REPORT

The State of Ransomware 2026

Insights from 2,158 IT and Cybersecurity Leaders Across 17 Countries

SOPHOS

Introduction

The ransomware landscape is changing fast in the wake of AI. Better outcomes are evident for organizations making sustained investments in cybersecurity defenses, but ransomware attacks are still costing firms millions.

This is the seventh edition of the annual Sophos State of Ransomware report, which offers new data on ransomware attacks from the trailing year. The findings are collected into sections covering:

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

The data tells a story of costly outcomes mixed with genuine progress:

- Ransomware recovery costs are high, with the typical recovery bill now $1.7 million.
- Over half of ransomware attacks (56%) still succeed in encrypting data, with the rate rising from 2025.
- However, ransom demands and payments are declining, and organizations are getting better at negotiating outcomes. Over the last two years, median demands have declined 65% and payments have dropped 62%.
- After three years in the top spot, exploited vulnerabilities are no longer the number one root cause for ransomware attacks (18%), with email-based attacks (phishing 24% or malicious emails 26%) now the most common attack vectors.

2,158

IT and security leaders across 17 countries whose organization was hit by ransomware in the last year participated in a vendor agnostic global survey, serving as the base for this year's research.

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, 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 seven-year history. All financial data points are in U.S. dollars.

Key findings at a glance

- **Identity compromise is the primary ransomware delivery mechanism**
  - Malicious email (26%) and phishing (24%) have become the top root causes of ransomware attacks.
  - Exploited vulnerabilities — the top root cause of the past three years — dropped 14 percentage points over the last year to 18%.
  - Two-thirds of ransomware victims (67%) confirmed their ransomware incident was also their most significant identity attack.
- **Protection, security, and resourcing gaps leave organizations exposed to attacks**
  - Security gaps (known or unknown) were the most cited operational root causes for the second year in a row at 62%, followed by lack of people or skills (58%), and lack of, or poor-quality, protection (57%).
- **Multi-factor authentication (MFA) deployment alone is not enough to stop ransomware**
  - MFA was deployed in some capacity for 97% of incidents where compromised credentials were the root cause of the ransomware attacks.
- **In more than half of incidents, organizations fail to detect and stop ransomware attacks in time**
  - Over half of ransomware attacks (56%) succeeded in encrypting data, including 16% where data was both encrypted and stolen.
- **When data is encrypted, attackers have a roughly 50-50 chance of receiving a ransom payment**
  - 48% of organizations whose data was encrypted paid the ransom.
  - The four-year average is now 50% ransom payment after encryption.
- **Ransom demands are decreasing but attackers ask for more when they gain hard-to-fix access to a privileged system**
  - The median ransom demand fell to $698,000, continuing a multi-year downward trend from a median of $1.3 million in the 2025 report and $2 million in the 2024 report.
  - 59% of ransom demands from attacks that started with an exploited vulnerability on the firewall are for $1M or more, compared to 48% of all demands.
- **Ransom payments are falling, with victims often successful in negotiating a lower amount than originally demanded**
  - The median ransom payment is now $769,000, a considerable drop from the $1 million reported last year.
  - Just under half (48%) of payments were $1 million or more, down from 52% in the previous year.
  - Almost half (51%) of organizations that paid a ransom paid less than the demanded amount, which closely matches the 2025 report (53%) and is 7% higher than the 2024 report (44%).
- **The cost to recover from a ransomware attack has increased**
  - The average (mean) cost to recover from a ransomware attack excluding any ransom paid is now $1,700,200, an 11% increase from the $1,525,716 average in the 2025 report.
- **Having data encrypted almost always has repercussions for members of the IT/cybersecurity team**
  - 99% of ransomware victims that had data encrypted said it affected their IT/cybersecurity team.
  - Increased anxiety or stress about future attacks is the most common impact (41%), followed by increased pressure from senior leaders (40%).
  - Increased recognition from senior leaders (36%, up from 31% in the 2025 report) was the only impact that rose year over year.

Attack and defense methods

Root causes of attacks

The leading technical root causes of ransomware changed in this year's report. Malicious email (26%) and phishing (24%) were the top two root causes of ransomware attacks, accounting for half of all incidents. This represents a significant change from prior years, when exploited vulnerabilities consistently led the rankings.

Reports of exploited vulnerabilities fell from 32% in the 2025 report to 18% in the 2026 report. However, given the speed and scale of frontier AI's vulnerability discovery capabilities, organizations should remain alert to the possibility of an increase in ransomware attacks where the root cause is an exploited vulnerability in the year ahead.

Compromised credentials remained the third most common root cause at 23%, consistent with prior years.

79% of attacks started with an identity-based approach, either securing credentials for abuse or exploiting credentials that had already been secured. This highlights why identity security is a critical piece in a holistic security posture.

Technical root cause of ransomware attacks (2023–2026)

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

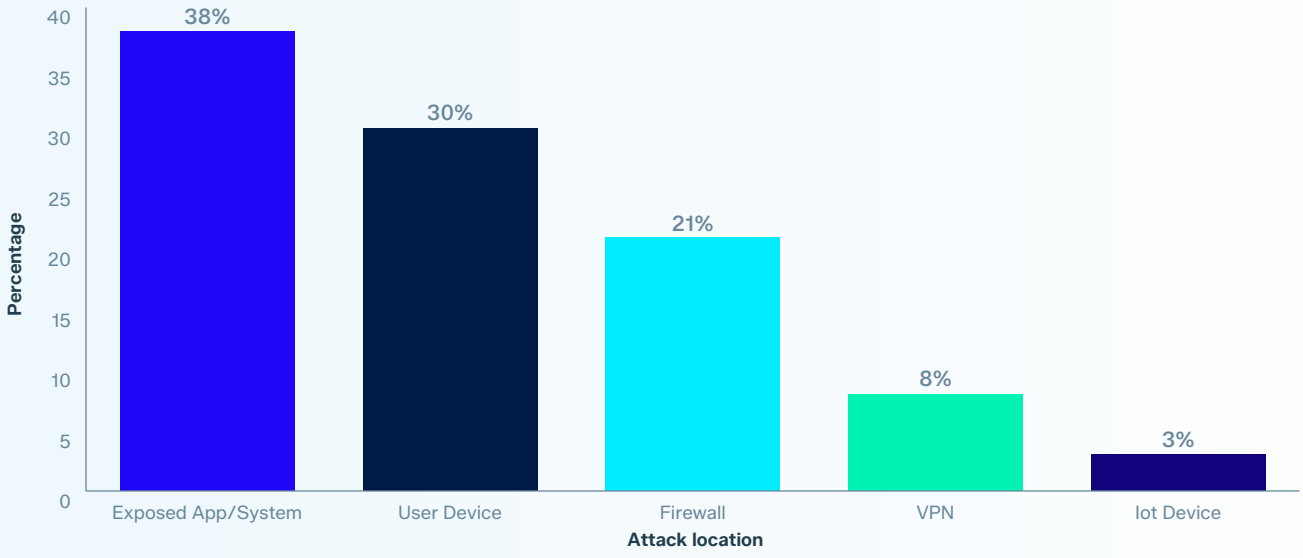
NEW RESEARCH

Where attacks start

This year, for the first time, we reveal where the root cause took place within the organizational environment. Understanding where attacks start is a key insight to inform risk reduction strategies. Across the ransomware incidents that started with an exploited vulnerability, compromised credentials, or a brute force attack, **exposed applications and systems were the most common attack entry point overall (38%)**, followed by user devices (30%) and firewalls (21%).

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.

Ransomware attack locations



You said the root cause was an exploited vulnerability, compromised credentials, or a brute force attack -where did this happen in your environment? n=1,022

Diving deeper, the data reveals how prevalent compromised credentials are across exposed apps and systems, firewalls, VPNs, and IoT devices.

Most common root causes for each location

Root cause	In an exposed application or system	In our firewall	In our VPN	In an IoT device
Compromised credentials	59%	41%	44%	48%
An exploited vulnerability	31%	33%	41%	36%
Brute force attack	10%	26%	15%	16%

You said the root cause was an exploited vulnerability, compromised credentials, or a brute force attack - where did this happen in your environment? Selection of responses. n=711

Compromised credential attacks were especially dominant in exposed applications and systems (59%), reinforcing the importance of securing externally accessible assets and identity controls.

