SOPHOS

THE STATE OF RANSOMWARE IN EDUCATION 2025

Findings from an independent survey of 441 IT and cybersecurity leaders in the education sector across 17 countries whose organizations were hit by ransomware in the last year.

A Sophos Whitepaper. August 2025

Introduction

Welcome to the fifth edition of the annual Sophos State of Ransomware in Education report, which reveals the reality of ransomware for both lower education providers (for students up to 18 years old) and higher education providers (for students over 18 years old) in 2025.

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

Drawing on the real-world experiences of 441 IT and cybersecurity leaders, 243 from lower education and 198 from higher education institutions hit by ransomware in the past year, this report offers unique insights into:

- Why education providers fall victim to ransomware.
- What happens to the data.
- Ransom demands and payments.
- The human and business 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 full report is based on the findings from an independent, vendor-agnostic survey of 3,400 IT/cybersecurity professionals whose organizations were hit by ransomware in the last year, including 441 from the education sector. The research 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.

Respondents span 17 countries, ensuring that the survey results reflect a broad and diverse range of experiences. The report includes comparisons with the findings from our previous reports, enabling year-over-year juxtaposition. All financial data points are in U.S. dollars.

Key findings

Why education providers fall victim to ransomware

- **Phishing** is the top reported technical root cause of ransomware attacks on lower education (22%), but attack methods are evenly spread across phishing, malicious email, exploited vulnerabilities, and compromised credentials. In contrast, higher education continues to see **exploited vulnerabilities** as the leading cause, used in 35% of attacks.
- Looking at organizational root causes, for higher education providers, **unknown security gaps** were the most commonly perceived root cause (49%), while lower education victims cited both **a lack of expertise and a lack of people/capacity** to deal with attacks as the most common reasons they were hit (both 42%).

What happens to the data

- **Data encryption rates in education have fallen to a four-year low:** 29% of attacks in lower education — the lowest of any sector — and 58% in higher education resulted in data encryption.
- 26% of lower education providers and 33% of higher education providers that had data encrypted also experienced **data exfiltration**.
- 97% of education providers that had data encrypted were able to recover it.
- **Backup use for data recovery has dropped** — only 59% of lower education providers that had data encrypted used backups, and 47% of those in higher education.
- Half of lower education victims and 54% of higher education victims **paid the ransom to recover their data**.

Ransoms: Demands and payments

- **Median ransom demands in education fell sharply:** From $3.85M to $1.02M in lower education, and from $3.55M to $697K in higher education—among the lowest demands across all industries surveyed.
- **Median ransom payments also fell sharply.** In lower education, payments dropped to $800K from $6.60M, while higher education saw a decline from $4.41M to $463K — both moving from being among the highest payers in 2024 to among the lowest in 2025.
- Reflecting the broader trend, the **proportion of the ransom demand actually paid also declined.** In lower education, it fell to 84% in 2025 from 115% in 2024, while higher education saw a sharper drop from 122% to 69%.
- Looking closely at **demands vs. payments**, 41% of lower education providers paid what was initially asked, 41% paid less, and 18% paid more. In higher education, only 26% matched the initial demand, while 60% paid less and 14% paid more.

Business impact of ransomware

- In 2025, **average recovery costs in education dropped sharply.** Higher education costs plummeted 77% from $4.02M in 2024 to $0.90M (joint lowest), while lower education, despite a 39% drop from $3.76M last year, reported the highest cost across all sectors at $2.28M.
- **Education providers are getting faster at recovering from attacks**. Half of lower education providers and 59% of higher education providers fully recovered within a week (both up from the 30% reported in 2024).

