



# THE STATE OF RANSOMWARE IN ENTERPRISE 2025

Findings from an independent survey of 1,733 IT and cybersecurity leaders in enterprise organizations that were hit by ransomware in the last year.

# Introduction

Welcome to the inaugural Sophos State of Ransomware in Enterprise report, which reveals the reality of ransomware for enterprise (1000+ employee) organizations in 2025.

This year's report unveils how enterprise organizations' experiences of ransomware — both the causes and consequences — have evolved over the past year. It also shines light onto the operational factors that left enterprise organizations exposed to attacks and the human impact of incidents on IT/cybersecurity teams.

Based on the real-world frontline experiences of 1,733 IT and cybersecurity leaders across 17 countries whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why enterprise organizations fall victim to ransomware.
- What happens to the data.
- Ransom demands and payments.
- Business impact of ransomware.
- Human impact of ransomware.

## About the survey

The report is based on the findings from an independent, vendor-agnostic survey commissioned by Sophos into organizational experiences of ransomware. A third-party specialist conducted the survey between January and March 2025. All enterprise respondents work in organizations with between 1,000 and 5,000 employees and were asked to answer based on their experiences in the previous 12 months.

The 1,733 enterprise respondents that contributed to the report span 17 countries and 14 industries, ensuring that the survey results reflect a broad and diverse range of experiences. The report includes comparisons with the findings from data captured in our previous surveys, enabling year-over-year juxtaposition. All financial data points are in U.S. dollars.

## 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 and impacts referenced occurred in 2024.

## Key findings

### Why enterprise organizations fall victim to ransomware

- ▶ **Exploited vulnerabilities** are the most common technical root cause of attacks, used in 29% of incidents. **Phishing** and **compromised credentials** followed closely behind, each cited in 21% of incidents.
- ▶ Multiple operational factors contribute to enterprises falling victim to ransomware, with the most common being **an unknown security gap**, named by 40% of victims. It is followed in very close succession by both a **lack of people/capacity** and a **lack of expertise**, which were contributing factors in 39% of attacks.

### What happens to the data

- ▶ The data encryption rate in enterprise organizations is at its lowest level in five years, with **49% of attacks now resulting in data encryption**, down from a 64% peak in 2022.
- ▶ 30% of enterprises that had data encrypted also experienced data exfiltration.
- ▶ 96% of enterprises that had data encrypted were able to recover it.
- ▶ The use of backups by enterprise organizations to restore encrypted data is at the lowest rate in four years, used in 53% of incidents.
- ▶ **48% of enterprise 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 enterprise organizations has plummeted 56% over the last year, coming in at **\$1.20 million** in 2025 compared to \$2.75 million in 2024. The primary factor behind this significant decline is a 24% decrease in the percentage of ransom demands of \$5 million or more, down from 38% of demands in 2024 to 29% in 2025. However, it's important to note that there was a 17% increase in demands between \$1M and \$5M.
- ▶ The average (median) **ransom paid** by enterprises has also dropped, coming in at **\$1 million** in 2025 compared to \$1.26 million in 2024. The decline is largely driven by a 37% decrease in the percentage of ransom payments of \$5 million or more. It should be emphasized however, that there have been increases across nearly all sub \$5 million payments bands.
- ▶ The **proportion of the ransom demand paid** by enterprises dropped to 86% in 2025 from 95% in 2024.
- ▶ Looking closely at **demands vs. payments**, close to a third (31%) of enterprises said their payment matched the initial demand. 51% paid less than the initial ask, while 18% paid more.

### Business impact of ransomware

- ▶ The average **cost for enterprises to recover** from a ransomware attack dropped by 41% over the last year, coming in at **\$1.84 million**, down from \$3.12 million in 2024.
- ▶ Looking at **speed of recovery**, enterprise organizations are recovering faster, with exactly half recovered within a week in 2025, up from 36% in 2024.

## Human impact of ransomware

Every enterprise organization that had data encrypted reported that there were direct repercussions for the IT/cybersecurity team:

- 40% of IT/cybersecurity teams reported **increased pressure** from senior leaders, while 31% reported **increased recognition**.
- 39% reported both an ongoing **increase in workload** and **increased anxiety or stress** about future attacks.
- 37% reported a **change of team priorities/focus**.
- Over a third of respondents (35%) cited both **feelings of guilt** that the attack was not stopped and **changes to team/organizational structure** as repercussions of the incident.
- 31% of teams experienced **staff absence** due to **stress/mental health** issues related to the attack.
- In over a quarter of cases (27%), the team's **leadership was replaced** because of the attack.