Rebasing the same data comparison revealed the most popular targets for compromised credentials and brute force attacks.

Where ransomware attacks start

Attack location	Total %	Compromised credentials %	Brute force attack %
In an exposed application or system	38%	46%	30%
On a user's device (on or off the network - e.g. laptop, desktop)	30%	27%	13%
In our firewall	21%	18%	44%
In our VPN	8%	7%	9%
In an IoT device	3%	3%	4%

You said the root cause was a compromised credentials or brute force attack - where did this happen in your environment? Selection of responses. n=628

Different attack types targeted different locations.

- Compromised credential attacks concentrated on exposed applications and systems (46%), followed by users' devices.
- Brute force attacks targeted firewalls at a high rate (44%), highlighting the importance of rate-limiting and account lockout policies on network perimeter devices.

NEW RESEARCH

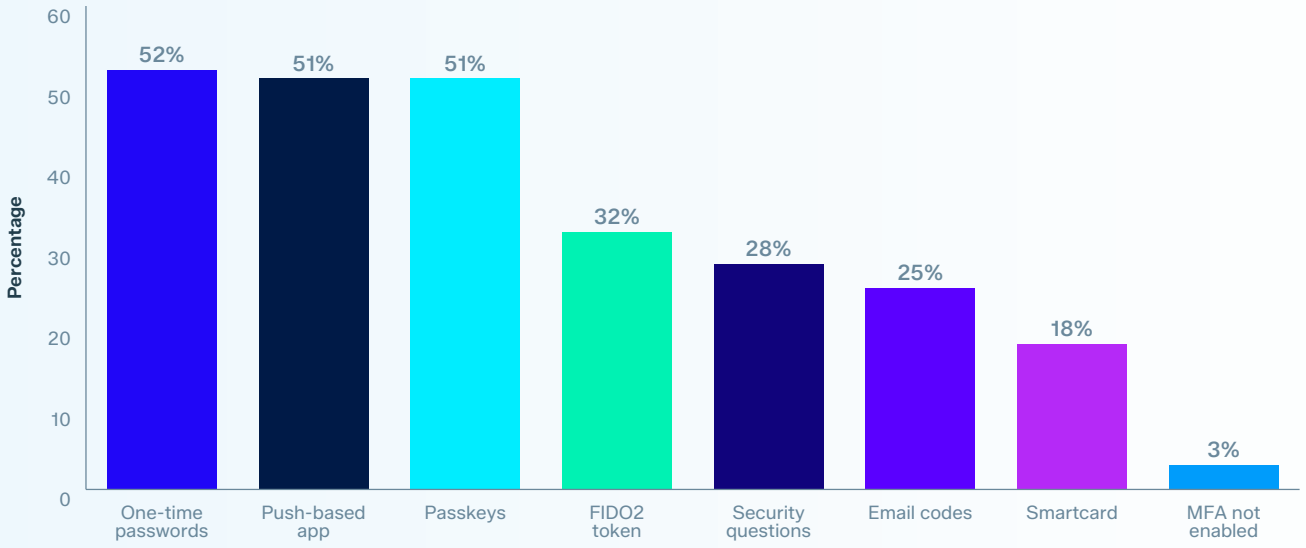
The role of multi-factor authentication (MFA)

This year also introduces brand new insights into the role of MFA in ransomware attacks.

Among organizations where compromised credentials were the root cause of the ransomware attack, **97% had multi-factor authentication enabled in some capacity at the time of the incident**. One-time passwords (52%), push-based applications (51%), and passkeys (51%) were the most widely deployed methods, with respondents reporting, on average, the use of 2.5 MFA methods.

The high percentage of ransomware victims that had MFA deployed at the time of the attack indicates that it may not have been fully deployed across all relevant systems, creating gaps for attackers to exploit. It also suggests that, while MFA remains an essential element of effective cyber defense strategies, it is not sufficient on its own to prevent credential-based attacks as bypass techniques continue to evolve.

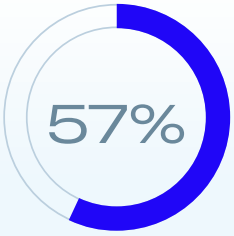
MFA methods enabled at the time of attack



What type of multi-factor authentication was enabled at the time of the attack, if any? Base: The attack occurred due to compromised credentials. n=503

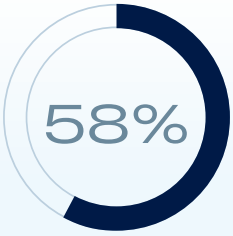
What made organizations vulnerable

For the second year, there was no single dominant organizational factor that left organizations exposed to attacks, with respondents reporting a broad range of challenges — from missing or poor protection and a shortage of people/skills, to gaps in their security.



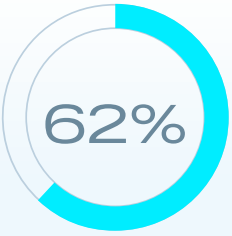
Protection issues

(lack of or poor-quality protection solutions)



Resourcing issues

(lack of expertise or people/capacity)



Security gap

(known or unknown)

Security gaps were the most cited category of operational root causes for the second year in a row at 62%, followed by lack of people or skills (58%), and lack of, or poor-quality, protection (57%).

Encouragingly, all individual factors (except one) saw a decline year over year, with **human error (35%) the only operational factor that increased in the last year**.

As in 2025, ransomware victims reported multiple organizational challenges, with **2.5 factors cited on average**, down from 2.7.

Top 7 operational root causes of ransomware attacks

Rank	2025	%	Rank	2026	%
1	Lack of expertise	40.2%	1	Lack of protection	36.4%
2	Unknown security gap	40.1%	2	Unknown security gap	36.3%
3	Lack of people/capacity	39.4%	3	Known security gap	36.0%
4	Lack of protection	39.0%	4	Lack of people/capacity	35.3%
5	Known security gap	38.2%	5	Human error	35.3%
6	Poor quality protection	37.1%	6	Lack of expertise	35.1%
7	Human error	34.2%	7	Poor quality protection	32.6%

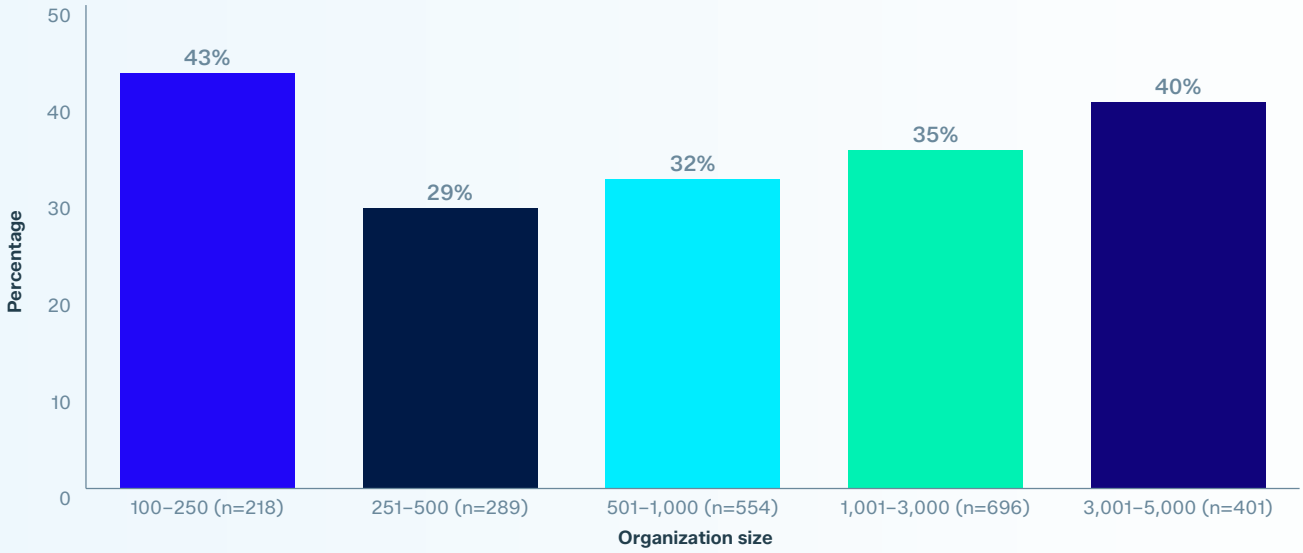
Why do you think your organization fell victim to the ransomware attack? n=3,400 (2025), n=2,158 (2026)

35%

Human error: the one constant. The only operational root cause of attacks that did not decline from the 2025 report.