Human impact of ransomware

Every educational establishment (both lower and higher) that had data encrypted reported that there were **direct repercussions** for their IT/cybersecurity teams:

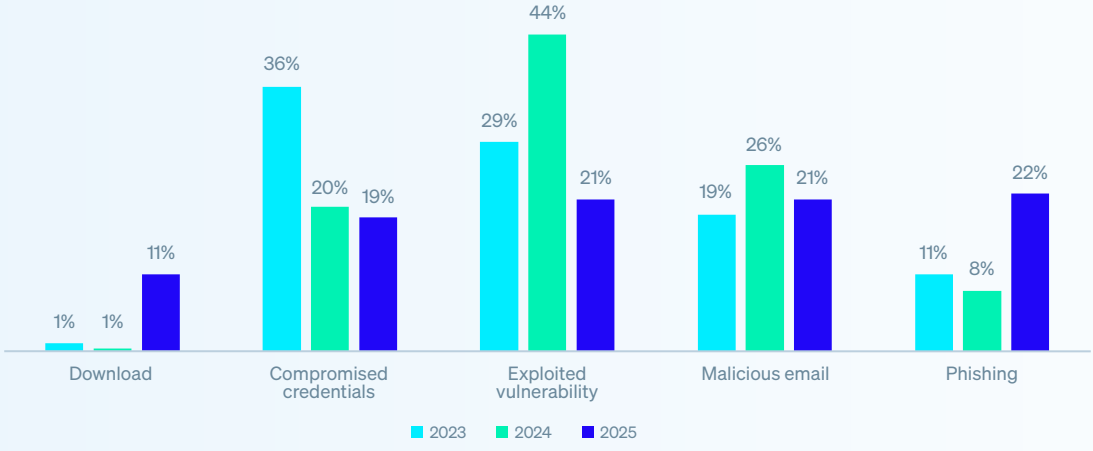
- 41% of education sector-based IT/cybersecurity teams reported **increased anxiety or stress** about future attacks.
- 40% reported **increased pressure** from senior leaders, while 31% reported **increased recognition**.
- 38% cited both **a change of team priorities/focus** and an **ongoing increase** in workload as impacts on their IT/cybersecurity team.
- 37% reported changes to the **team/organizational structure** because of the incident.
- One third (34%) said the team experienced **feelings of guilt** that the attack was not stopped in time.
- 31% of teams 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 education providers fall victim to ransomware

Technical root cause of attacks in education

The top reported technical root cause of attacks varies between lower education and higher education providers. For the first time in our research, **phishing** is the top-reported root cause of attacks on lower education providers, used in 22% of incidents. However, four main vectors (phishing, malicious email, exploited vulnerabilities and compromised credentials) sit within 3% of one another — a uniquely even root cause spread not seen in other sectors.

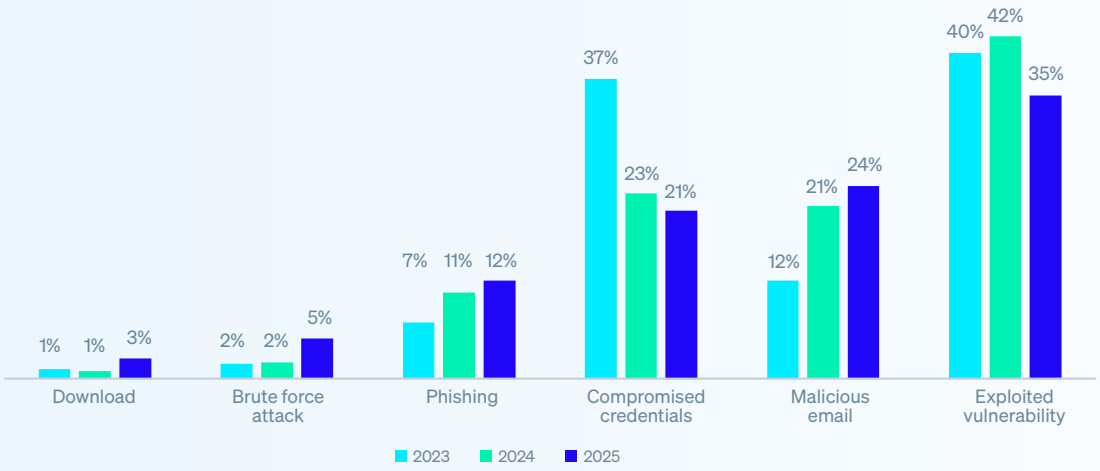
Chart 1: Technical root cause of ransomware attacks in lower education 2023 - 2025



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=243 (2025), 189 (2024), 159 (2023).

