academia
the technology group

SOPHOS

THE STATE OF RANSOMWARE 2025

Findings from an independent survey of 3,400 IT and cybersecurity leaders across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. June 2025

Introduction

Welcome to the sixth edition of the annual Sophos State of Ransomware report which reveals the reality of ransomware in 2025.

This year's report details how organizations' experiences of ransomware — both cause and consequences — have evolved over the last 12 months. It also shines light into previously unexplored areas, including the operational factors that left organizations exposed to attack and the human impact of incidents on the IT/cybersecurity team.

Based on the real-world frontline experiences of 3,400 IT and cybersecurity leaders across 17 countries whose organizations were hit by ransomware in the last year, the report provides unique insights into:

- Why organizations fall victim to ransomware.
- What happens to the data.
- Ransoms: 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.

Participants came from 17 countries and a wide range of industries, ensuring that the survey results reflect diverse experiences across the public and private sectors. The report includes comparisons with the findings from our previous reports, enabling year-over-year comparisons. All financial data points are in U.S. dollars.

Key findings

Why organizations fall victim to ransomware

- For the third year running, victims identified **exploited vulnerabilities** as the most common technical root cause of attack, used in 32% of incidents.
- Multiple operational factors contribute to organizations falling victim to ransomware, with the most common being a **lack of expertise**, named by 40.2% of victims. It is followed in very close succession by having **security gaps that the organization was not aware of**, which was a contributing factor in 40.1% of attacks. In third place was **lack of people/capacity**, which contributed to 39.4% of attacks.

What happens to the data

- **Data encryption** is at the lowest level in six years, with 50% of attacks now resulting in data encryption, down from 70% in 2024.
- 28% of organizations that had data encrypted also experienced **data exfiltration**.
- 97% that had data encrypted were able to recover it.
- The use of **backups** to restore encrypted data is at the lowest rate in six years, used just in 54% of incidents.
- 49% of victims **paid the ransom** to get their data back. While this represents a slight drop from last year's 56%, it is the second highest ransom payment rate in six years.

Ransoms: Demands and payments

- The average (median) **ransom demand** has dropped by one third (34%) over the last year, coming in at $1,324,439 in 2025 compared to $2 million in 2024.
- The average (median) **ransom payment** has fallen by 50% in the last year, down from $2M in 2024 to $1M in 2025. The primary factor behind this drop is a reduction in the percentage of ransom payments of $5M or more, down from 31% of payments in 2024 to 20% in 2025.
- When comparing **demands vs. payments**, only 29% said their payment matched the initial demand. 53% paid less than the initial ask while 18% paid more.

Business impact of ransomware

- Excluding any ransom paid, the average **cost to recover** from a ransomware attack dropped by 44% over the last year, coming in at $1.53 million, down from $2.73 million in 2024.
- Looking at **speed of recovery**, organizations are getting faster, with 53% fully recovered after a week, up from 35% in 2024.

Human impact of ransomware

- Every organization that had data encrypted reported that there were **direct repercussions** for the IT/cybersecurity team:
  - 41% of IT/cybersecurity teams say they have **increased anxiety or stress** about future attacks.
  - One third (34%) said the team experienced **feelings of guilt** that the attack was not stopped in time.
  - 40% report **increased pressure** from senior leaders but 31% report **increased recognition**.
  - 31% of teams have experienced **staff absence** due to stress/mental health issues related to the attack.
  - In one quarter of cases, the team's **leadership was replaced** as a consequence of the attack.

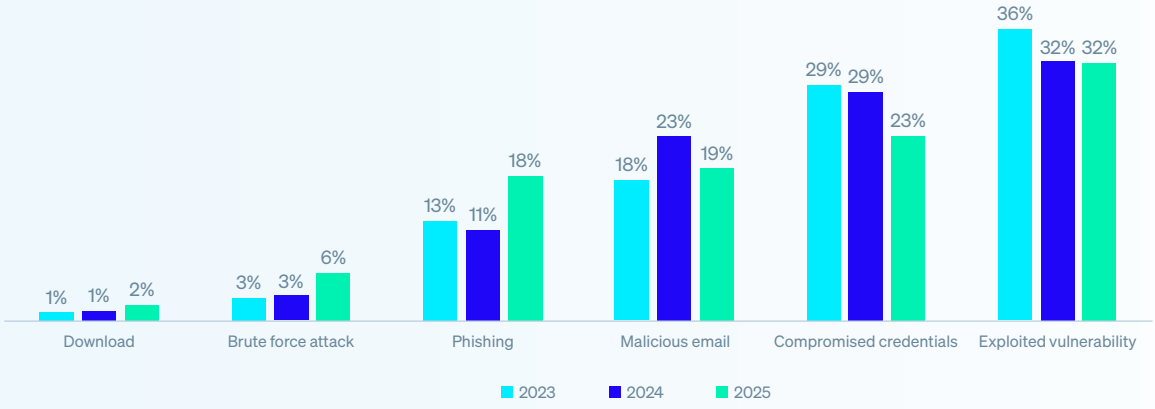
Why organizations fall victim to ransomware