As you may expect, lack of people/capacity was cited heavily by small organizations in the 100-250 range. However, four in 10 enterprises with 3,001-5,000 employees also cite capacity challenges at a rate only 3% below the 100-250 employee organizations, indicating that resourcing doesn't always get easier with scale.

Lack of people/capacity contributed to falling victim to ransomware



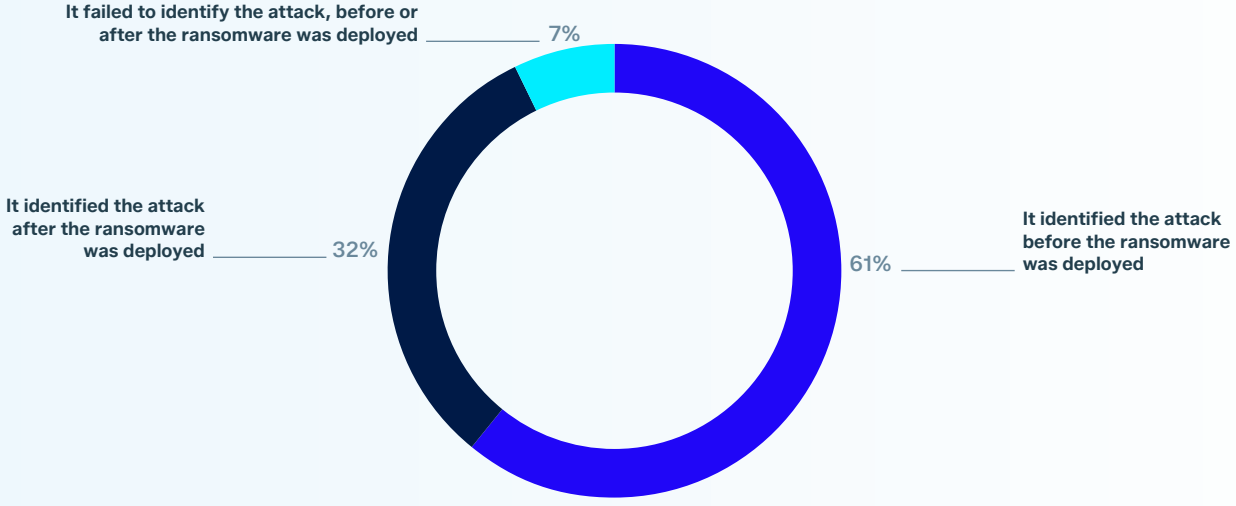
Why do you think your organization fell victim to the ransomware attack? We did not have a sufficient number of cybersecurity experts monitoring our systems at the time of the attack. Base numbers in the chart.

NEW RESEARCH

The role of firewalls in ransomware defenses

61% of victims reported that their firewall detected the ransomware attack before the payload was detonated, and 32% said the firewall identified it after the ransomware was deployed. Only 7% reported that their firewall did not identify the attack at all.

What role did your firewall play in identifying the attack?



What role did your firewall play in identifying the attack? n=2,158

The 7% of victims whose firewall did not detect the attack experienced the worst encryption outcomes, with 71% having their data encrypted, compared to 50% when the firewall detected the attack before the ransomware was deployed. Detection after ransomware deployment — typically post-incident identification of signals that were subsequently associated with the ransomware attack — correlated with a 65% encryption rate.

The findings make clear that firewalls play a key role in helping detect ransomware attacks, with telemetry from these devices providing valuable early signals of adversary activity. When combined with insights from across the security environment, for example from endpoint protection or email security solutions via an XDR tool or MDR service, firewall telemetry can help defenders to detect and block ransomware attacks before data is encrypted.

Impact of firewall-assisted attack identification on encryption rate

	It identified the attack before the ransomware was deployed	It identified the attack after the ransomware was deployed	It failed to identify the attack, before or after the ransomware was deployed
Cybercriminals succeeded in encrypting their data	50%	65%	71%
Cybercriminals were unsuccessful in encrypting their data	50%	35%	29%

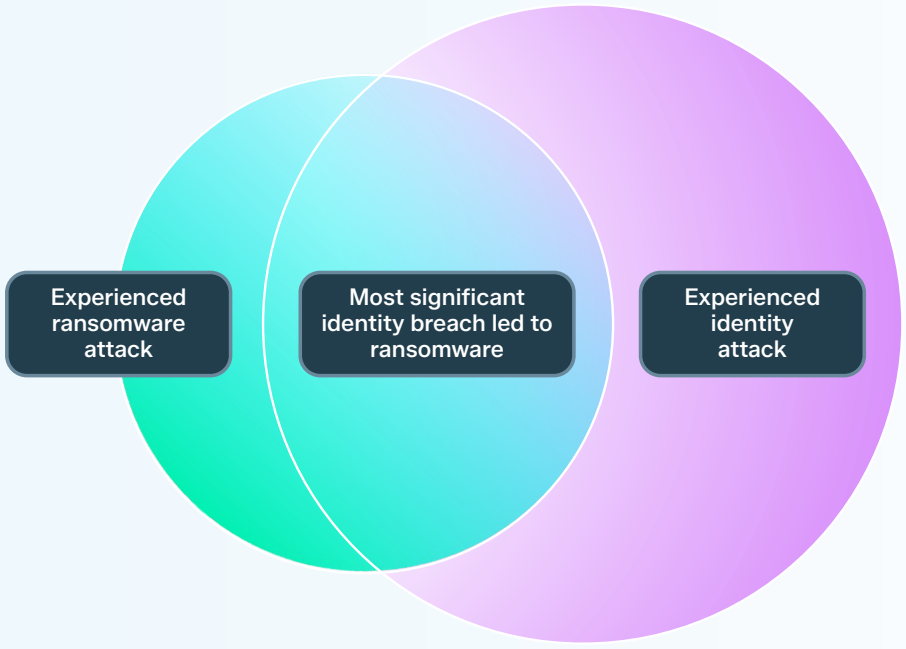
What role did your firewall play in identifying the attack? Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? n=2,158

Firewalls hold a very privileged position in the organizational infrastructure, opening the business up to more significant impacts when it is compromised compared to other parts of the environment. If attackers successfully exploit a vulnerability on the firewall, they often gain extensive access across the business. The difference in ransom demands for these scenarios supports this point: **59% of ransom demands from attacks that started with an exploited vulnerability on the firewall are for $1M or more**, compared to 48% of all attacks.

NEW RESEARCH

The identity-ransomware connection

One of the most striking findings in this year's research is the confirmation of the direct link between identity attacks and ransomware. Among organizations that were hit by ransomware in the past year, two-thirds (67%) confirmed that the ransomware incident was the same event as their most significant identity attack. Although not all the attacks resulted in data encryption, this finding establishes identity compromise as a dominant ransomware delivery mechanism.



Data split: In the last year, has your organization been hit by ransomware? n=5,000. Has your organization experienced any identity-related security breaches in the past 12 months? n=5,000. [If yes to both] Was that ransomware incident the same event as your most significant identity-related attack?