In contrast, for the third year running, higher education victims identified **exploited vulnerabilities** as the most common root cause of ransomware incidents, used to penetrate establishments in 35% of attacks, aligning with the majority of industries surveyed. Malicious emails are the second most common attack vector, with the percentage of attacks that used this approach increasing from 21% in 2024 to 24% in 2025. This is followed very closely by compromised credentials, reported by 21% of higher education providers.

Chart 2: Technical root cause of ransomware attacks in higher education 2023 - 2025

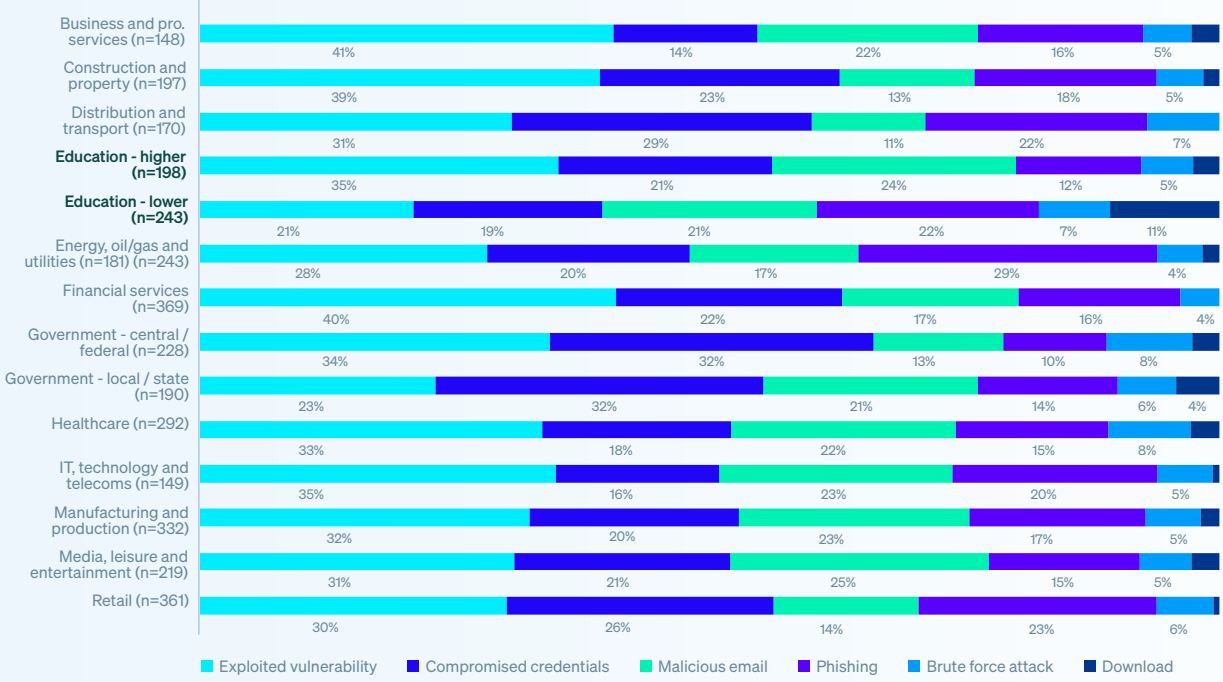


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=196 (2025), 197 (2024), 156 (2023).

The research reveals that while root causes vary by industry, **exploited vulnerabilities are a major vector** for most sectors. Notable exceptions:

- Phishing was the most common root cause cited by both lower education (22%) and energy, oil/gas, and utilities providers (29%).
- **Compromised credentials** were the most commonly perceived attack vector for local/state government organizations — accounting for nearly a third of incidents (32%).

Chart 3: Technical root cause of ransomware attacks split by industry

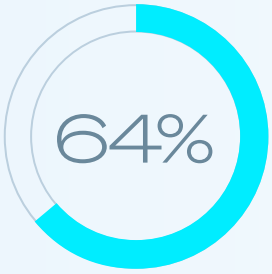


Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. Base numbers in chart.

