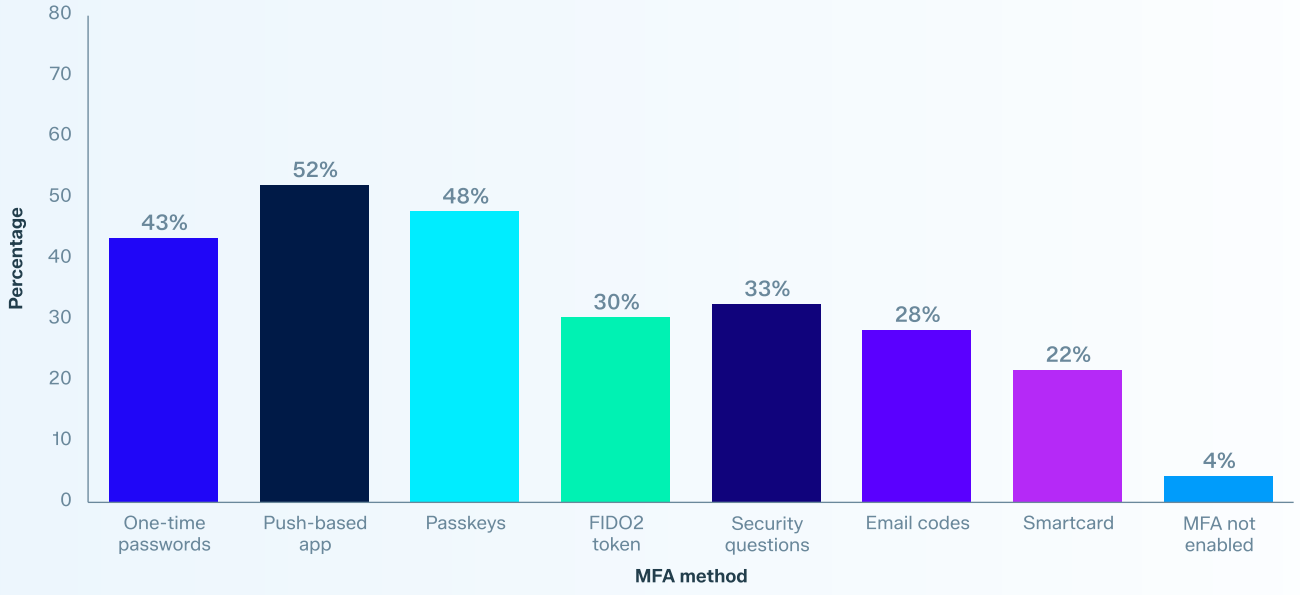
The role of multi-factor authentication (MFA)

We also examined the MFA methods in place at the time of the attack among financial services providers whose attack began with compromised credentials. Almost all victims had some form of MFA enabled (96%) in credential-based attacks.

However, among financial services providers asked about MFA, **70% still had data encrypted despite MFA enablement**. This suggests that either MFA was not comprehensively deployed across all critical systems, attackers found ways to bypass MFA protections, or the attack vectors did not rely solely on credential compromise.

Push-based applications (52%) and passkeys (48%) were the most frequently deployed methods for the sector. When compared to other industries, the slightly lower usage of one-time passwords (43%) and slightly higher usage of security questions (33%) is notable.

The role of MFA: Financial services



What type of multi-factor authentication was enabled at the time of the attack, if any? Multiple responses permitted. Base: the attack occurred due to compromised credentials. n=46.

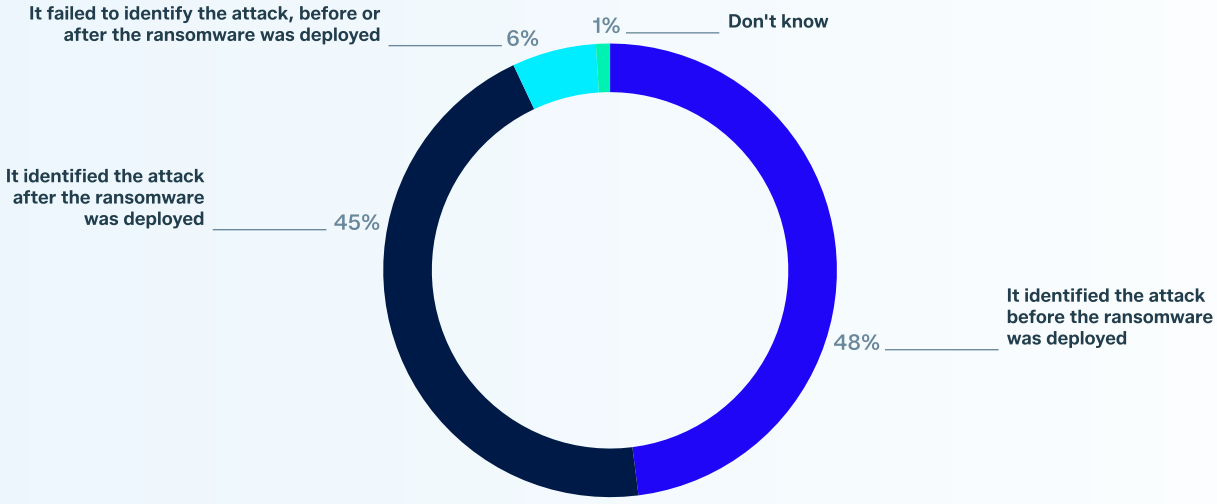
NEW RESEARCH

The role of firewalls

48% of financial services organizations said their firewall identified the attack before the ransomware was deployed, 45% said it identified the attack afterward, and 6% said it did not identify the attack at all.