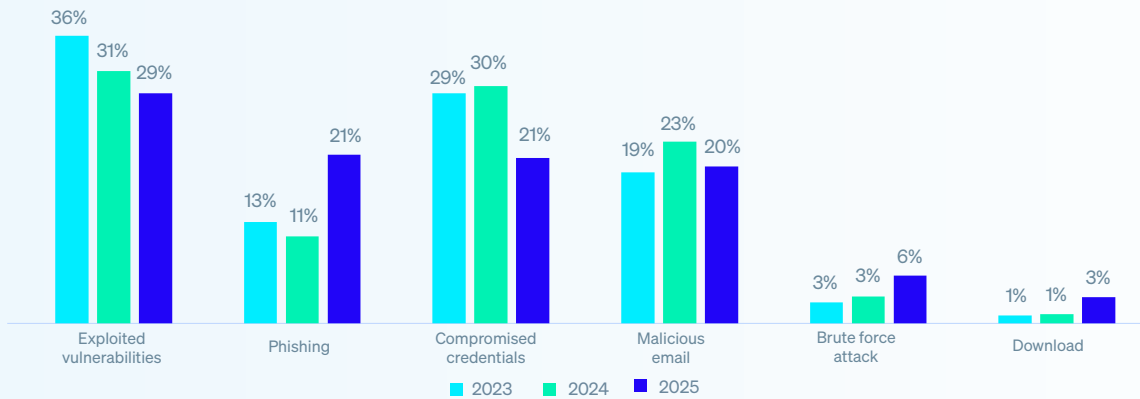
## Why enterprise organizations fall victim to ransomware

### Technical root cause of attacks in enterprises

For the third consecutive year, enterprise organizations identified **exploited vulnerabilities** as the leading root cause of ransomware attacks, responsible for 29% of incidents. **Phishing emails** ranked second, with their share surging from 11% in 2024 to 21% in 2025.

**Credential-based attacks** continue to pose a significant risk, though reports of this attack vector dropped significantly — from 30% in 2024 to 21% in 2025. By contrast, **small and midsize businesses** (those with between 100 and 250 employees) cited credential-based attacks as the leading root cause of ransomware attacks, responsible for close to one-third (30%) of incidents.

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

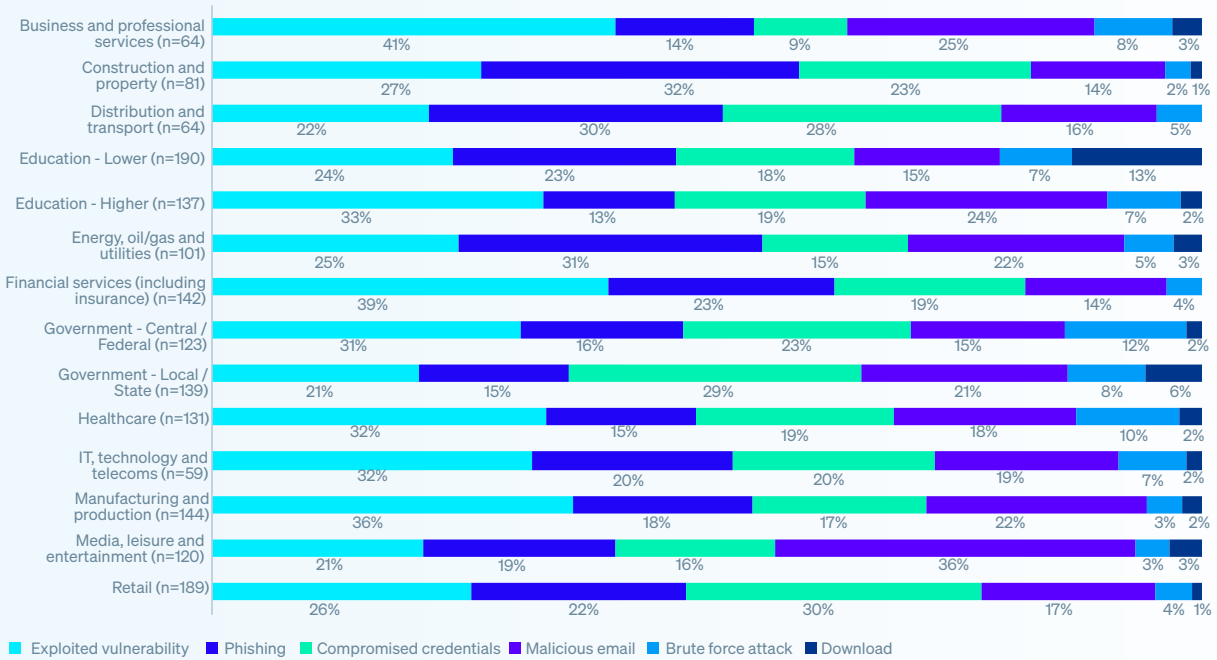


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=1,733 (2025), 1,409 (2024), 1,045 (2023).