Technical root cause of attacks

For the third year running, victims identified **exploited vulnerabilities** as the most common root cause of ransomware incidents, used to penetrate organizations in 32% of attacks overall.

Compromised credentials remains the second most common perceived attack vector, although the percentage of attacks that used this approach dropped from 29% in 2024 to 23% in 2025. Email remains a major vector of attack with 19% of victims reporting **malicious email** as the root cause and a further 18% citing **phishing** — a notable jump from last year's 11%.

Chart 1: Technical root cause of ransomware attacks 2023–2025

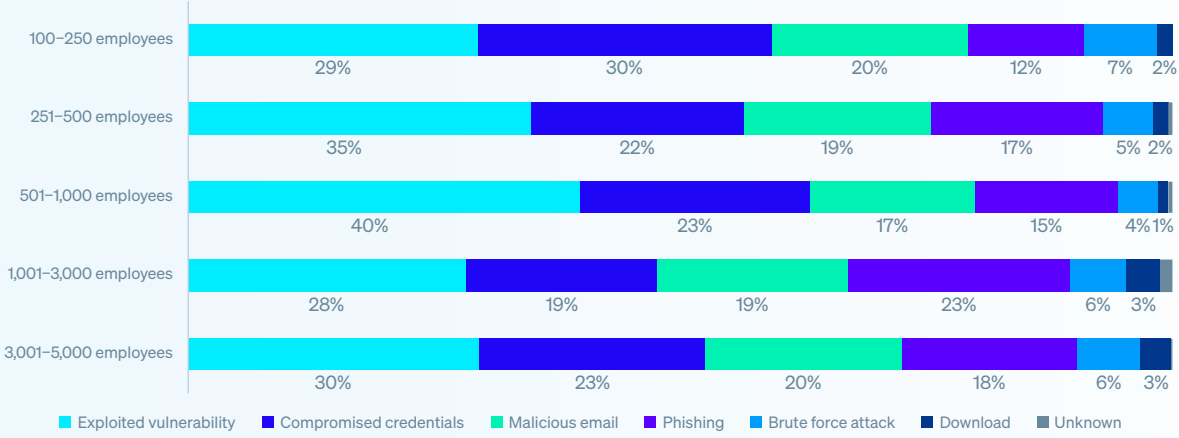


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400 (2025), 2,974 (2024), 1,974 (2023).

The research reveals differences in attack vectors based on organization size:

- **Compromised credentials** were the most common root cause in the 100–250 employee segment, used in 30% of attacks.
- 40% of attacks in the 501–1,000 employee segment started with an **exploited vulnerability**.
- Approaching one quarter (23%) of attacks on organizations with 1,001–3,000 employees began with a **phishing email**.