Against the cross-sector average (61%, 32%, and 7%), the financial services sector detection skews noticeably toward the “after” column.

The role of firewalls: Financial services



What role did your firewall play in identifying the attack? n=177.

Among those early-detection cases, victims in financial services still had their data encrypted 53% of the time. Firewalls are doing a good job of collecting data to identify attacks, but attacks still aren't being stopped at the same rate they're being identified. It is likely that firewalls often log the data needed to detect and stop an attack, but they may not be connecting deeply enough with other systems to recognize the threat and respond in time.

NEW RESEARCH

The identity-ransomware connection

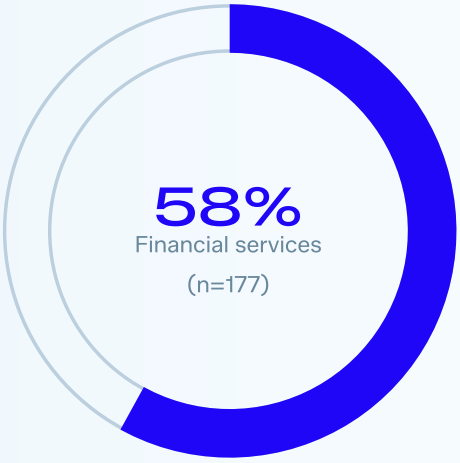
One of the survey's clearest findings is the direct link between identity attacks and ransomware. Across all sectors, two-thirds of ransomware victims (67%) confirmed the incident was the same event as their most significant identity attack. Financial services had the lowest share of these overlaps of any sector, but their rate still exceeded half of all ransomware attacks.

Still, these findings point to a more broadly targeted attack surface in finance and insurance.

58%

The share of financial services victims whose ransomware incident was the same event as their most significant identity attack.

Ransomware attack was also their most significant identity-related attack



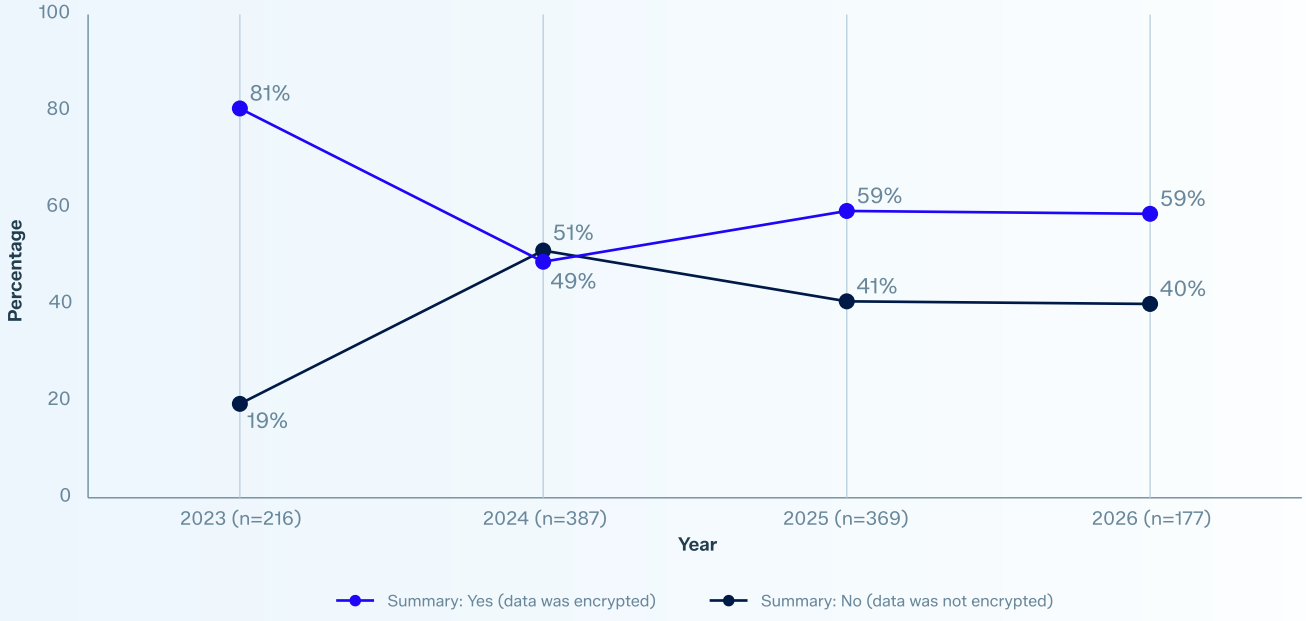
Was that ransomware incident the same event as your most significant identity-related attack? Base: organizations hit by ransomware. n=177.

Data encryption and recovery

Data encryption rate

Financial services' encryption picture has held steady for two years. 59% of attacks succeeded in encrypting data, which is unchanged since the 2025 report. In 2024, the rate was closer to a 50/50 chance of encryption.