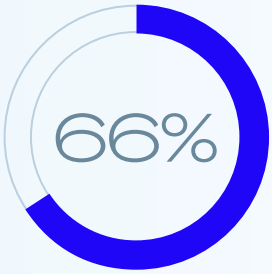
Organizational root cause of incidents in education

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

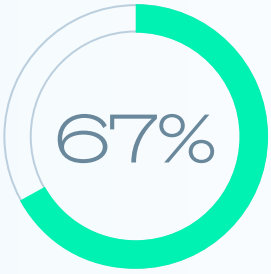
Overall, the organizational root causes are fairly evenly split across protection issues (64%), resourcing challenges (66%), and security gaps (67%).



PROTECTION CHALLENGES
Lack of protection or poor-quality protection solutions that could not stop the attack



RESOURCE CHALLENGES
Lack of human expertise (skills or capacity) to detect and stop the attack in time



SECURITY GAP
Had a known or unknown weakness in their defenses

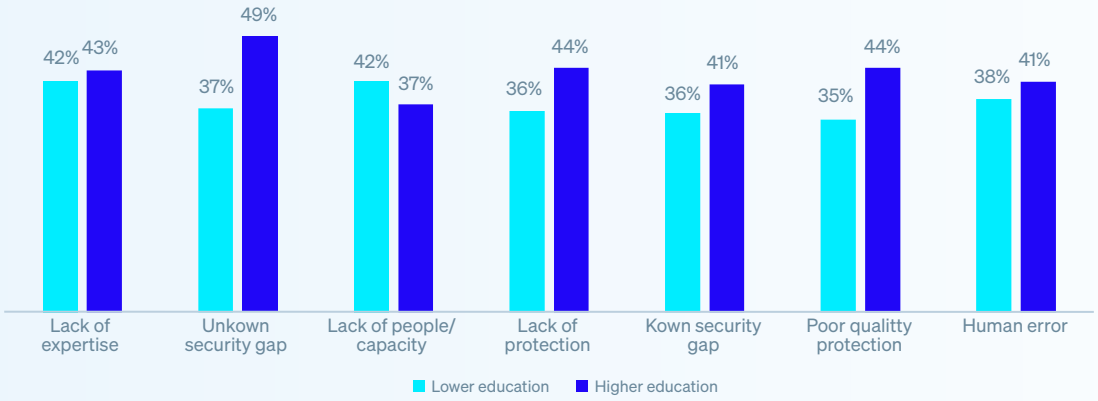
Why do you think your organization fell victim to the ransomware attack? n=441 Consolidated responses.

However, the lower/higher education split reveals variations for lower education providers in particular who were slightly more likely to cite resource constraints as the primary organizational root cause of the attack ahead of security gaps.

Diving deeper into **individual** organizational root causes, both a **lack of expertise** to detect and stop the attack in time and a **lack of people/capacity** to monitor systems at the time of the attack were the joint most common reasons lower education providers fell victim – perceived by 42% of victims in both instances. This is followed by **human errors** (i.e., the teams made a mistake/failed to follow processes properly) which contributed to 38% of attacks.

For higher education providers, **unknown security gaps** (i.e., weaknesses in defenses the organization was unaware of) are the most common individual reason given, named by close to half (49%) of respondents — the highest percentage attributed to this cause of all industries surveyed. This is followed by both **poor-quality protection** (i.e., their cybersecurity products and services were not able to stop the attack) and a **lack of protection** (i.e., they did not have the necessary cybersecurity products and services in place) which contributed to 44% of attacks in both instances.