Chart 2: Technical root cause of ransomware attacks split by organization size

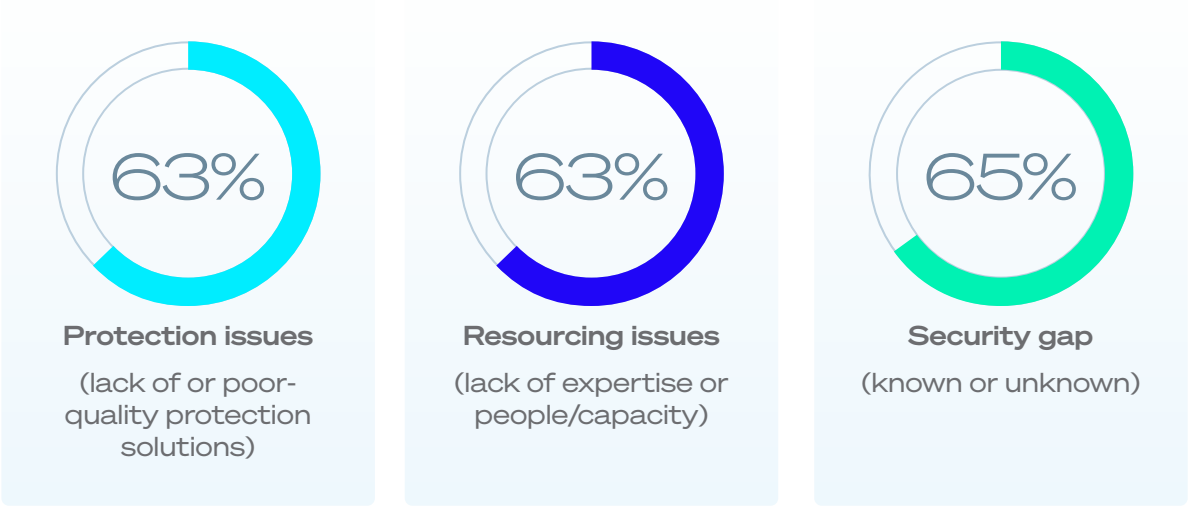


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400

Operational root cause of incidents

This year's report explores for the first time the organizational factors that left companies exposed to attacks. The findings reveal that victims are typically facing multiple operational challenges with respondents citing 2.7 factors, on average, that contributed to them falling victim to the ransomware attack.

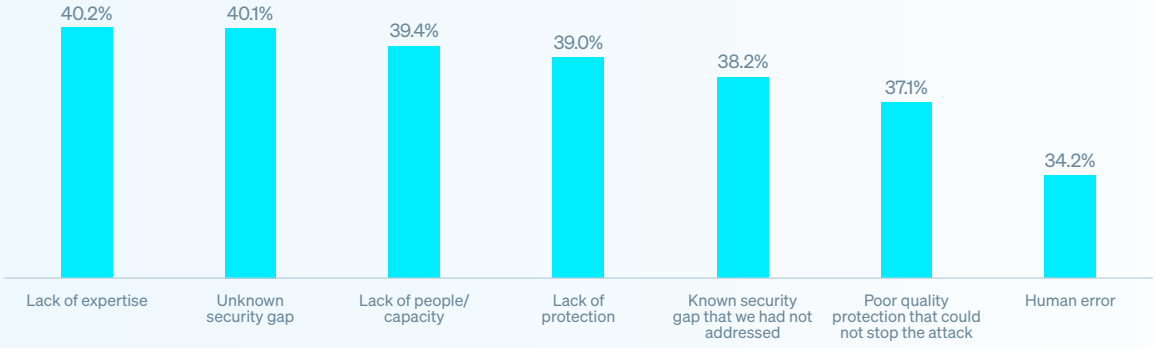
Overall, there is no single stand-out source, with the organizational root causes very evenly split across protection issues, resourcing issues, and security gaps.



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

Lack of expertise (i.e., not having the skills or knowledge to detect and stop the attack in time), is the most common operational reason given, named by 40.2% of respondents. It is followed in very close succession by **security gaps that the organization was not aware of**, which was a contributing factor in 40.1% of attacks. In third place was **lack of people/capacity** (i.e., not having a sufficient number of cybersecurity experts monitoring their systems at the time of the attack) which contributed to 39.4% of attacks.