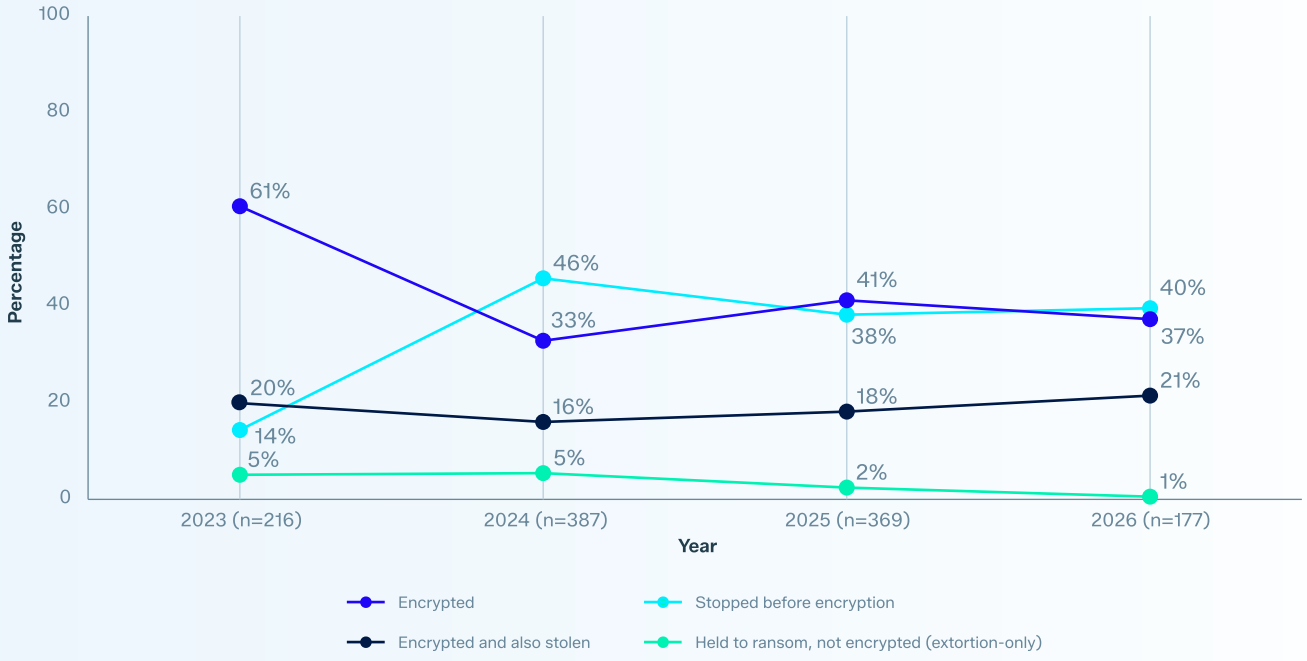
Data encryption summary (Yes/No) over time: Financial services



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Summarized Yes / No answers. "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

While the overall encryption rate held steady, the mix of encryption types shifted. The survey asks respondents if their data was just encrypted, or encrypted and stolen in the same attack. **The proportion of attacks where data was encrypted and stolen (sometimes referred to as a "double extortion attack") rose to 21% of all financial services attacks, up from 18% in 2025**. However, the overall encryption rate has stayed at 59% because encryption-only attacks fell from 41% in 2025 to 37% this year.

Data encryption rate over time: Financial services



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? "Don't know" answers excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

In double extortion attacks, the stolen data gives attackers a second point of leverage, a costly dynamic for a data-rich, heavily regulated sector where stolen records carry outsized regulatory and reputational cost. Double extortion attacks have been trending up for two years in a row, from 16% in 2024 to 18% in 2025, and finally hitting 21% in 2026. The double extortion rate for financial services is also above the 16% cross-sector rate.

Extortion-only attacks (where data is held to ransom without encryption) were negligible at 1%, down from 2% in 2025.

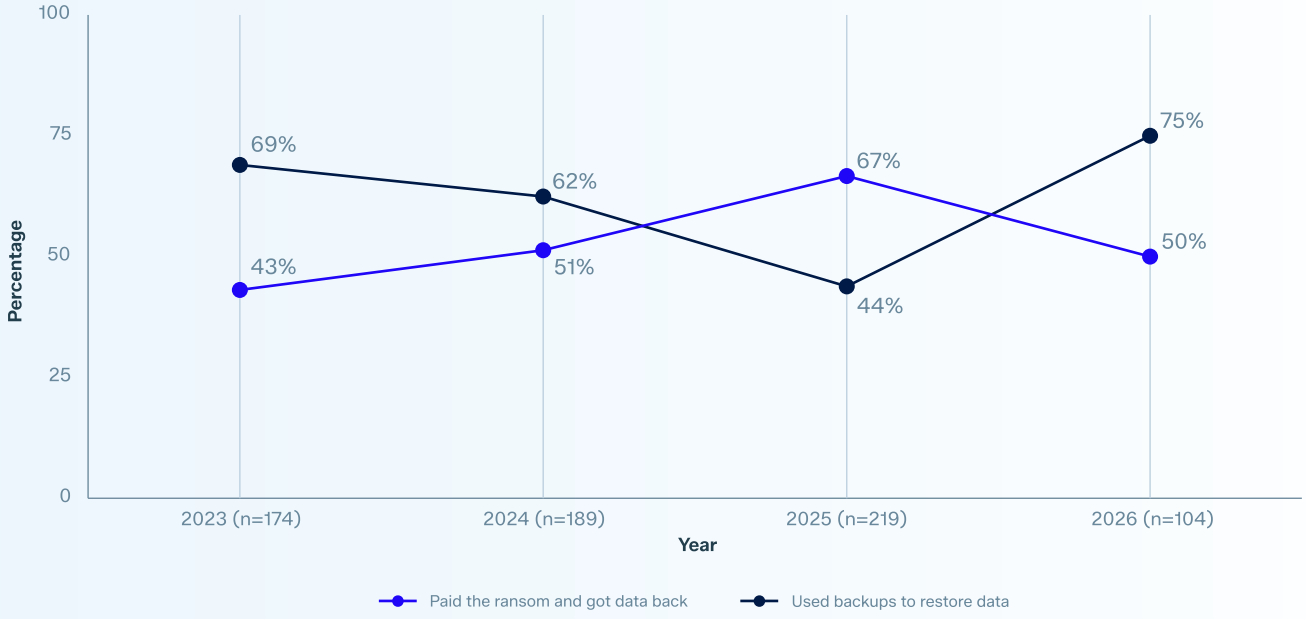
How organizations recovered encrypted data