Data encryption and recovery

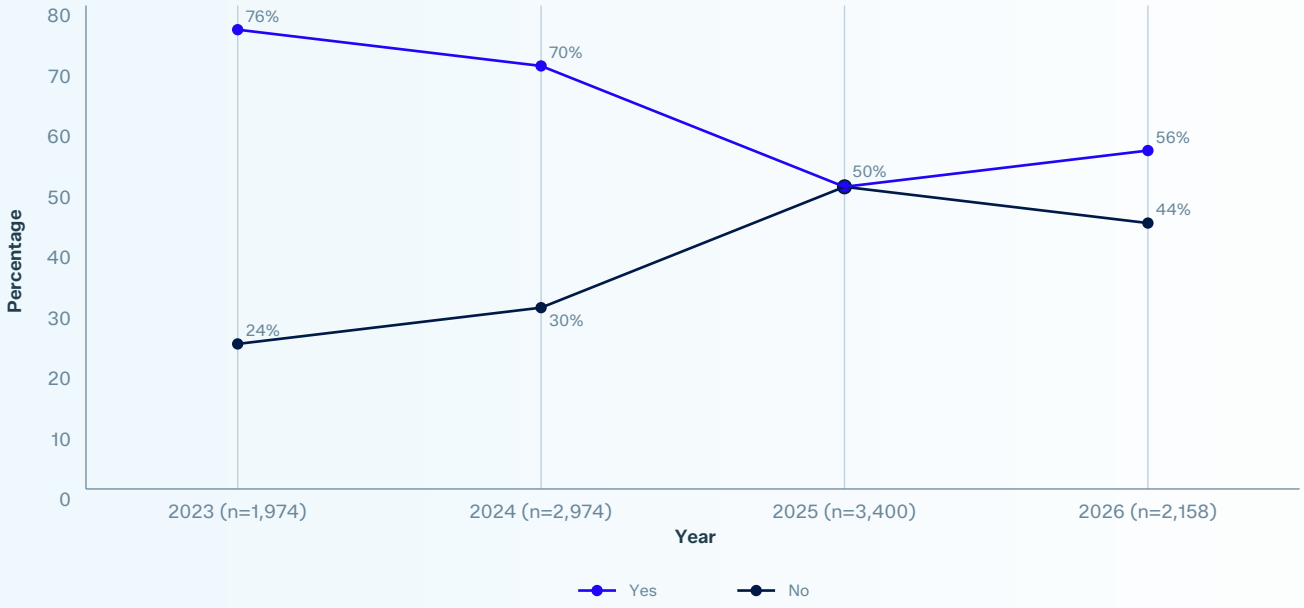
Data encryption rate

Over half of ransomware attacks (56%) succeeded in encrypting data. This includes 40% where data was encrypted only and 16% where data was both encrypted and stolen. 41% of attacks were stopped before encryption, while 2% involved extortion-style attacks without encryption.

+6%

The increase in ransomware encryption rate from last year's report.

Was data encrypted in the attack? (Summarized: Yes/No)

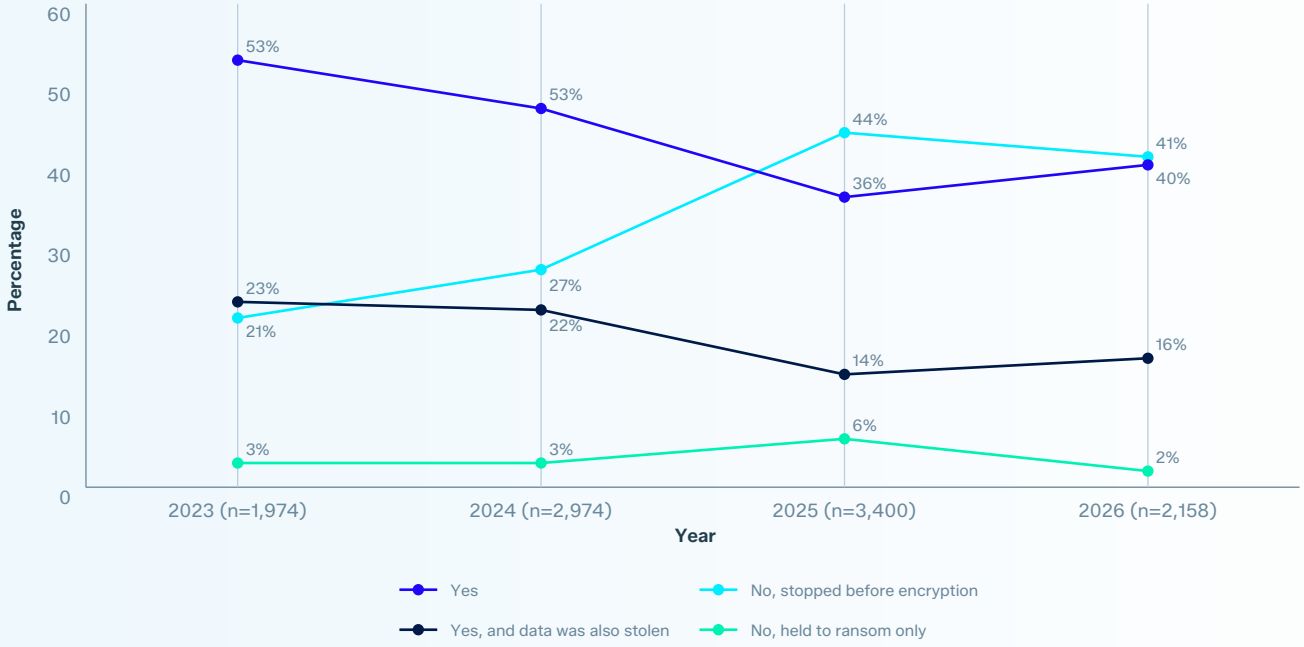


Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Summarized answers: Yes / No. Base numbers in the chart.

While the encryption rate remains well below the 76% peak in the 2023 report, it has edged upward from the 50% low point in the 2025 report. This reversal warrants attention: after two years of declining encryption success, attackers appear to be regaining some ground.

The 16% of attacks involving both encryption and data theft are particularly concerning, as these dual-impact attacks give attackers multiple leverage points for extortion.

Was data encrypted in the attack?

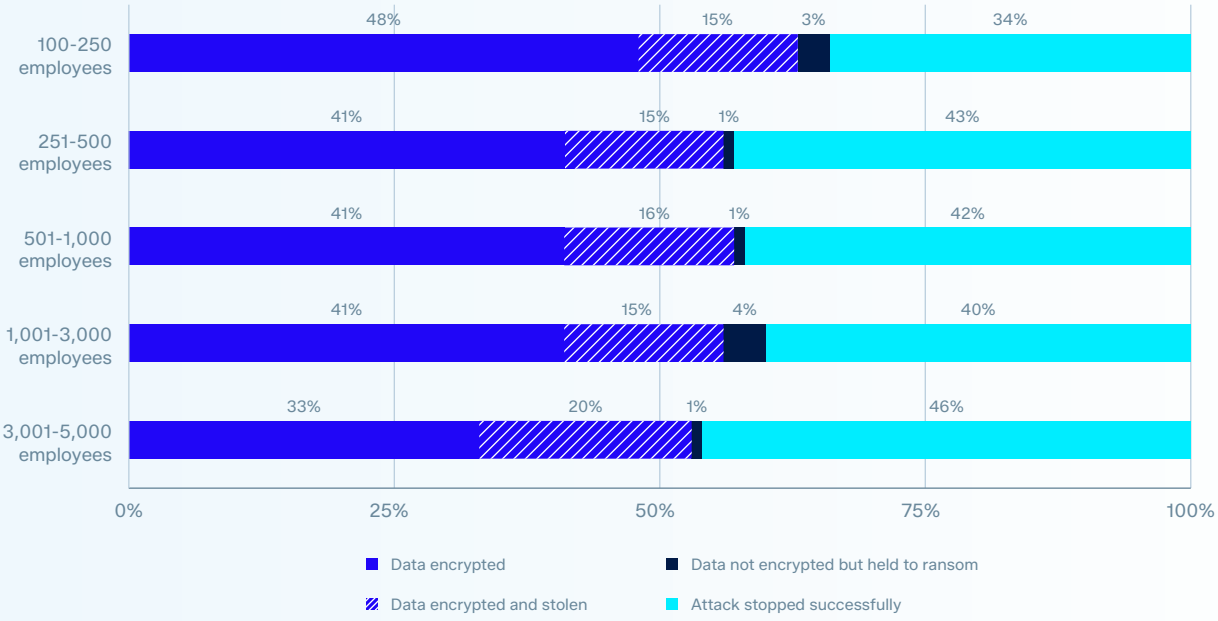


Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? (Full list of answer choices) Base: organizations hit by ransomware. Base numbers in the chart.

Encryption outcomes varied by organization size, with **the largest organizations surveyed (3,001–5,000 employees) most likely to stop attacks before encryption or extortion (46%)** compared to just 34% for the smallest (100–250 employees).