Chart 4: Organizational root cause of ransomware attacks on education providers

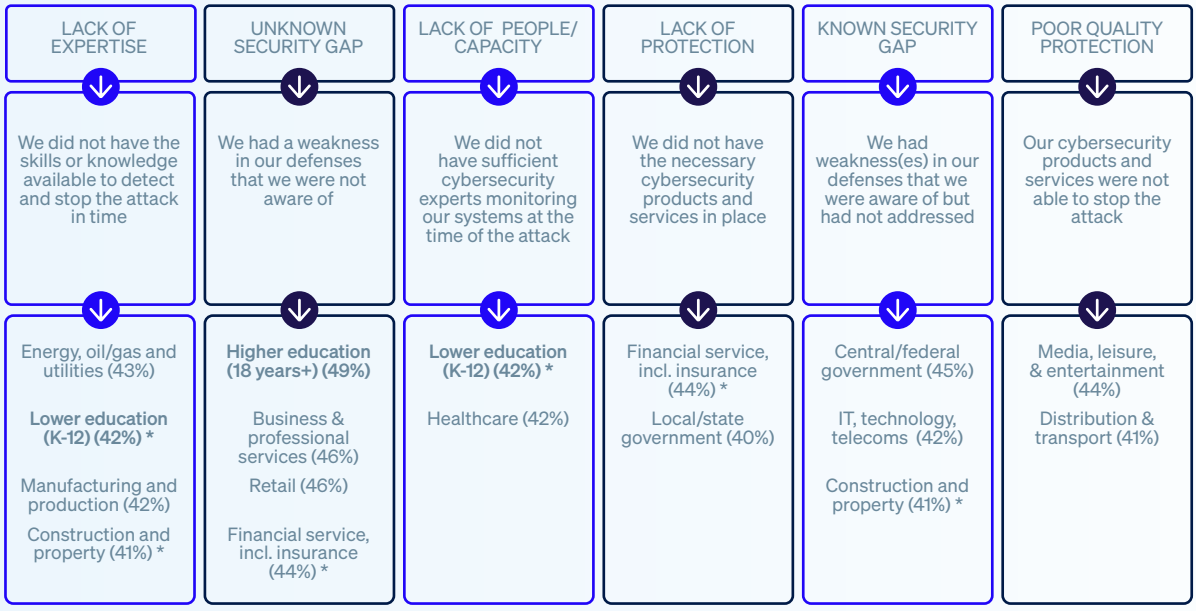


Why do you think your organization fell victim to the ransomware attack? n=243 (Lower education), 198 (Higher education)

Organizational root cause by sector

The most common organizational root cause also varies by sector, reflecting the differing challenges businesses face. It's worth noting that no sector reported human error as the most common reason they fell victim to the ransomware attack.

Chart 5: Top organizational root cause of ransomware attacks by sector



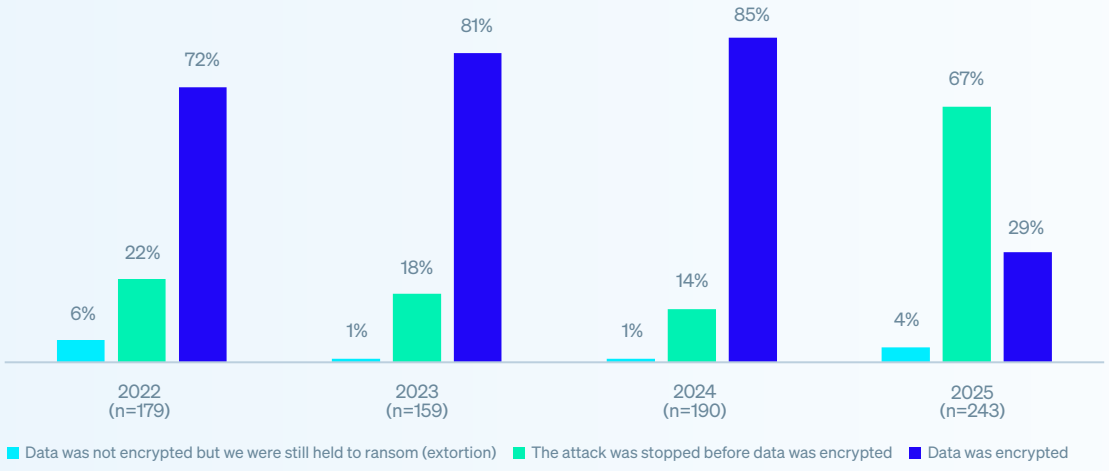
Why do you think your organization fell victim to the ransomware attack? n=3,400. Split by industry.
* denotes two joint top root causes

What happens to the data

Data encryption in education

Encouragingly, **data encryption rates in the education sector have fallen**. In lower education, just 29% of attacks led to data encryption, a four-year low and the lowest rate recorded across all industries surveyed. In line with the lower encryption rate, the rate of attacks successfully stopped before encryption soared from 14% in 2024 to 67% in 2025 — again, the highest of any industry and well above the 44% cross-sector average. This indicates that lower education providers are now more effective than ever at detecting and blocking ransomware attacks before they can do damage.