Backups were financial services' most-common recovery route in 2026. **75% of financial services providers restored data from backups**, above the 66% cross-sector rate and a sharp rebound from 44% in 2025. That return to backups points to renewed investment in the sector's recovery infrastructure and a growing ability to resist ransom demands.

75%

3 out of 4 financial services organizations restored encrypted data from backups in 2026, above the 66% cross-sector rate.

Data recovery methods over time: Financial services



How did your organization get the data back? Base: organizations that had data encrypted. Multiple responses permitted. Base numbers in chart.

At the same time, half (50%) paid the ransom and got data back, down from 67% in 2025. With backup restoration rising and payment-based recovery falling, the financial services sector is recovering more on the strength of its own capabilities than on the attackers' cooperation.

Ransom demands and payments

Ransom demands

Financial services faced steeper ransom demands than organizations across all industries. The median demand was $1 million, above the $698,000 median for all sectors. The distribution skewed high: **53% of demands were for $1 million or more, and 26% were for $5 million or more**, compared with 46% and 23% respectively across all industries.

Note: Outlier ransoms of $40 million or more were removed from this data.

Median ransom demand

	2025	2026
Financial services	$3.00M (n=217)	$1.00M (n=103)
All sectors	$1.32M (n=1,700)	$0.70M (n=1,214)

How much was the ransom demand from the attacker(s)? Base: organizations that had data encrypted. Base numbers in chart.

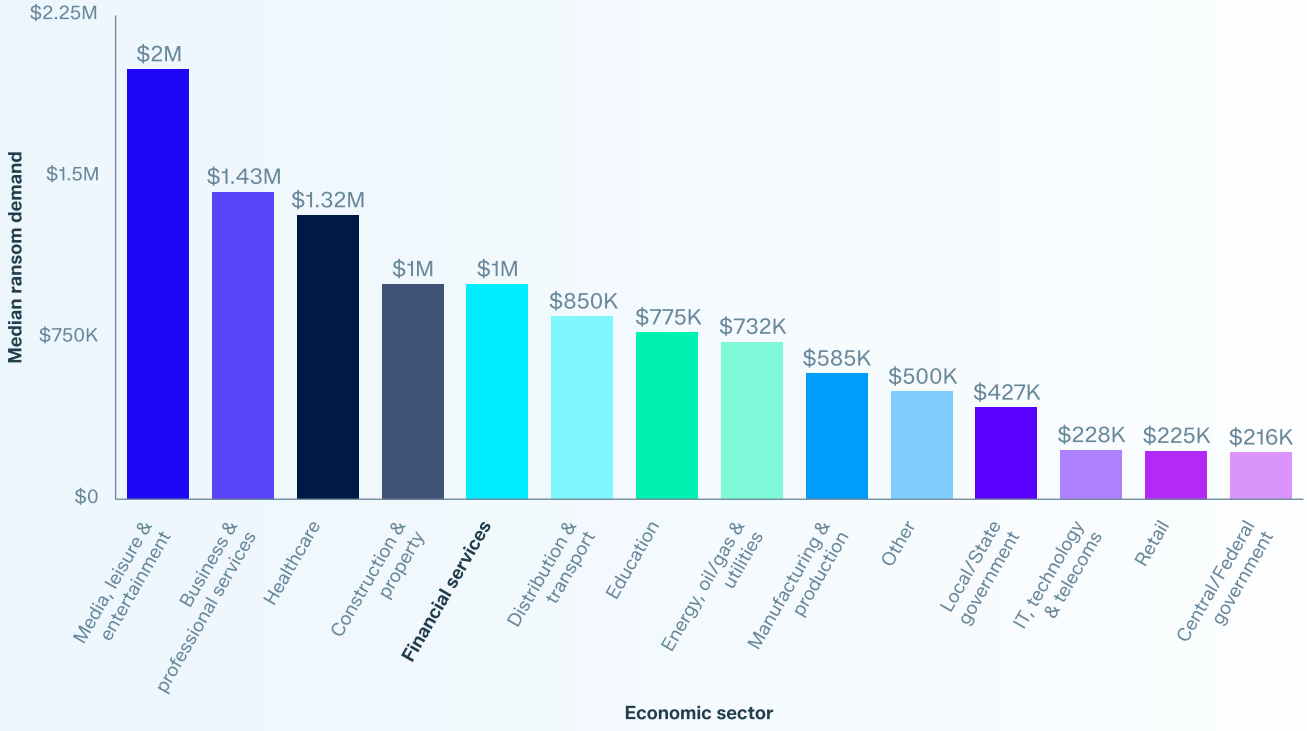
Against other sectors, financial services has some of the highest ransom demands. At $1 million, its median demand trails only media, leisure and entertainment ($2 million), business and professional services ($1.43 million), and healthcare ($1.32 million) sectors, and runs well above lower-demand sectors like retail ($225,000) and central government ($216,000). It's in a tie with construction and property ($1 million).