Chart 3: Operational root cause of ransomware attacks

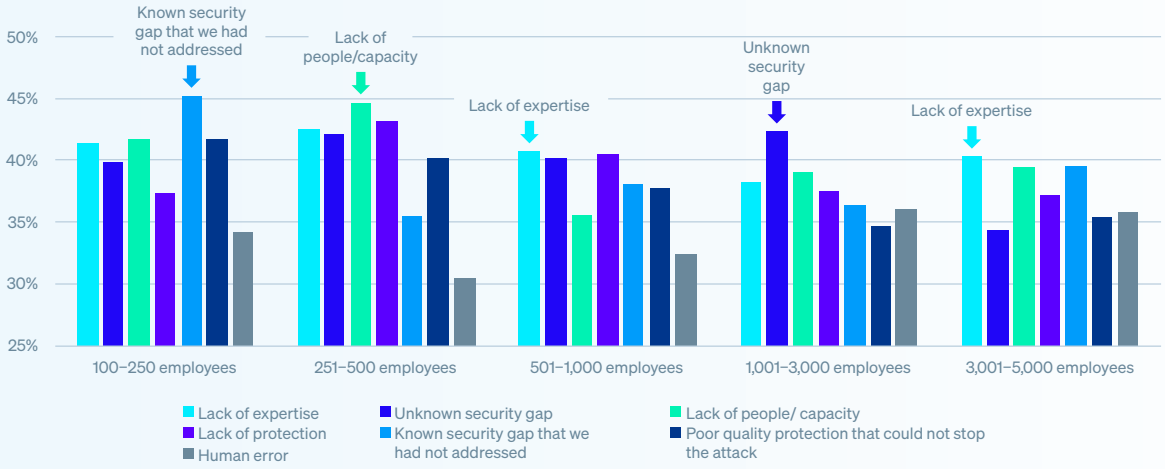


Why do you think your organization fell victim to the ransomware attack? n=3,400

Operational root cause by business size

The most common organizational reason companies fall victim to ransomware varies based on the size of the organization, reflecting the different challenges they face. Across the five employee size segments used in this report, four different challenges topped the factors that contributed to them falling victim to the attacks, as shown in the chart below.

Chart 4: Operational root cause of ransomware attacks split by organization size

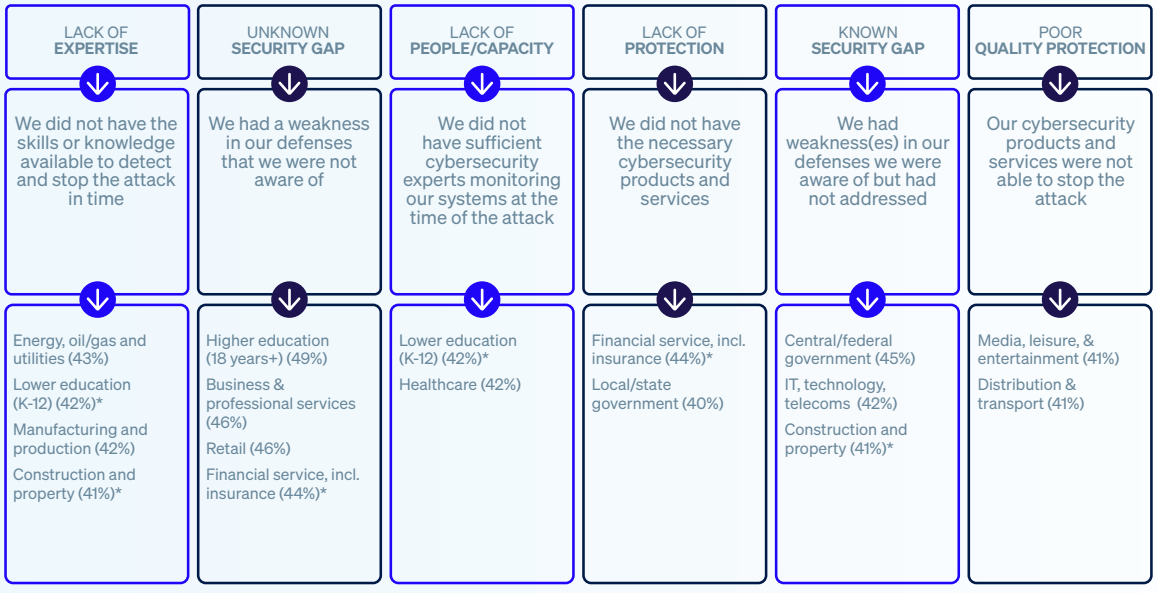


Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by organizational size (number of employees)

Operational root cause by sector

Similarly, the most common operational 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 5: Top operational root cause of ransomware attacks by sector



* indicates joint top root cause of attacks.

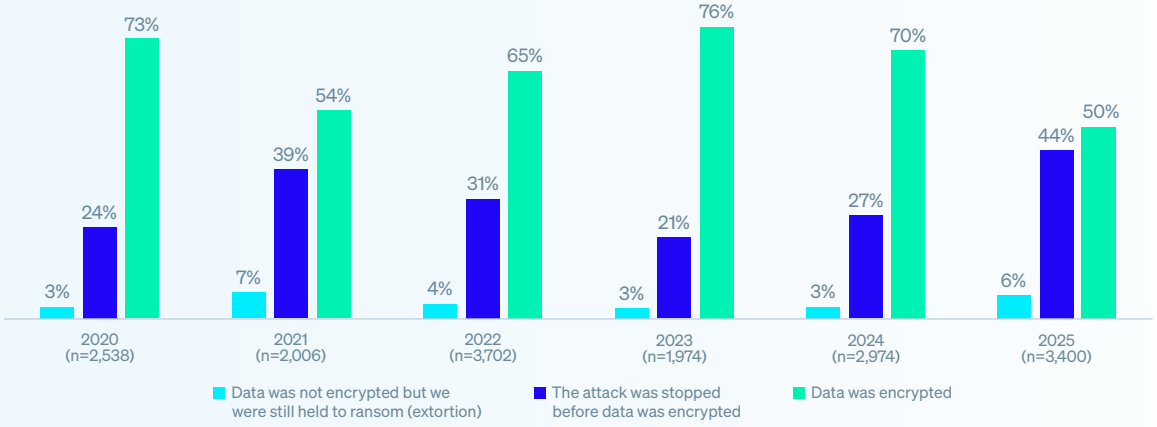
Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by industry