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

- **Phishing** was the most common root cause cited by both **construction and property** (32%), **distribution and transport** (30%) and **energy, oil/gas and utilities** (31%) providers.
- **Compromised credentials** were the most perceived attack vector for enterprises in the **retail sector**, accounting for nearly a third of incidents (30%).

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

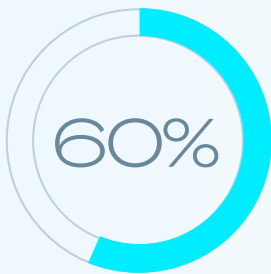


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

### Organizational root cause of incidents in enterprise organizations

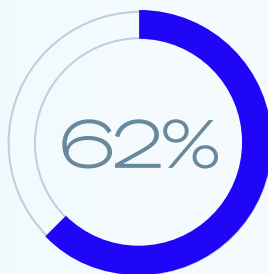
Alongside the technical root causes of incidents, it's also valuable to understand the organizational factors that left enterprises exposed to attacks. The findings reveal that victims in enterprise organizations typically face multiple organizational challenges, with respondents citing three factors, on average, that contributed to them falling victim to the ransomware attack.

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



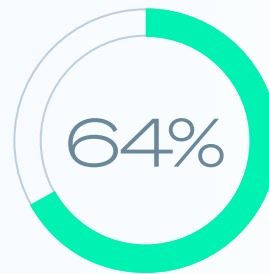
**LACK OF/POOR QUALITY PROTECTION**

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)**

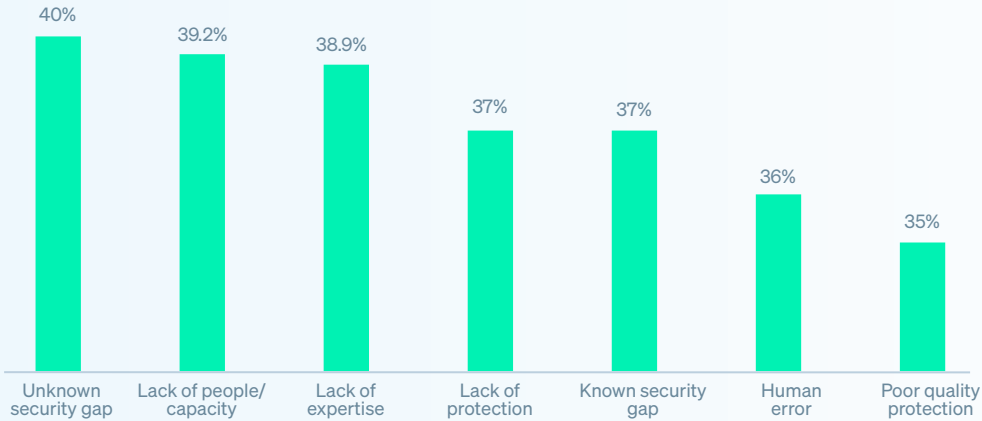
Had a known or unknown weakness in their defenses

Why do you think your organization fell victim to the ransomware attack? n=1,733. Consolidated responses.

**Unknown security gaps** (i.e., weakness(es) in defenses that respondents were unaware of) are the most common individual reason given, named by 40% of enterprise respondents. They are closely followed by both a **lack of people/capacity** (i.e., an insufficient number of cybersecurity experts monitoring systems at the time of the attack) and a **lack of expertise** (i.e., insufficient skills or knowledge available to detect and stop the attack in time) which were identified as contributing factors by 39% of enterprises.

Interestingly, **SMBs** also identified a lack of **people/capacity** as a common factor, with 42% citing it as a key reason for falling victim to an attack, highlighting that resource constraints remain a widespread challenge regardless of organization size.

Chart 3: Operational root cause of ransomware attacks on enterprise organizations



Why do you think your organization fell victim to the ransomware attack? n=1,733.