Chart 6: Data encryption rate in ransomware attacks on lower education providers 2022 - 2025

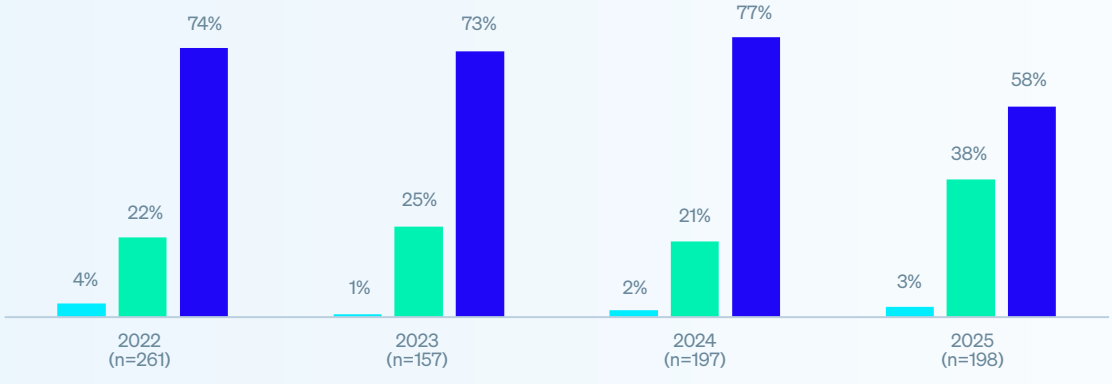


Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

Higher education providers continued their downward data encryption trend, with rates dropping to a four-year low of 58%, down from 77% in 2024. While encouraging, it is still above the cross-sector average of 50%.

On a more positive note, the **proportion of attacks stopped before encryption nearly doubled**, rising from 21% to 38% (though below the 44% cross-sector average). This points to improving defensive capabilities but also highlights that higher education establishments remain exposed, likely due to complex IT environments, legacy infrastructure, and broad, decentralized user bases.

Chart 7: Data encryption rate in ransomware attacks on higher education providers 2022 - 2025



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

Data theft

Adversaries don't just encrypt data — they also steal it. Higher education providers faced a greater risk, with 19% of all victims, and 33% of those with encrypted data, reporting data theft, compared to just 7% and 26% in lower education. This is likely due to the more valuable data, decentralized systems, and broader external access typical of higher education, which make detection and control more challenging. The trend also aligns with prevention outcomes: lower education providers stopped 67% of attacks before encryption, considerably more than higher education at 38%.

Extortion-style attacks

As shown in charts 6 and 7, the percentage of education providers that did not have data encrypted but were held to ransom anyway (extortion) have marginally risen over the year (from 1% in 2024 to 4% for lower education and from 2% in 2024 to 3% for higher education), suggesting a shift in attacker tactics as defenses improve.

Overall, lower education providers are most able to successfully prevent the repercussions of a ransomware attack (i.e., to stop data being encrypted, to prevent data exfiltration, and to avoid being subjected 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 education

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

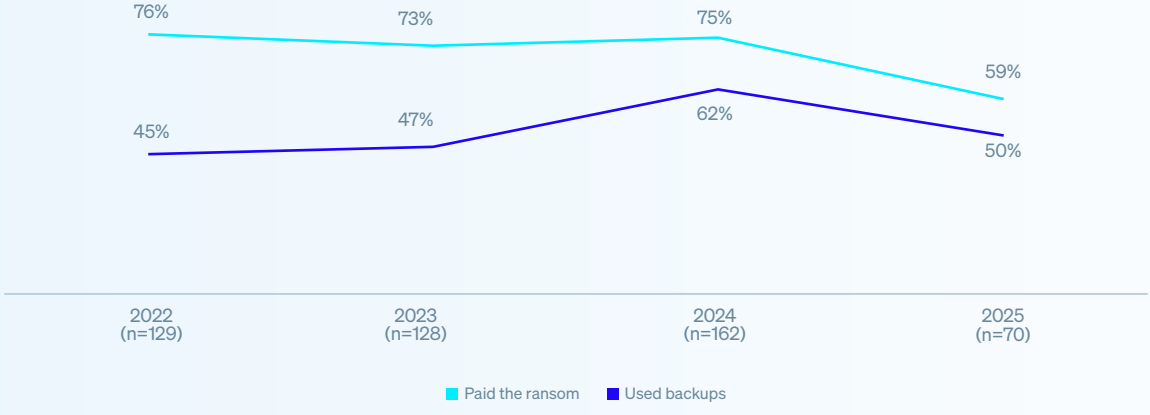
Use of backups by lower education providers to restore data reached a four-year low of 59% – a considerable drop from the 75% recorded in 2024. Despite this, lower education remains among the top four sectors using backups to restore data in this year's survey.