$1M

Financial services' median ransom demand. More than half of all financial services ransom demands were for $1 million or more.

Financial services is seen as a high-revenue, heavily regulated sector holding highly sensitive data, which may give attackers more leverage when they set an opening demand.

Median ransom demands by sector



How much was the ransom demand from the attacker(s)? Base: organizations that had data encrypted. n=1,214.

The good news for financial services is their steep year-over-year decline in the ransom demand amount. Financial services' median demand fell from $3 million in 2025 to $1 million in 2026. With a median demand of $2 million in 2024, the three-year trend is also down.

Ransom payments

Financial services' higher demands were matched by higher payments. **The median ransom payment was $1.07 million, above the $769,000 cross-sector median**. Payments clustered high: 57% were $1 million or more (versus 44% across all industries) and 21% were $5 million or more (versus 16% cross-sector).

Median ransom payment

	2025	2026
Financial services	$1.50M (n=147)	$1.07M (n=52)
All sectors	$1.00M (n=847)	$0.77M (n=587)

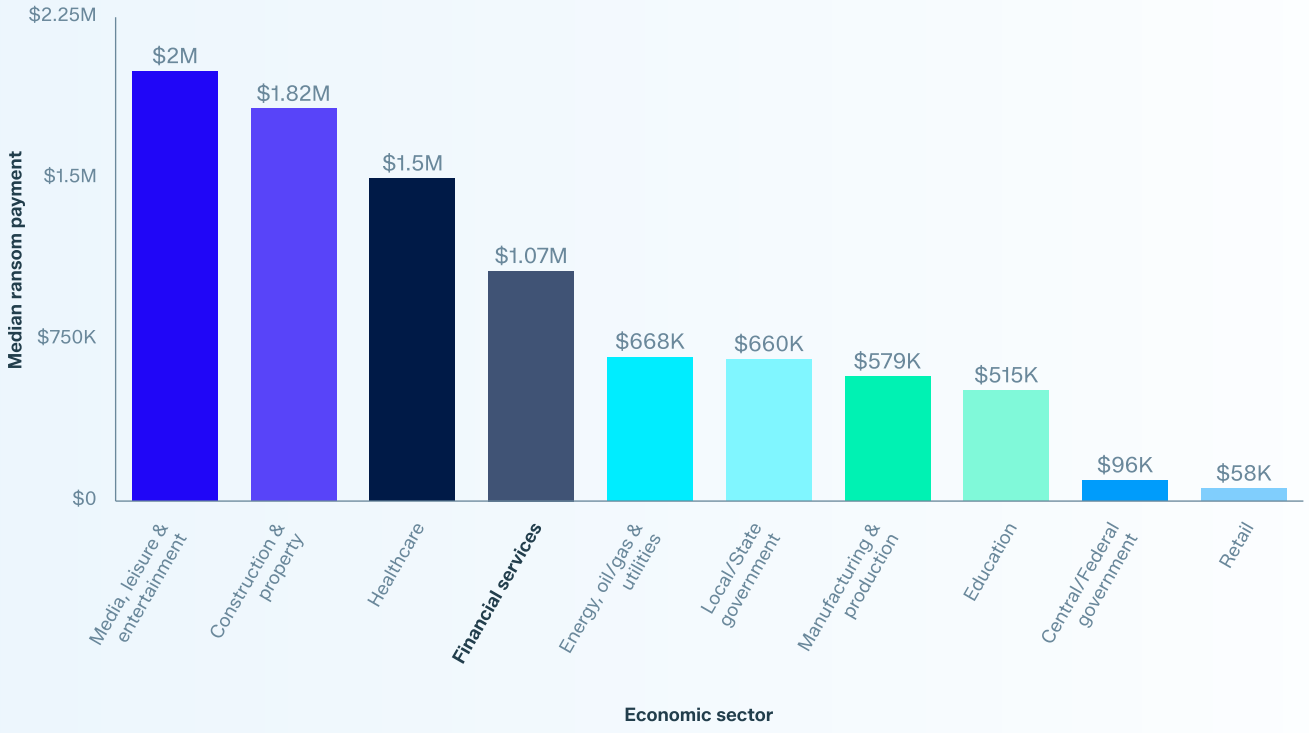
Approximately how much was the ransom payment paid to attackers? Base: organizations that paid the ransom. Base numbers in chart.

When financial services pays, it tends to pay more than other sectors. At $1.07 million, its median payment trails only media, leisure and entertainment ($2 million), construction and property ($1.82 million), and healthcare ($1.5 million) sectors, and runs well above lower-payment sectors like central government ($96,000) and retail ($57,500).

$1.07M

Financial services' median ransom payment.