However, when attacks did succeed in encrypting data at larger organizations, victims were more likely to also experience data theft, with the "encrypted and stolen" rate reaching 20% for the largest size band versus 15% for most others. Exfiltrating data in addition to deploying ransomware gives attackers a secondary opportunity to monetize the attack.

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=2,158

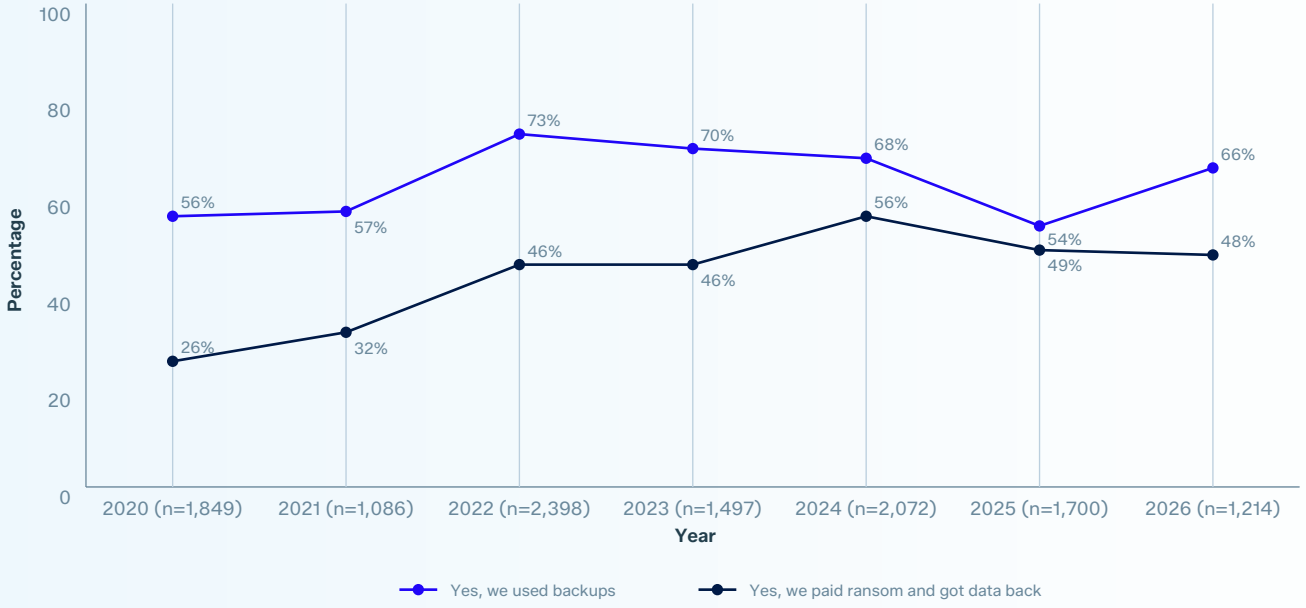
How organizations recovered encrypted data

Backup-based recovery surged to 66% of attacks where data was encrypted, up from 54% in the 2025 report. This sharp rebound suggests that organizations have renewed their investment in backup infrastructure after a drop in usage in 2025 and are increasing their resilience against ransom demands.

+12%

The increase in use of backups to recover from ransomware attacks from 2025 to 2026.

How did your organization recover data after ransomware attacks



How did your organization get the data back? Base: Organizations that had data encrypted. Base numbers in the chart. Multiple answers permitted, so percentages may exceed 100%.

The proportion of organizations paying the ransom to recover data dropped to 48%, the lowest rate in the last 3 years. Only 2% of organizations reported getting no data back at all, indicating that when data is encrypted, recovery through some means is nearly universal.

Ransom demands and payments

Ransom demands

The median ransom demand fell to $698,000 in this year's report, continuing a multi-year downward trend. This represents a drop of 65% over the last two years. The mean ransom demand has also fallen in this period, coming in at $3,126,372, a 28% reduction since the 2024 report.

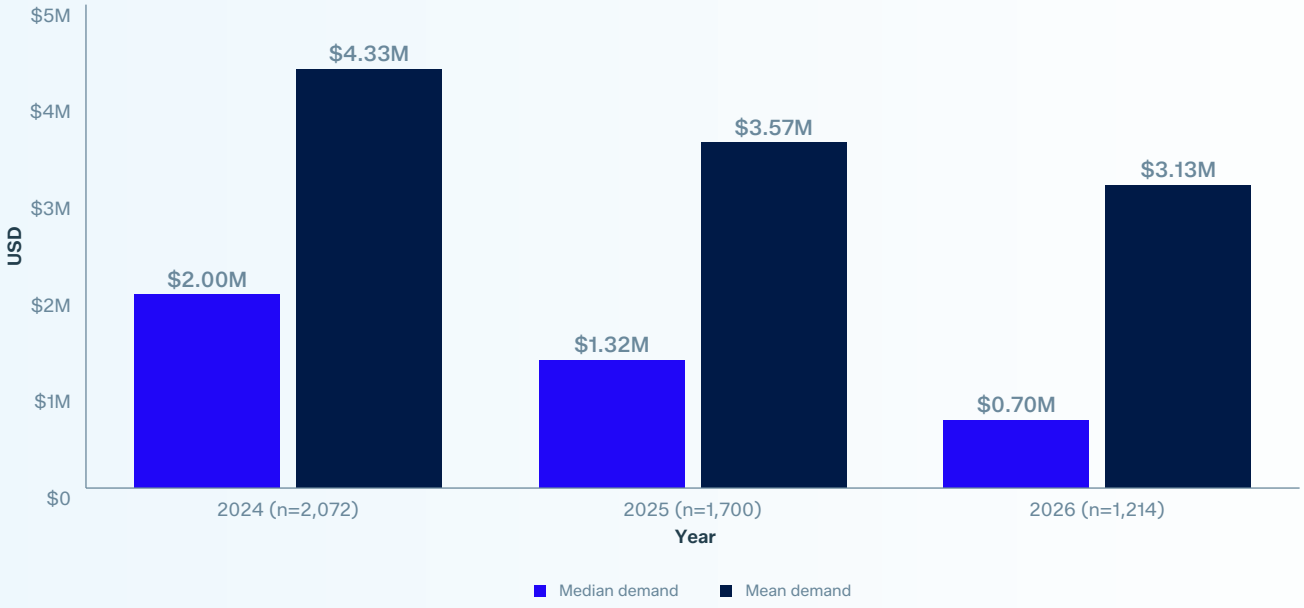
The widening gap between the mean and median demands signals a heavily skewed distribution: a small number of very large demands inflate the mean, while the typical organization faces a demand just under $700,000.

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

$698K

The median ransomware demand in the past year.

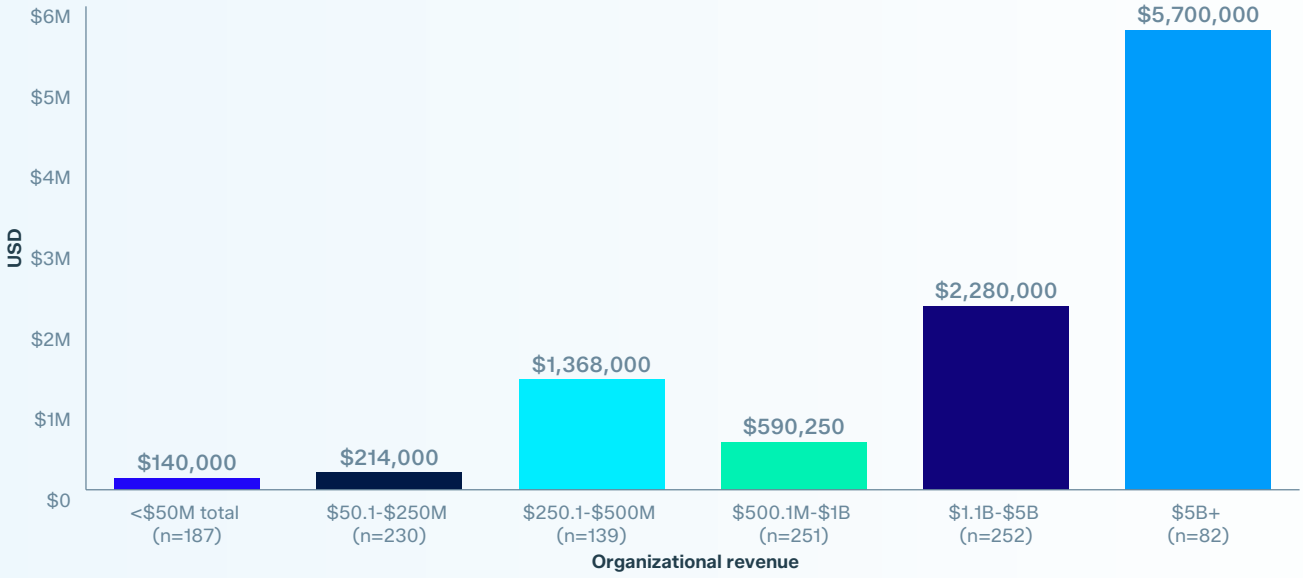
Mean and median ransom demands



How much was the ransom demand from the attacker(s)? Base: organizations that had data encrypted. Base numbers in the chart. Excludes outlier demands of $40M or higher.