What happens to the data

Data encryption

Encouragingly, data encryption is at the lowest reported rate in the six years of our study, with 50% of attacks resulting in data being encrypted. There has been a marked drop in the percentage of attacks that resulted in data encryption over the last year, down from 70% in our 2024 survey to 50% in 2025, suggesting organizations are more capable of stopping attacks before the encrypted payload is deployed.

Chart 6: Data encryption rate in ransomware attacks 2020–2025



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

The largest organizations surveyed were most likely to have data encrypted, with 65% of attacks on organizations with 3,001–5,000 employees resulting in data encryption, the highest encryption rate reported across all size cohorts. This suggests that larger organizations are less able to detect and stop the attack before encryption, and/or are less able to block and roll back malicious encryption than smaller ones.

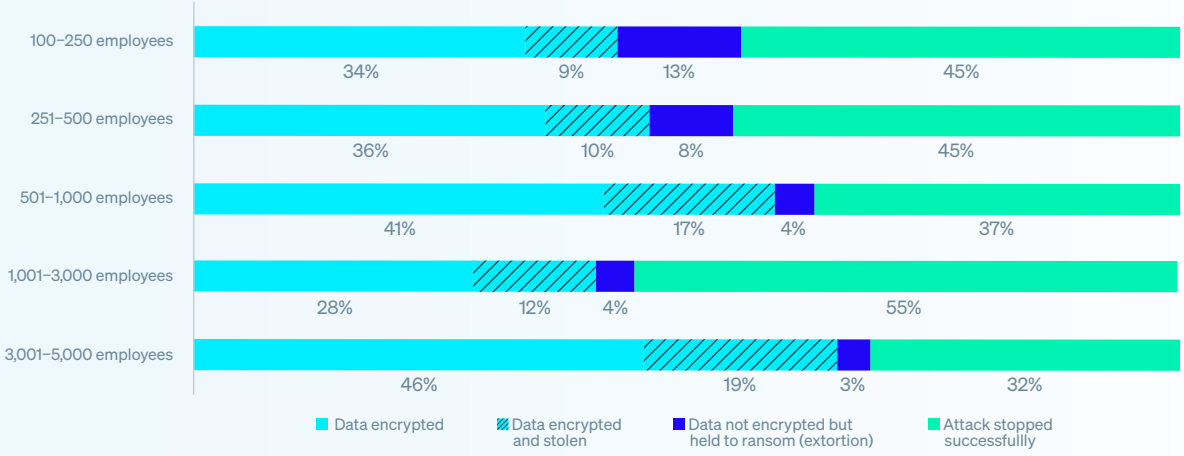
Data theft

Adversaries don't only encrypt data — they also steal it. 14% of all ransomware victims and 28% of those that had data encrypted experienced data theft. Breaking down the data by company size we see that smaller organizations are almost 40% less likely to have data stolen than larger ones.

- 22% of 100–500 employees organizations that had data encrypted also had data stolen.
- 30% of 501–5,000 employee organizations that had data encrypted also had data stolen.

While it is possible that smaller organizations are more able to prevent the data theft than larger ones, this variance is probably due to attackers being more likely to attempt to exfiltrate data in larger organizations and/or smaller companies being less able to identify that data has been stolen.

Chart 7: Data encryption rate in ransomware attacks split by organization size



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? n=3,400

Extortion-style attacks

As shown in chart 6, the percentage of organizations that did not have data encrypted but were held to ransom anyway (extortion) doubled in the last year, reported in 6% of attacks in 2025 compared to just 3% in 2024. Smaller organizations are most likely to be held to ransom without data being encrypted (an extortion-style attack) than larger ones:

- 13% of victims with 100–250 employees experienced an extortion-style attack.
- 3% of victims with 3,001–5,000 employees experienced an extortion-style attack.