Median ransom payments by sector



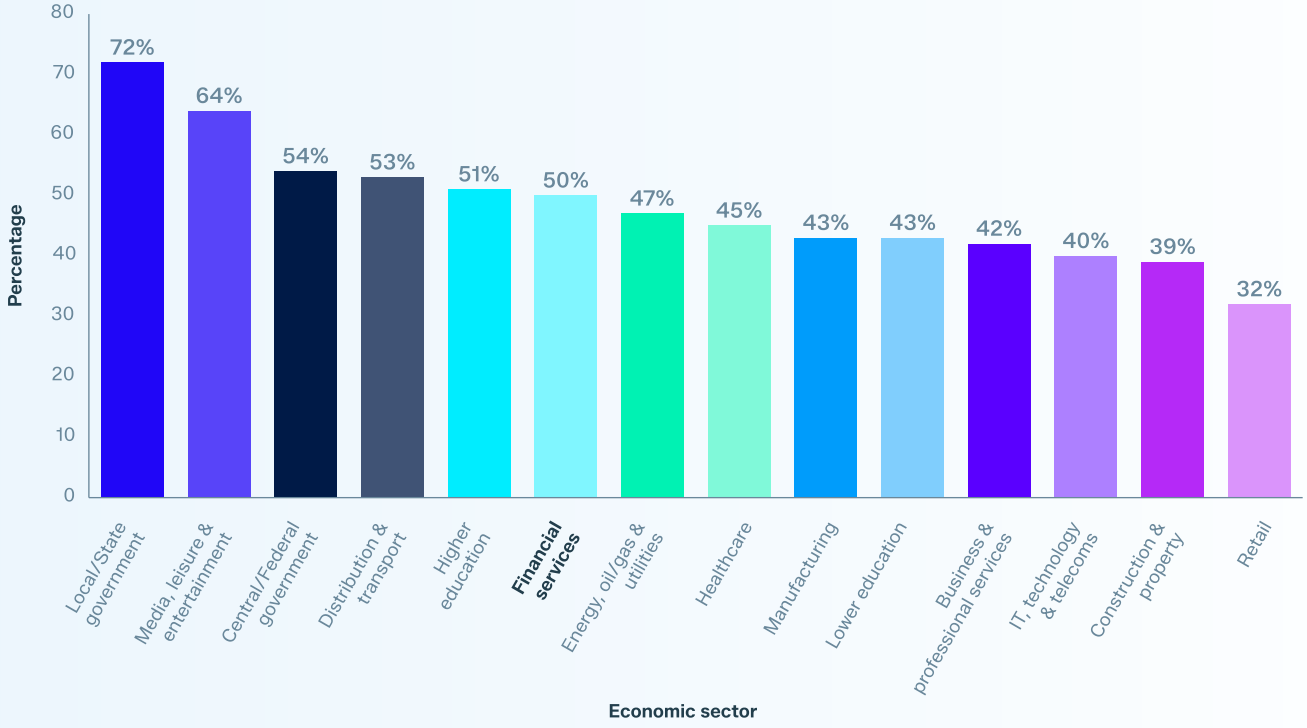
Approximately how much was the ransom payment paid to attackers? Base: organizations that paid the ransom. n=587. Excludes sectors with fewer than 30 respondents to this question.

Year-over-year, the median payment eased from $2.2 million in 2024, to $1.5 million in 2025, to $1.07 million in 2026. This followed the trend for organizations across all sectors, from $2 million in 2024, to $1 million in 2025, to $769,000 in 2026.

Ransom payment rates, by sector

Half of financial services victims (50%) paid the ransom and got their data back. There was an additional 1% portion of financial services that paid the ransom and did not get their data back. This was a rare outcome for all sectors.

Percentage who paid the ransom and got data back, by sector



Did your organization get any data back? Answer: Yes, we paid the ransom and got data back. Base: organizations that had data encrypted. n=1,214.

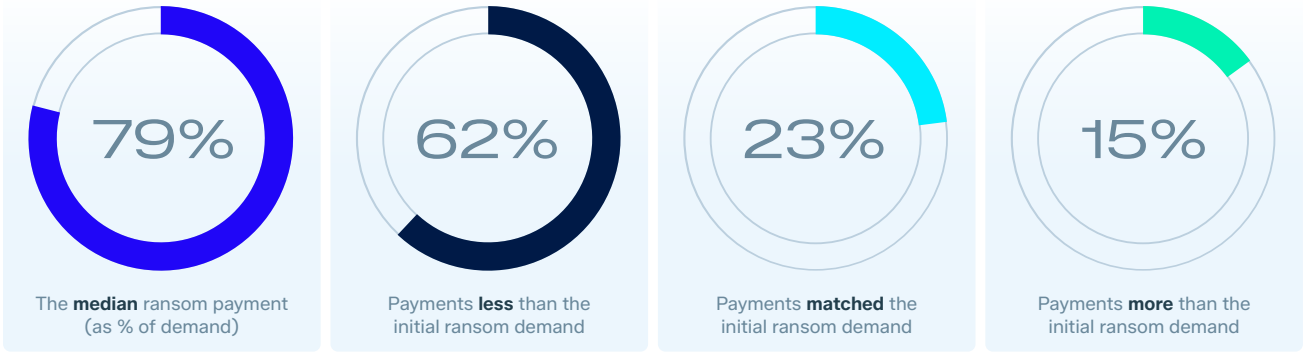
Actual payments versus initial demands

Among financial services organizations that paid their ransoms, the median payment was 79% of the original demand, the third-lowest percentage of any sector. In absolute ransom reduction numbers, **the financial services sector negotiated attackers down by a median of $64,000. That was the largest dollar reduction below the demand of any sector** with more than 30 respondents that paid the ransom.

62% of financial services organizations paid less than the initial demand, 23% paid exactly what was demanded, and 15% paid more. The 62% rate of lower payments was the third-highest among all sectors.

The pattern points to a sector with the leverage, playbooks, and negotiation experience to discount a ransom meaningfully rather than pay the first demand amount.

Actual payment vs. initial demand: Financial services



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? Base: organizations that shared both ransom demand and payment. n=48.

Business and human impact

Ransomware recovery costs

Financial services' recovery costs tell a two-sided story. **The average (mean) cost to rectify a ransomware attack, excluding any ransom paid, was $1.5 million. That mean is below the $1.7 million cross-sector average** and among the lowest average recovery costs of any sector.