Ransom demands scale sharply with organizational revenue. Organizations with revenue under $50 million faced median demands of approximately $140,000, while those with revenue above $5 billion faced median demands of $5.7 million. This pattern strongly suggests that attackers conduct reconnaissance to calibrate demands based on perceived ability to pay.

Median ransom demand



How much was the ransom demand? Base: organizations that had data encrypted. Base numbers in the chart. Excludes outlier demands of $40M+.

Ransom payments

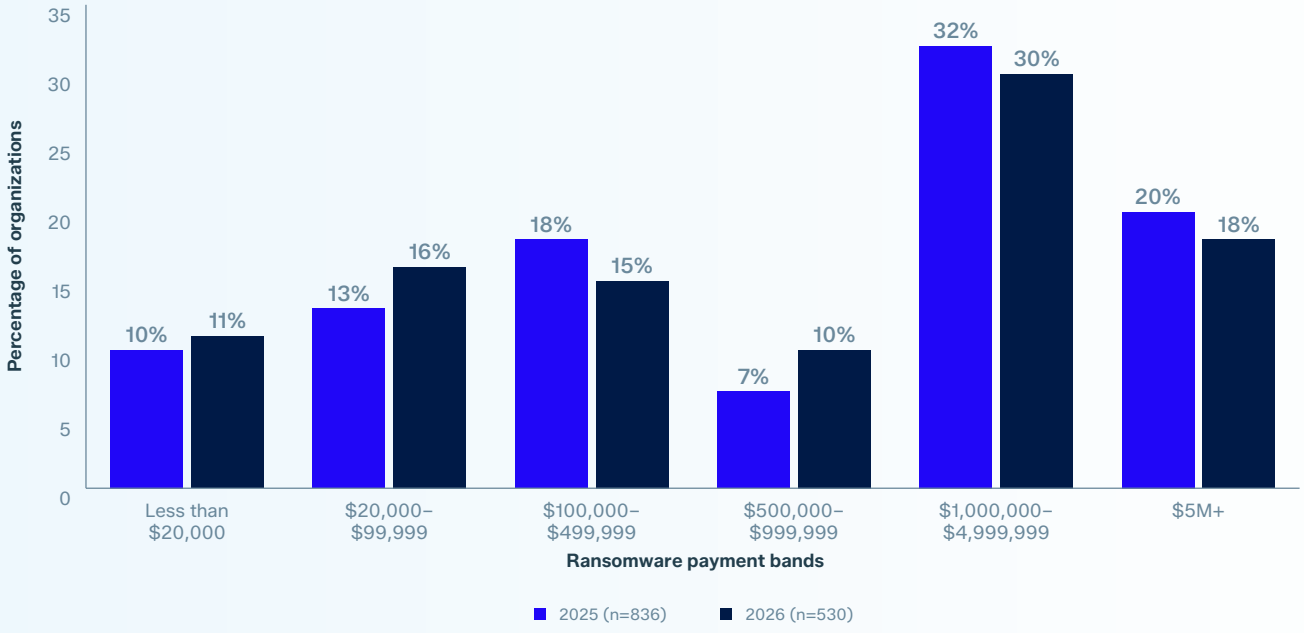
530 organizations that paid the ransom shared the amount with us, revealing that the median ransom payment is now $769,000, a considerable drop from the $1 million reported last year. Just under half (48%) of payments were for $1 million or more, down from 52% in the previous year.

Looking at the full distribution of payments reveals a clear shift toward the middle of the range. The two highest bands ($1M–$5M and $5M+) both saw declines from last year's report, while the $20,000–$99,999 and $500,000–$999,999 bands each grew, suggesting attackers and victims are increasingly settling in low-to-mid-tier payment territory.

$769K

The median ransomware payment in the past year.

Ransomware payment bands

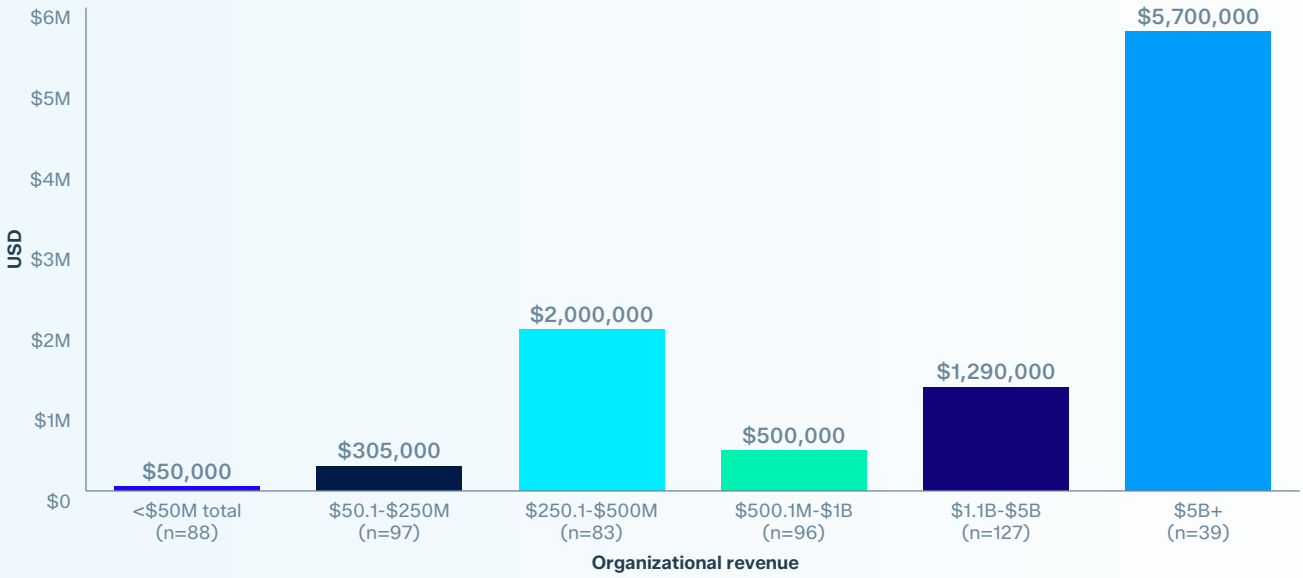


How much was the ransom payment that was paid to the attackers? Base numbers in the chart.

Splitting ransom payments by organizational revenue showed a spike at the $250.1M–$500M range, with victims paying a median of $2M. This is more than any other segment bar the very largest ($5B+ annual revenue) and four times higher than for organizations with $500.1M–$1B revenue.

The ransom demand data shows a similar spike at the $250.1M–$500M revenue tier, with median demands of $1.37M compared to $590K in the band above it, suggesting that this segment is particularly exposed to the impacts of ransomware.

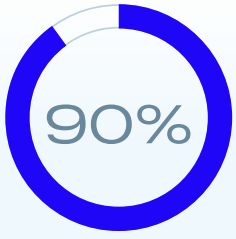
Median ransom payment



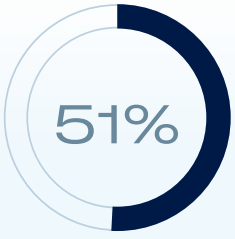
How much was the ransom payment that was paid to the attackers? Base: organizations paid the ransom. Base numbers in the chart.