Overall, organizations with 1,001–3,000 employees 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.) It is possible that these organizations are at a sweet spot where they are large enough to have a higher level of cybersecurity tools and expertise but are not subject to the same levels of organizational complexity as larger businesses.

Recovery of encrypted data

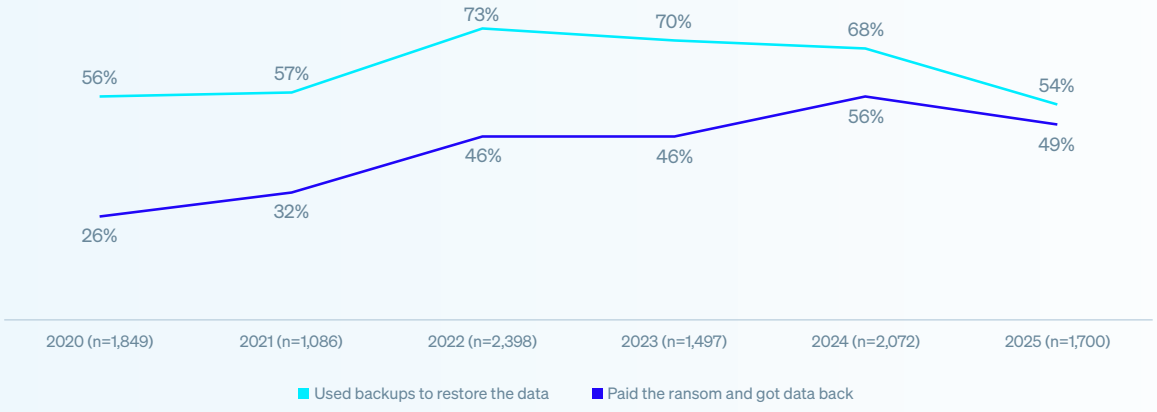
97% of organizations that had data encrypted were able to recover it.

Just over half (54%) restored their data using backups — the third year in a row this number has shrunk. Overall, data recovery through backups is at its lowest rate in six years.

Just under half (49%) paid the ransom and got their data back. While this represents a small reduction from last year's 56%, it remains the second highest rate of ransom payments in the last six years.

29% of those that had data encrypted said they used "other means" to restore their data. This likely includes those that used decryption keys that had previously been made public.

Chart 8: Recovering data via backups and ransom payments 2020–2025



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

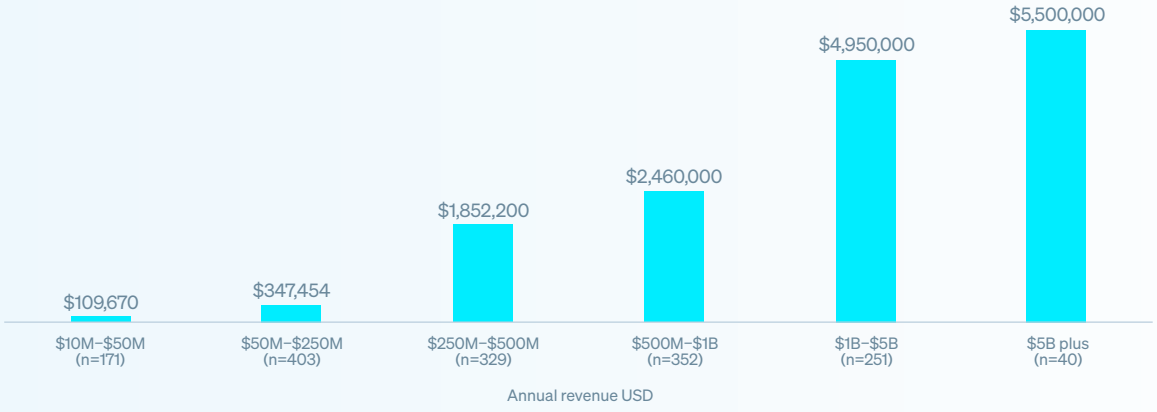
Ransom demands

The average (median) ransom demand fell by one third (34%) over the last year, coming in at $1,324,439, down from $2 million in 2024. This reduction was largely driven by a decrease in ransom demands of $5 million or more, down from 30% to 24%. While this drop is encouraging, it's important to keep in mind that 57% of ransom demands were for $1 million or more.

Ransom demands increase in line with organization revenue, suggesting that adversaries "price" their ransom demands based on their victim's perceived ability to pay:

- $109,670: Median ransom demand for organizations with $10 million–$50 million annual revenue.
- $5,500,000: Median ransom demand for organizations with $5 billion plus annual revenue.