Yet the median cost was $750,000, double the $375,000 cross-sector median. The sector has a higher floor (fewer cheap recoveries, so the median cost is roughly double the all-sector median) and a lower ceiling (no multi-$10 million outliers) compared to recoveries across all sectors.

Financial services costs sit in a tighter, more predictable mid-to-upper band of ransomware recoveries. In practice, financial services is more likely to face a costly recovery than most of the other sectors, but less likely to face a ruinous one.

Average (mean) recovery cost

	2025	2026
Financial services	$1.74M (n=369)	$1.50M (n=177)
All sectors	$1.53M (n=3,400)	$1.70M (n=2,158)

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack? Base numbers in chart.

Year-over-year, the mean eased from $1.74 million in 2025 to $1.5 million in 2026, even as the cross-sector average rose from $1.53 million to $1.7 million.

$750K

Financial services' median recovery cost.

Average (mean) vs. Median:

The average (mean) is the total of all responses divided by the number of respondents. The median is the middle value, with half of responses above and half below. Averages can be skewed by a few unusually high or low figures, while the median shows the most typical response recorded.

Recovery time

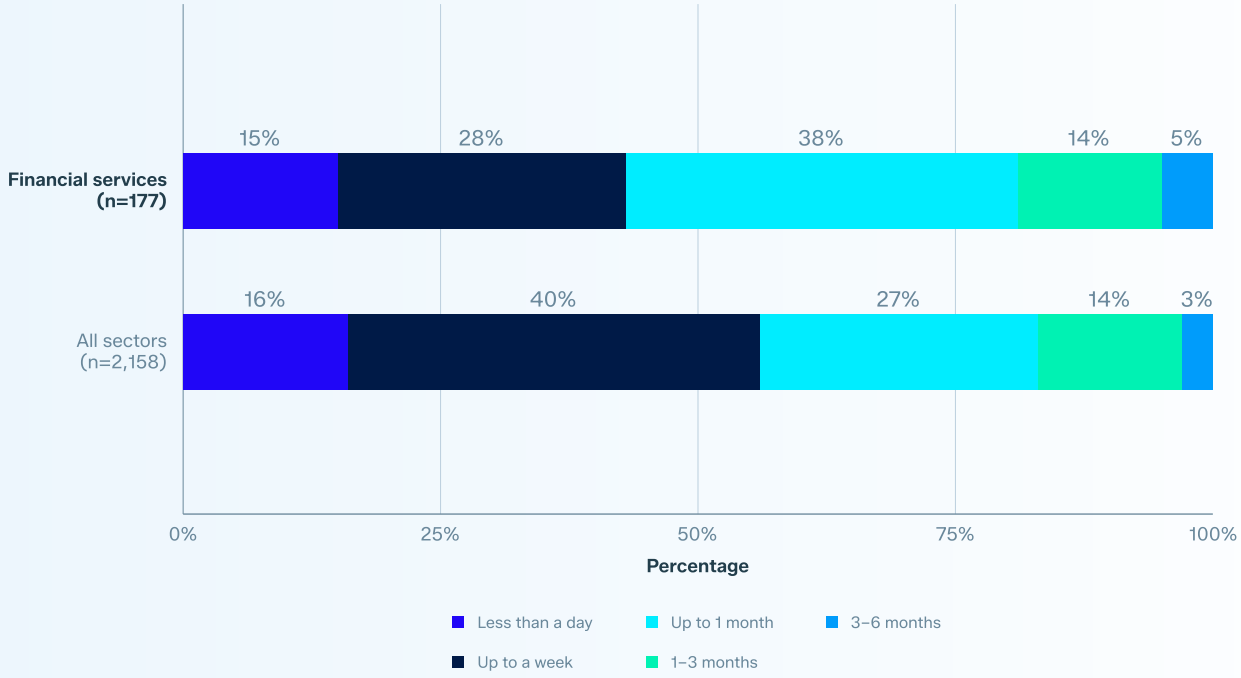
Financial services took longer to recover than the average sector. **The mean time to fully recover was 3.79 weeks, nearly a full week longer than the 2.80-week cross-sector average and the second slowest among all sectors** behind only the healthcare sector.

42% of financial services organizations recovered within a week, versus 55% across all sectors. 38% took between one week and a month to fully recover, the highest of any sector for that band of recovery times.

3.79 weeks

The average time financial services took to fully recover from a ransomware attack, the second slowest among all sectors.

How long it took to recover from ransomware



How long did it take your organization to fully recover from the ransomware attack? Percentages in this chart rounded using the largest remainder method and may differ from percentages in the report text. Base numbers in chart.

Year-over-year, recovery time has increased by over a week, with financial services recoveries taking an average of 2.72 weeks in 2025. One possible factor behind this jump in recovery time is the sector's rebound in backup use, since rebuilding and validating systems from backups typically takes longer than paying the ransom and running a decryption key across systems left in place.

Human impact of ransomware

The human toll on financial services IT/cybersecurity teams after a ransomware attack was heavier in many areas when compared to all other industries. **More than half (52%) reported increased anxiety or stress about future attacks, the highest percentage among all sectors** and roughly 11 points above the 41% cross-sector rate.

Other pressures in financial services ran above the cross-sector average too: 42% cited increased pressure from senior leaders, 38% had an ongoing increase in workload, and 38% saw changes to team or organizational structure.

52%

The proportion of financial services IT/cybersecurity teams that reported increased anxiety or stress about future attacks, the highest of any sector.