Actual payments vs. initial demands

507 organizations shared both their ransom demand and the ransom payment, revealing how effective organizations are at negotiating with attackers. **The median payment was 90% of the demand (mean: 85%)**, with just over half (51%) paying less than the initial demand, 30% paying the actual demand, and 18% paying more. These numbers are very close to last year's figures, revealing that the relationship between demands and actual payments has remained relatively stable.

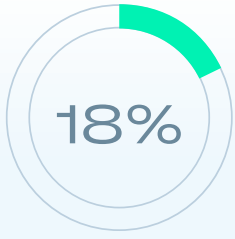


The **median** ransom payment percentage



Payments **less** than the initial ransom demand

Payments **matched** the initial ransom demand



Payments **more** than the initial ransom demand

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=507

As shared above, median ransom demands usually increase when the targeted organization has higher revenue, but different revenue bands have varying levels of success negotiating final payments down.

Mid-sized organizations ($50M-$250M revenue) are least successful at reducing ransom payments, with 25% paying more than the demand. The largest enterprises ($5B+ revenue) are the most effective at negotiating lower ransoms, with 11% paying more than the initial demand and 57% paying less — the highest percentage of all cohorts.

The higher revenue organizations (above $500 million) had better success paying below the ransom demand, indicating that at higher ransom payments, attackers were more willing to allow discounts for larger overall ransoms. Organizations under $50M in revenue also had modest success reducing their ransom payments.

Ransom percentage paid (median) by organization revenue

Revenue	Proportion of ransom paid (Median)
<$50 million	95%
$50.1–$250 million	100%
$250.1–$500 million	100%
$500.1 million–$1 billion	83%
$1.1 billion–$5 billion	83%
$5 billion or more	83%

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=507

Ransom payments by sector

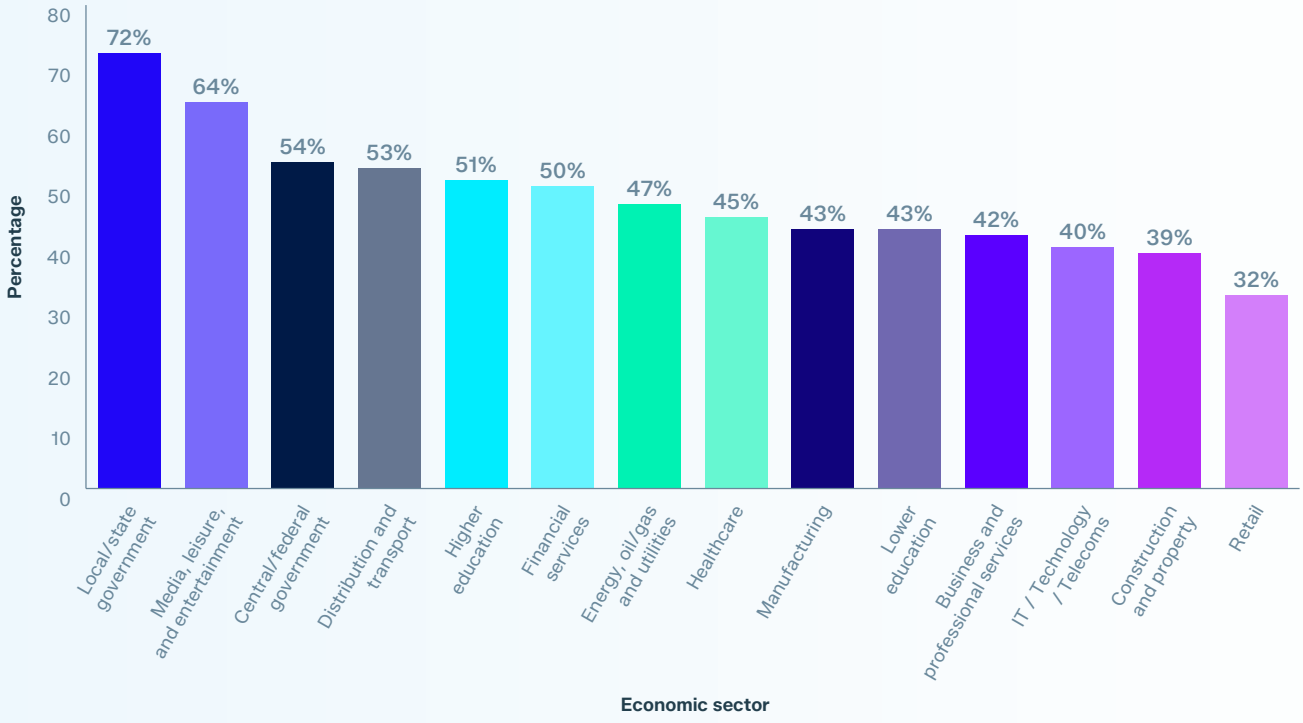
Propensity to pay the ransom varies by sector. **Local/state government (72%) and media, leisure, and entertainment (64%) were most likely to pay the ransom**, reporting more than double the rate of retail (32%).

Public sector and media organizations often face acute pressure to restore citizen-facing or time-sensitive services quickly, while retail organizations may be more willing to "weather the storm".

Retail

was the sector with the lowest occurrence of paying ransomware attackers (32%).

Percent of organizations that paid the ransom by sector



How did your organization get the data back? We paid the ransom. Base: organizations that had data encrypted. n=1,214

Business and human impact

Ransomware recovery costs

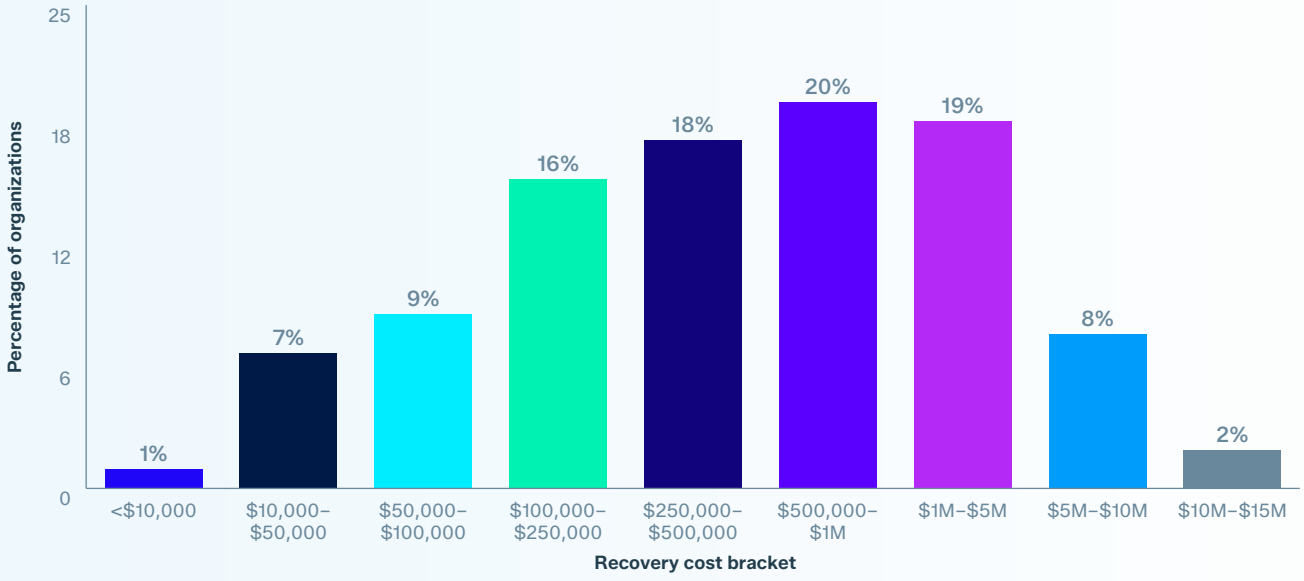
The average (mean) cost to recover from a ransomware attack excluding any ransom paid was $1,700,200 in the past year. This represents an 11% increase from the $1,525,716 average in the 2025 report but remains 38% below the $2,730,684 peak recorded in the 2024 report. The median cost comes in at $375,000, unchanged from last year's report.