Chart 9: Ransom demands split by company annual revenue



How much was the ransom demand from the attacker(s)? Base numbers in chart.

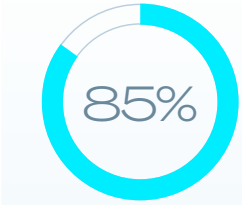
Ransom payments

The average (median) ransom payment fell by 50% in the last year, down from $2 million in 2024 to $1 million in 2025. As with ransom demands, the primary factor behind the lower median ransom payment is a reduction in the percentage of payments of $5M or more, down from 31% in 2024 to 20% in 2025.

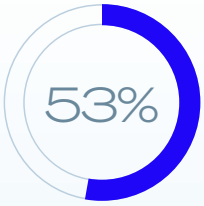
While ransom demands and payments have fallen in the last year, it's encouraging that payments have seen the greatest drop. That said, $1 million remains a very significant sum — one that has major consequence for most organizations.

How actual payments stack up with the initial demand

826 organizations that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 85% of the initial ransom demand. Overall, 53% paid less than the initial ask, 18% paid more, and 29% matched the initial demand.

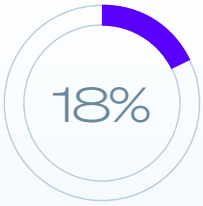


of the ransom demand **was paid**, on average



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

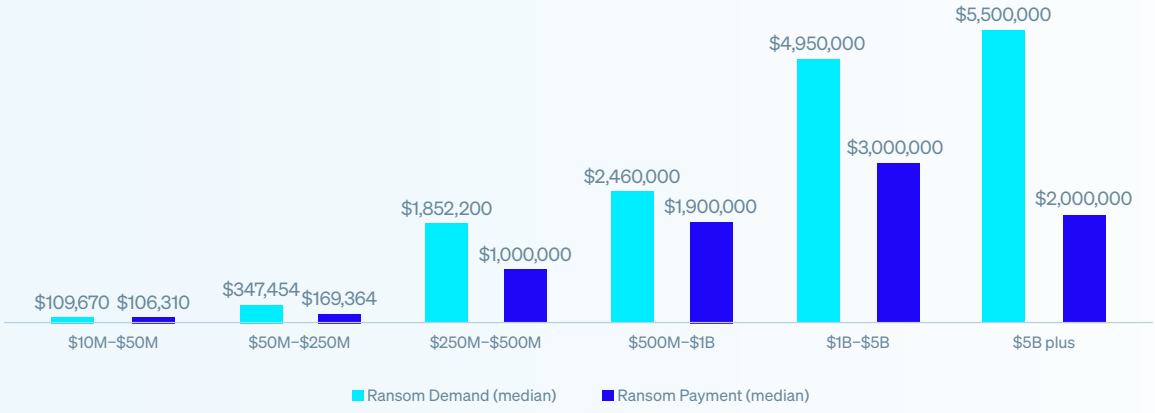
of payments **matched** the initial ransom demand



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

Splitting the data by annual revenue, we see that all revenue cohorts paid, on average, less than the initial demand. However, the largest revenue organizations ($5 billion or more annual revenue) saw the greatest reduction with their actual average payment ($2 million) coming in at just 36% of the initial demand ($5.5 million), when excluding outliers. Conversely, organizations with $10 million–$50 million annual revenue reported the smallest reduction with their median payment coming in at 97% of the median demand.

Chart 10: Ransom demand vs ransom payment split by company annual revenue



How much was the ransom demand from the attacker(s). How much was the ransom payment that was paid to the attackers? (n=1,552/836)

Why most ransom payments differ from the amount initially demanded

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

151 organizations that **paid more** than the initial demand revealed that:

- 50%: The attackers believed we could afford to pay more.
- 48%: The attackers realized we are a high value target.
- 38%: The attackers got frustrated and increased the price.
- 38%: Our backups failed or were malfunctioning.
- 32%: We did not pay quickly enough, so the price went up.

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

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

- 47%: We negotiated a lower amount with the attackers.
- 45%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement).
- 45%: The attackers reduced their demand to encourage us to pay.
- 43%: We paid the ransom quickly, so we got a discount.
- 40%: 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

The average (mean) cost to recover from a ransomware attack (excluding any ransom payment) dropped by 44% over the last year, coming in at $1.53 million, down from $2.73 million in 2024. It is also just over $300,000 lower than the sum reported in 2023.