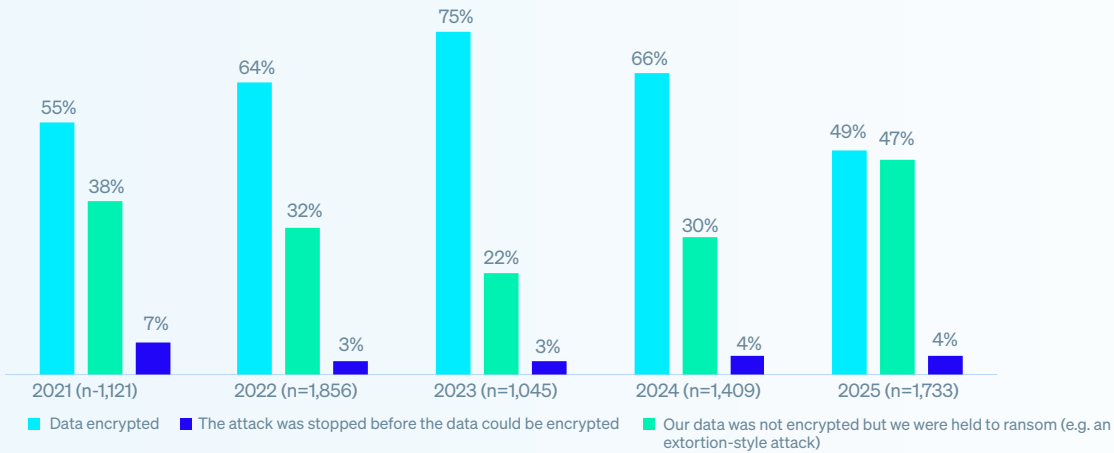
## What happens to the data

### Data encryption in enterprises

Encouragingly, the data encryption rate in enterprise organizations is at its lowest reported rate in the five years of our survey, with under a half (49%) of attacks resulting in data being encrypted down from the 66% 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 22% in 2023 to 47% in 2025. This suggests that enterprise organizations are becoming more effective at detecting and stopping attacks before they cause serious damage.

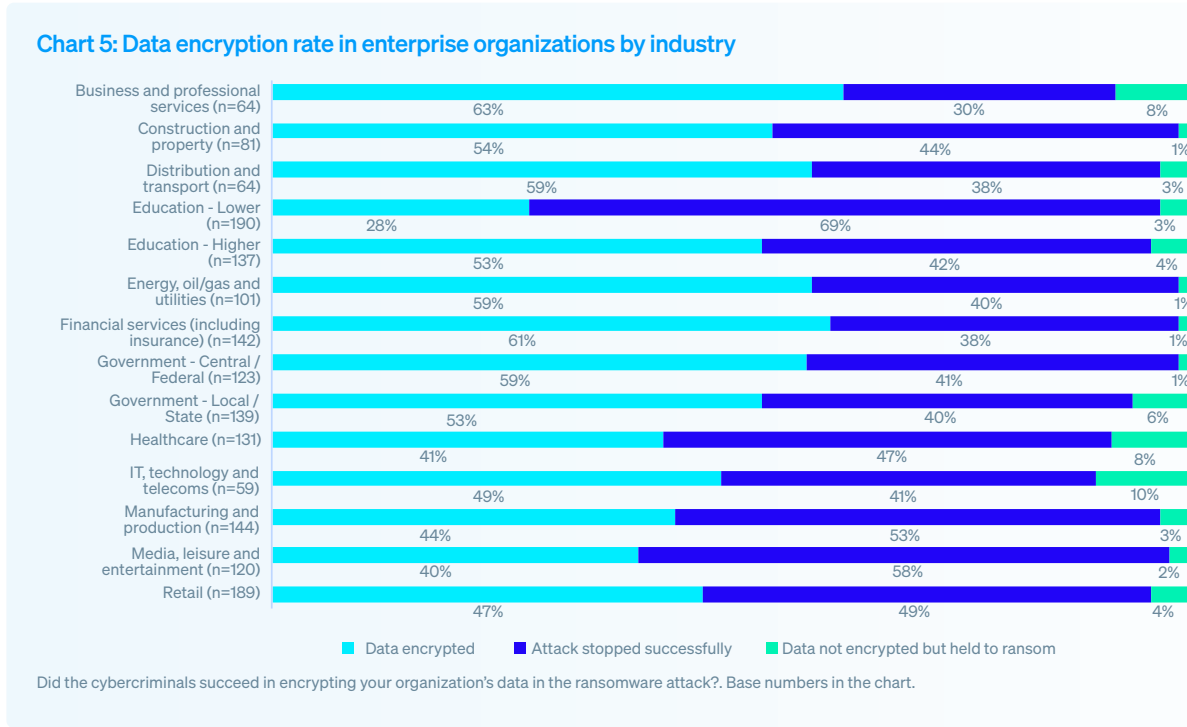
**Chart 4: Data encryption rate in ransomware attacks on enterprise organizations 2021 - 2025**



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

## Data encryption rate by industry

Enterprises within the **business and professional services** sector are most likely to have data encrypted (63%), indicating that organizations in this sector have lower success rates in detection and stopping 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 28%.