2024	2025	2026
$2.73 million	$1.53 million	$1.70 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=2,158 (2026), n=3,400 (2025), 2,974 (2024)

Recovery costs span a wide range: 20% of organizations incurred bills between $500,000 and $1 million, while 19% spent between $1 million and $5 million.

The recovery costs of ransomware attacks



What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack? n=2,158

Recovery time

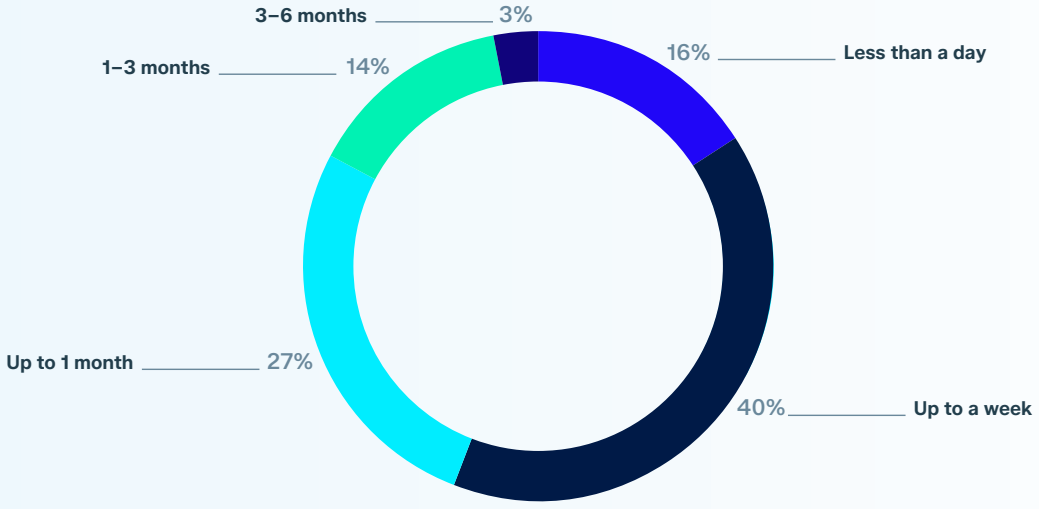
Over half of organizations (55%) recovered from ransomware within one week (16% in less than a day) and 83% recovered within one month. Only 3% took longer than three months.

The 55% one-week recovery rate is up 3% year over year. The average number of weeks to recover remained at three (2026 and 2025 reports) down from five weeks in the 2024 report.

55%

Percentage of organizations that recovered within one week from the ransomware attack.

How long it took to recover



How long did it take your organization to fully recover from the ransomware attack? n=2,158

Human impact of ransomware

Virtually all organizations that had data encrypted (99%) reported lasting repercussions on their IT and cybersecurity teams. The most cited impacts were increased anxiety or stress about future attacks (41%) and increased pressure from senior leaders (40%). For more than one in five victims (21%), the leadership team was replaced as a direct result of the attack.

Increased recognition from senior leaders was the only impact that rose year over year, climbing from 31% to 36%. Every other measured repercussion declined, including changes to team priorities (down seven points), ongoing workload increases (down seven points), and team restructuring (down five points).

21%

The percentage of IT/cybersecurity leadership teams that were replaced due to the ransomware attack.

How ransomware affected IT/cybersecurity teams

Repercussions	2026	Change from 2025
Increased anxiety or stress about future attacks	41%	-
Increased pressure from senior leaders	40%	-
Increased recognition from senior leaders	36%	↑ 5pp
Changes to team/organizational structure	32%	↓ 5pp
Change of team priorities/focus	32%	↓ 6pp
Feelings of guilt that the attack was not stopped	31%	↓ 3pp
Ongoing increase in workload	31%	↓ 7pp
Staff absence due to stress/mental health issues	29%	↓ 2pp
Team's leadership was replaced	21%	↓ 4pp

What repercussions has the ransomware attack had on the people in your IT/cybersecurity team? Base: Organizations that had data encrypted. n=1,214 (2026), n=1,700 (2025)

The rise in executive recognition may itself be a contributing factor to the positive operational trends seen elsewhere in this report, as greater leadership attention can translate into better resourcing and organizational support for cybersecurity programs.

Recommendations

Strengthen identity security as a ransomware defense. Two-thirds of ransomware victims confirmed their ransomware incident was the same event as their most significant identity attack, underscoring the tight link between identity compromise and ransomware. Organizations 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. As the survey results showed (97% of organizations had enabled MFA in some capacity at the time of their attack), MFA alone is not enough to stop attacks, and it needs to be comprehensively enabled.

Strengthen endpoint protection for AI frontier models. Frontier AI is accelerating vulnerability discovery and exploitability. Having strong endpoint defenses that automatically block exploit-based attacks is essential.

Bring in specialist support or MDR. Lack of capacity, skills, and expertise is a continuing theme for both SMBs and enterprises. Dealing with AI-augmented threats will put even more strain on these areas as security professionals try to stay up to date with fast-changing AI technology. Unless you can confidently staff a security operations team in-house, look to work with an external specialist to fill the gap, either directly with a 24/7 coverage MDR vendor or with a managed services provider. Vendors that can resolve more incidents end-to-end with AI and automation will also be a force-multiplier that can help close your skills and capacity gaps.

Prioritize email security. With phishing and malicious email now accounting for half of all ransomware root causes in this report, organizations should deploy advanced email filtering, implement DMARC/DKIM/SPF protocols, and invest in regular phishing awareness training. The shift toward email-based attacks suggests that technical vulnerability patching alone is insufficient.

Invest in backup and recovery infrastructure. Organizations that maintained robust backup systems recovered encrypted data at nearly record rates in the past year. Backups 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. The 14-percentage-point drop in exploited vulnerabilities as a root cause is encouraging, but these attacks remain a major attack vector and are likely to increase as frontier AI models find new vulnerabilities faster. Organizations 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. 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 solutions to enable firewall telemetry to help detect ransomware attacks before payloads are deployed.

Support cybersecurity teams through the aftermath. With 99% of affected teams reporting repercussions, the human cost of ransomware is nearly universal. Organizations should establish clear post-incident support protocols and ensure that the rising executive recognition translates into sustained investment in people, not just technology.

Conclusion

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

There are genuine signs of progress: ransom demands and payments are declining, backup-based recovery has surged to near-record levels, and organizations are increasingly effective at negotiating outcomes when they do pay. The dramatic decline in exploited vulnerability attacks suggests that AI-driven discovery and sustained investment in patch management are paying dividends.

The most encouraging signal in the data may be the rise in executive recognition of cybersecurity teams. When leadership pays attention, resources follow. The positive operational trends in this report, from improved backup usage to better negotiation outcomes, may reflect exactly that dynamic.

At the same time, the challenges that remain are significant. Over half of ransomware attacks still succeed in encrypting data, recovery costs average $1.7 million per incident, and the human toll on cybersecurity teams is nearly universal.

The finding that two-thirds of ransomware victims traced their incident back to an identity compromise **underscores the critical role that identity security plays in the ransomware defense chain**. Organizations that treat identity as a foundational security layer, rather than an afterthought, are better positioned to prevent attacks from succeeding in the first place.

Organizations also need to prepare for **the defining cybersecurity challenge of the next decade: AI-augmented threats**. The data already hints at why: 62% of victims cited a security gap, known or unknown, as a factor in their attack, and 58% pointed to a lack of people or skills. Both 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.

The pattern across this year's findings — from the better outcomes when firewalls detected attacks early to the surge in backup-based recovery — points in a consistent direction: **when defenses operate together rather than in isolation, results improve**. 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 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.

Methodology

This survey was conducted by Vanson Bourne on behalf of Sophos in Q1 2026. 2,158 IT and cybersecurity decision-makers from organizations that had been hit by ransomware in the previous 12 months were interviewed across 17 countries: USA, Brazil, Chile, Colombia, Mexico, UK, France, Germany, Italy, Spain, Switzerland, Australia, India, Japan, Singapore, South Africa, and UAE. Respondents came from organizations with 100 to 5,000 employees across 15 industry sectors.

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

2026-06-09 EN (DD)