2023
$1.82 million

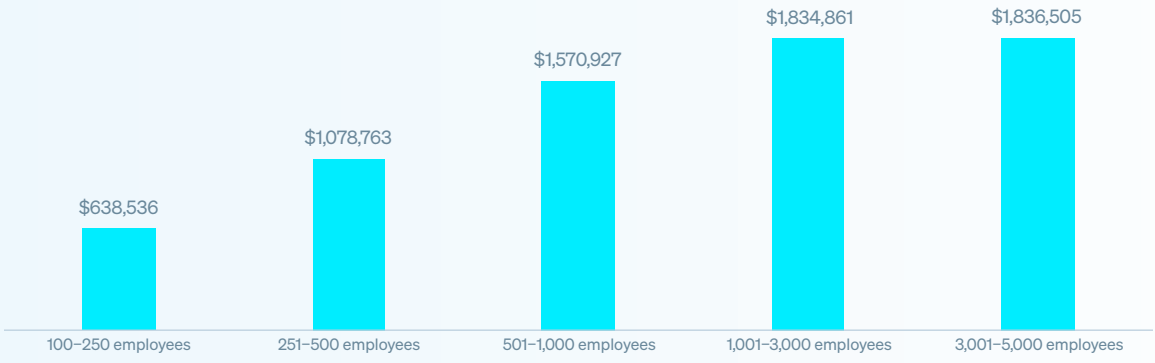
2024
$2.83 million

2025
$1.53 million

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=3,400 (2025), 2,974 (2024), 1,974 (2023)

Recovery costs increase in line with organization size until they plateau for organizations with between 1,000 and 5,000 employees. Those with 100–250 employees report an average recovery cost of $638,536, while those with 1,000–5,000 employees incurred costs of $1.83 million.

Chart 11: Ransomware recovery cost split by company size

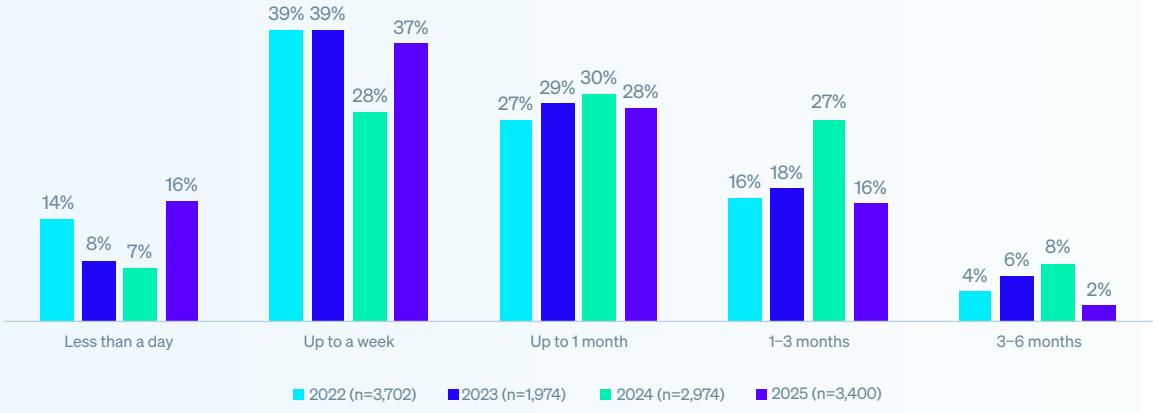


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, etc.) excluding any ransom payments made? n=3,400

Recovery time

The data reveals that organizations are getting faster at recovering from attacks with 16% fully recovered in a day, up from 7% in 2024 and 8% in 2023. Over half (53%) were recovered within a week, a significant jump from the 35% reported in 2024. Overall, almost all victims (97%) were fully recovered three months on from the attack. This improved recovery speed may indicate that organizations have been investing in cyber incident preparation and recovery readiness over the last year.

Chart 12: Recovery time 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, organizations that had data encrypted typically were slower to recover than those that were able to stop the encryption: 9% that had data encrypted were fully recovered in a day, compared with 24% of those were 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 the IT/cybersecurity team with all respondents saying their team has been impacted in some way.

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

What repercussions has the ransomware attack had on the people in your IT/ cybersecurity team, if any? n=1,700

Recommendations

While there have been several changes in organization's experiences of ransomware over the last year, it remains a major threat to all organizations. 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 take 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.

© Copyright 2025. 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.

2025-06-25 WP (DD)

SOPHOS