## Data theft

Adversaries don't just encrypt data — they steal it. Among enterprise organizations, 15% of all ransomware victims and 30% of those that had data encrypted experienced data theft. Breaking down the data by industry we see that:

- At the higher end, 52% of enterprises in the **media, leisure and entertainment** sector that experienced data encryption also had data stolen.
- By contrast, only 11% of enterprises in the **construction and property** sector faced data theft alongside encryption.

## Extortion-style attacks

As shown in chart 4, the share of enterprises that avoided data encryption yet were still held to ransom remained steady year on year at 4%. When viewed by industry, **IT, technology and telecom** organizations were the most exposed to this type of attack at 10%, while enterprises within **construction and property, energy, oil and gas and utilities, financial services, and central/federal government** were the least affected, each reporting just 1%.

Overall, enterprises within **lower education** were the 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.

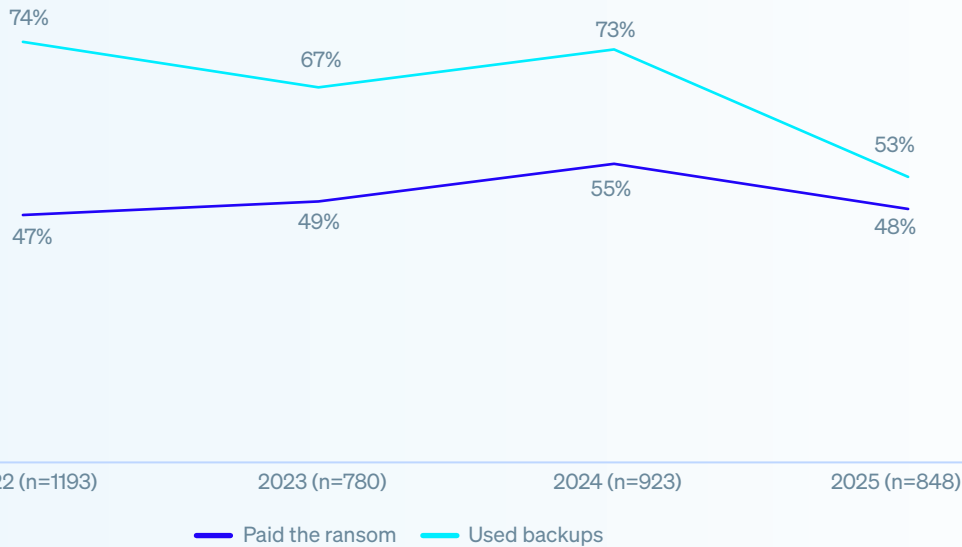
## Recovery of encrypted data in enterprise organizations

96% of enterprises that had data encrypted recovered it.

In 2025, 48% of enterprises **paid the ransom to recover their data** — down from 55% in 2024. At the same time, **backup use** dropped sharply to a four-year low (53%, down from 73% in 2024). Collectively, these findings point to stronger resistance to demands together with weaknesses and lack of backup resilience.

Furthermore, the narrowing gap between enterprises 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 close to a third (30%) of enterprises that had data encrypted said they **used other means to restore their data**. Alternative methods could include restoration from shadow copies, utilizing endpoint protection rollback features or recovering data from unaffected systems.

Chart 6: Recovery of encrypted data in enterprise organizations 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

### Enterprise ransom demands

The average (median) ransom demand for enterprise organizations plummeted 56% over the last year, coming in at \$1.20 million in 2025, down from \$2.75 million in 2024. The decrease in ransom demands targeting enterprises is largely driven by a 24% decrease in demands of \$5 million or more over the last year. However, it's important to note that there was a 17% increase in demands between \$1 million and \$5 million — accounting for 27% of demands — up from 23% in 2024.