Human impact of ransomware

Repercussion	Financial services (n=104)	All sectors (n=1,214)
Increased anxiety or stress about future attacks	52%	41%
Increased pressure from senior leaders	42%	40%
Ongoing increase in workload	38%	31%
Changes to team/ organizational structure	38%	32%
Change of team priorities/focus	34%	32%
Increased recognition from senior leaders	32%	36%
Staff absence due to stress/ mental health issues	29%	29%
Feelings of guilt that the attack was not stopped	28%	31%
Team's leadership was replaced	27%	21%

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team? Base: organizations that had data encrypted. Base numbers in chart.

Leadership turnover was also elevated, with 27% of financial services teams seeing their leadership replaced after the attack, compared with 21% across all sectors.

Recommendations

Strengthen identity security as a ransomware defense. Although financial services was the sector least likely to report that its ransomware incident and most significant identity attack were the same event (58%), identity-based approaches still initiated 85% of its attacks, above the 79% cross-sector rate. And 58% is still over half of the sector's respondents. That's why financial services and every other sector should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Enable MFA comprehensively, specifically phishing-resistant MFA. The survey showed that 96% of financial services providers with compromised credentials had enabled MFA in some capacity at the time of their attack, yet 70% still had data encrypted. MFA alone is not enough to stop attacks, and it needs to be comprehensively enabled rather than left on for the SaaS apps that force it and off for VPN logins, firewall admin consoles, and legacy apps.

Strengthen endpoint protection against AI-discovered exploits. Even though reports of exploited vulnerabilities fell to 12% in this report, Sophos experts expect exploits to climb again. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Bring in specialist support or MDR. Financial services' operational weaknesses are concentrated in security gaps rather than skills, but the resourcing burden is real. 58% cited a resourcing issue: a lack of expertise or people and capacity. Dealing with AI-augmented threats will put even more strain on these areas as security teams try to stay current with fast-changing AI technology. Unless you can confidently staff a security operations team in-house, look to an external specialist to fill the gap, either a 24/7 MDR vendor or a managed services provider. Vendors that resolve more incidents end-to-end with AI and automation act as a force multiplier that helps close skills and capacity gaps.

Invest in backup and recovery infrastructure. Backups were the dominant recovery route for financial services (75%). They should be tested regularly, stored offline or in immutable formats, and integrated into a documented incident response plan that can be executed under pressure.

Maintain exposure management programs. Financial services was the most likely sector to attribute its breach to a known security gap (44%), so closing the loop between awareness and remediation is the highest-value move here. Providers should maintain aggressive patching cadences and focus on mitigations including segmentation, zero trust network access, and MFA/continuous authentication deployments.

Reduce exposure via the firewall and leverage firewall telemetry to detect attacks early. Firewalls identified most attacks, but detection often landed late: only 48% of financial services firewalls identified the attack before the ransomware was deployed, and even among early-detection cases, victims still had their data encrypted 53% of the time. Ensure your firewall receives rapid, ideally automated, updates and minimize internet-facing services like admin access and user portals. Connect firewalls to XDR and MDR so firewall telemetry helps detect ransomware attacks before payloads deploy. A cybersecurity defense system, where controls share signal, is the answer.

Recommended actions at a glance:

- Segmentation to slow attackers down
- ZTNA to replace legacy VPNs and contain app exploits
- Identity threat detection and response (ITDR) to harden identity infrastructure
- Phishing-resistant MFA as the destination rather than the starting line
- Disciplined patching of internet-facing devices
- 24/7 detection and response

Conclusion

The State of Ransomware in Financial Services 2026 Report reveals a threat landscape in transition.

There are signs of progress: median ransom demands fell sharply year over year, backup-based recovery surged to 75%, and average recovery costs sit below the cross-sector average.

At the same time, the challenges that remain are significant. Nearly six in ten ransomware attacks against financial services still succeed in encrypting data, double extortion is climbing, and the sector's median recovery cost is double the cross-sector median **while recovery takes longer than almost any other sector**.

Although the sector was the least likely to report that its ransomware incident and most significant identity attack were the same event, 85% of its attacks still begin with an identity-based approach, so identity infrastructure is still a high-leverage place to invest.

Financial services providers also need to prepare for the defining cybersecurity challenge of the next decade: AI-augmented threats. The data already hints at why: 69% of financial services organizations cited a security gap as an operational root cause, and it was the sector with the highest rate of known security gaps at 44%. Both known and unknown gaps become more consequential as AI accelerates the speed and scale of attacks, with adversaries using AI to find weaknesses faster and orchestrate attacks on multiple control points at machine speed.

There's a deeper signal in this year's root-cause data, too. The perceived root-cause mix is equalizing; across all sectors, no single vector dominates. This is especially true for financial services, where two different technical root causes were tied for the top spot, and brute-force attacks (which were very low in most sectors) were unusually high in financial services. That makes focusing defenses too narrowly on any one entry method risky, because attackers are succeeding through multiple vectors.

The pattern across this year's findings, especially in the late timing of firewall detection and the limited effect of MFA enablement on outcomes, points in a consistent direction: when defenses operate in isolation, you're not protected. Closing the gap on AI-era attacks will depend less on adding more tools and more on connecting the ones already in place, so context, detection, and response can move at the speed the threats now demand.

The financial services organizations that will fare best against ransomware in the years ahead are those that sustain executive attention on this issue while adopting integrated, AI-driven defensive systems, investing not only in technology and processes but in the people who defend against these threats every day.

SOPHOS

To learn more about ransomware and how Sophos can help you defend your organization, visit our website.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

© Copyright 2026. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2026-10-19 EN (TA)