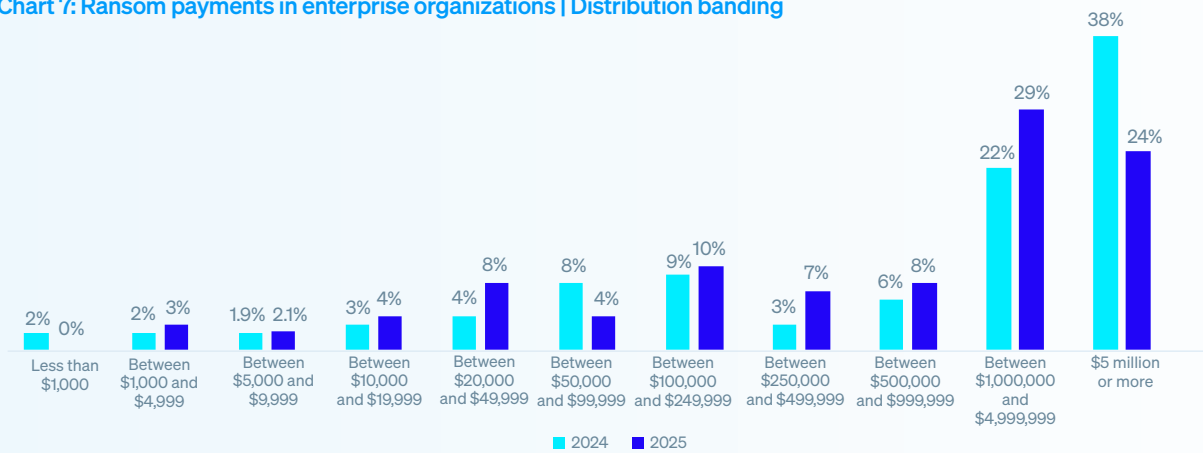
### Enterprise ransom payments

Following this trend, the average (median) ransom paid by enterprises also saw a decline from \$1.26 million in 2024 to just \$1 million in 2025. This is largely due to a 37% decrease in payments of \$5 million or more over the last year. However, the report revealed year-on-year increases across nearly all payment bands below \$5 million.

These patterns suggest that attackers are moving away from the very highest ransom asks and are instead targeting enterprises with more mid-range demands, aiming for amounts that are still damaging but more realistically able to be paid.

**SMBs** followed a similar pattern, although the drop in demands and payments was even more pronounced. Median ransom demands and payments dropped sharply from \$2 million in 2024 to \$126K and \$200K in 2025 respectively, reinforcing the broader trend of attackers recalibrating their expectations towards more attainable sums across organizations of all sizes.

Chart 7: Ransom payments in enterprise organizations | Distribution banding

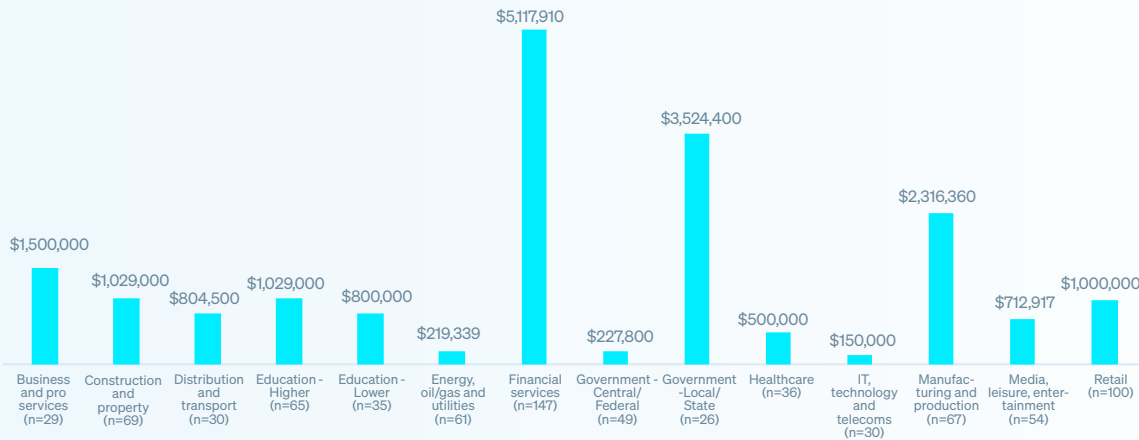


How much was the ransom payment that was paid to the attackers? n=414 (2025), 470 (2024)

## Ransom payments by industry

Ransom payments varied considerably by industry, with enterprises within the financial services sector paying the highest average (median) amount to attackers at \$5.1 million. This may be due to the sector’s high operational stakes and low tolerance for disruption, making attackers confident that larger payments are more likely to be considered.

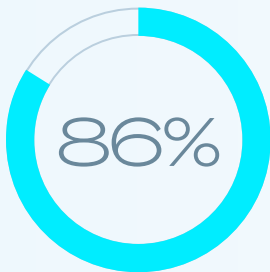
Chart 8: Ransom payments by industry



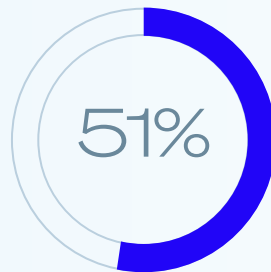
How much was the ransom payment that was paid to the attackers? Base numbers in chart. Note: Where base numbers are less than 30, findings should be considered indicative only.

## How actual payments made by enterprises stack up with the initial demand

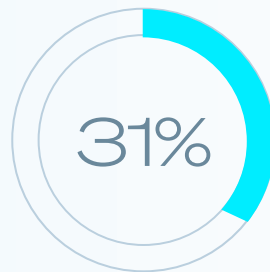
414 enterprises that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 86% of the initial ransom demand – a welcome drop from the 95% recorded in 2024. Overall, 51% paid less than the initial ask, 18% paid more, and close to a third (31%) matched the initial demand.



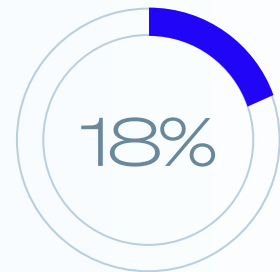
86%  
of the ransom demand was paid, on average



51%  
of payments were for less than the initial ransom demand



31%  
of payments matched the initial ransom demand



18%  
of payments were for more than the initial ransom demand

## Why most ransom payments made by enterprises differ from the amount initially demanded

The survey also explores why some enterprise organizations pay more than the initial demand and others pay less, shining light on an important area when dealing with a ransomware attack.

72 enterprises that **paid more** than the initial demand revealed that:

- 61%: The attackers believed we could afford to pay more.
- 49%: The attackers realized we are a high value target.
- 42%: Our backups failed or were malfunctioning.
- 39%: The attackers got frustrated and increased the price.
- 31%: We did not pay quickly enough, so the price went up.

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

214 enterprises that **paid less** than the initial demand explained how they were able to lower their payment:

- 49%: We negotiated a lower amount with the attackers.
- 46%: We paid the ransom quickly, so we got a discount.
- 45%: The attackers reduced their demand to encourage us to pay.
- 43%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement)
- 38%: 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.

## Business consequences of ransomware

### Recovery costs in enterprise organizations

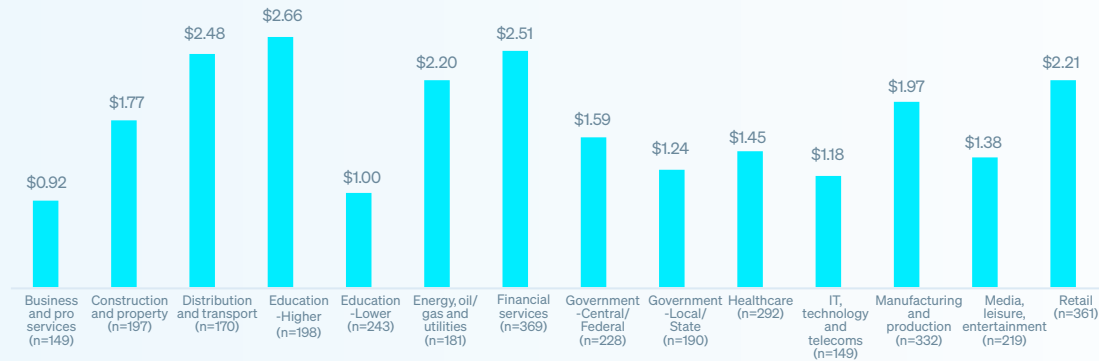
The average (mean) cost for enterprises to recover from a ransomware attack (excluding any ransom payment) has fallen to its lowest point in three years, dropping by 41% over the past year to \$1.84 million, down from \$3.12 million in 2024. It is also \$330K lower than the \$2.17 million reported in 2023.



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=1,733 (2025), 1,409 (2024), 1,045 (2023)

When looking at an industry split, recovery varies considerably. **Lower education** enterprises reported the highest average cost to rectify incidents at \$2.66 million. In contrast, enterprises within the **business and professional services** sector reported the lowest cost at \$0.92 million. This difference likely reflects in part the differing level of IT infrastructure rebuilding needed to recover from the attack, with lower education organizations typically running older solutions than private sector services providers.

Chart 9: Ransomware recovery cost split by industry (USD millions)

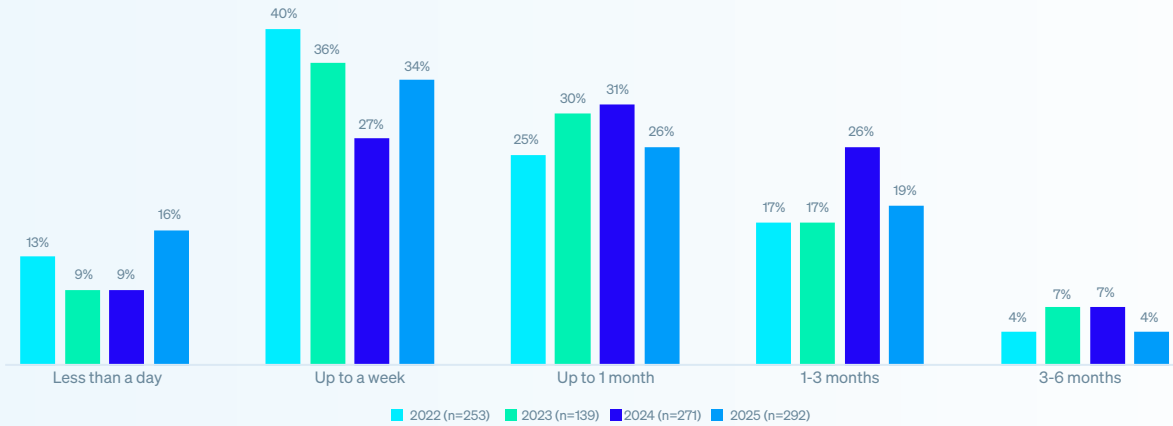


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

## Recovery time in enterprise organizations

The data reveals that, in 2025, enterprises are getting faster at recovering from ransomware attacks. Half recovered within a week, up from the 36% reported in 2024. At the same time, the proportion taking one to three months to recover fell to 19%, down from 26% in 2024. Overall, 95% of enterprise victims fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

Chart 10: Recovery time for enterprise organizations from ransomware attacks 2022 - 2025

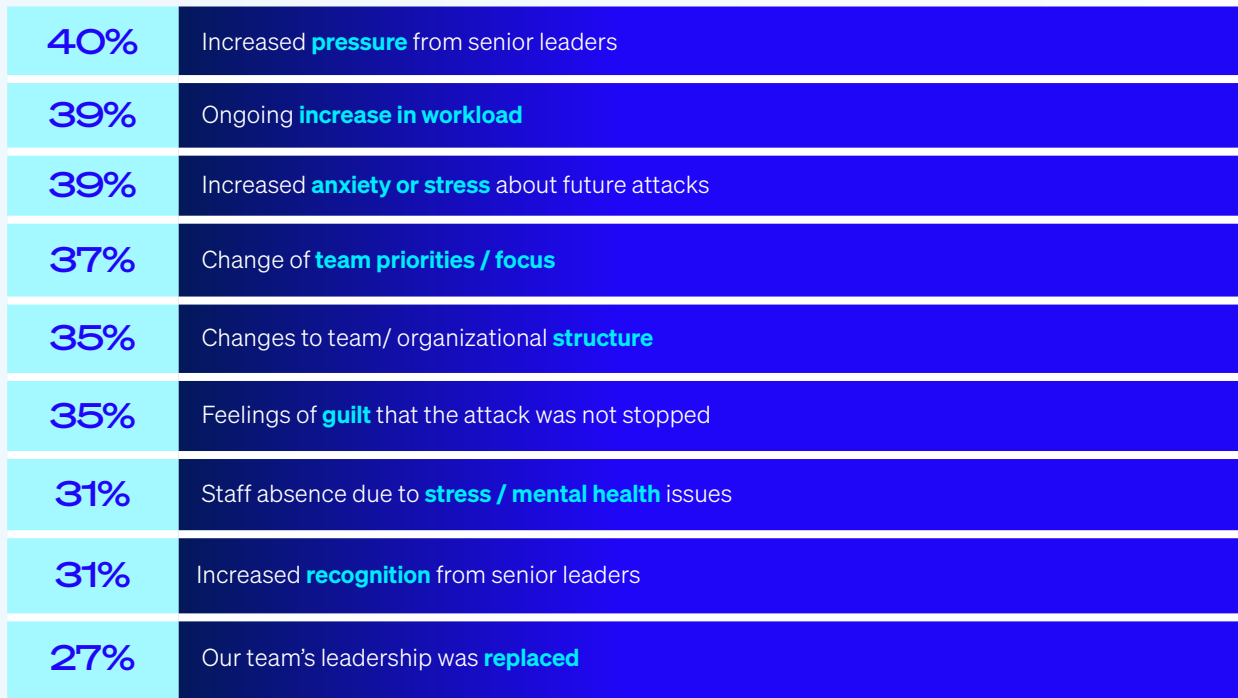


How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

## Human consequences of ransomware

The survey makes clear that having data encrypted in a ransomware attack has significant repercussions for IT/cybersecurity teams in enterprise organizations, 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=848.

## Recommendations

Although enterprise organizations have experienced several changes in their encounters with ransomware over the last year, it remains a significant threat. As adversaries continue to 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](http://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.