Half of lower education providers **paid the ransom and got their data back**, in line with the 49% cross-sector average. While this is a notable reduction from last year's 62%, it remains the second highest rate of ransom payments made by lower education establishments in the last four years.

The narrowing gap between lower education providers 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 over a third (34%) of lower education providers that had data encrypted said they **used more than one method to restore their data.**

Chart 8: Recovery of encrypted data in lower education 2022 - 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.

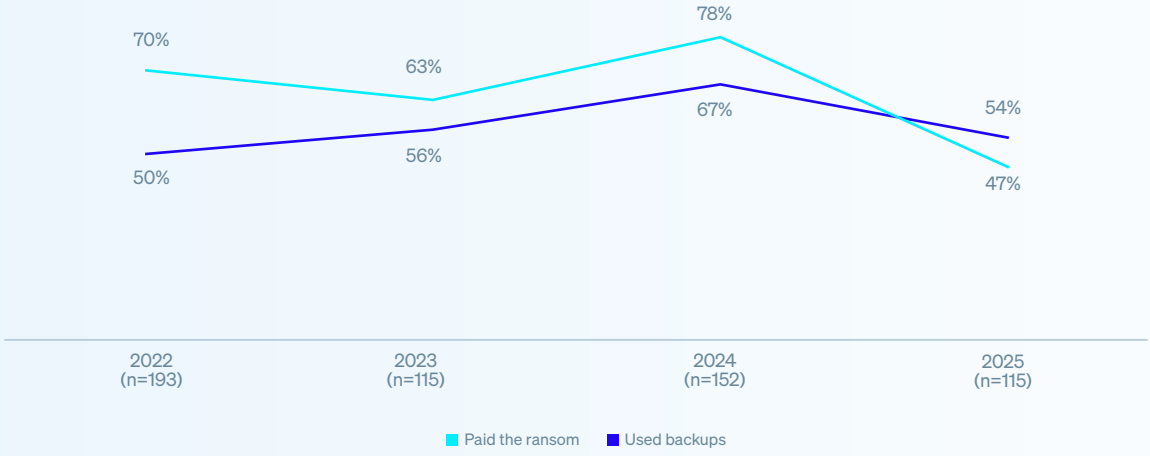
Among higher education providers, only 47% used **backups to restore data**, a sharp drop from 78% in 2024, placing the sector among the bottom three for backup use. This may be due to the decentralized IT infrastructure, complex data environments, legacy systems, and inconsistent backup practices often seen across higher education institutions.

54% of higher education providers **paid the ransom and got their data** back — slightly above the 49% cross-sector average, but a welcome decrease from the 78% recorded in 2024.

Just as observed among lower education establishments, the narrowing gap between higher education providers 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 38% of higher education providers that had data encrypted said they **used more than one method to restore their data**, placing the sector within the top three most likely to do so.

Chart 9: Recovery of encrypted data in higher education 2022 - 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 for education providers

The average (median) ransom demanded of education providers dropped sharply over the last year. The ransom demand for lower education plummeted 74% from $3.85M in 2024 to $1.02M, while the demand for higher education fell from $3.55M in 2024 to just $697K, one of the lowest demands recorded across all sectors surveyed.

	2024	2025
Lower education	$3.85M (n=154)	$1.02M (n=69)
Higher education	$3.55M (n=130)	$697K (n=112)

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

The cross-sector average followed a similar trend, dropping by a third (34%) to $1.32 million in 2025 from $2 million in 2024.

The decrease in ransom demands targeting education providers is largely driven by a considerable reduction in high value demands. Lower education providers saw an 86% decrease in demands of $5M or more while higher education providers saw a 34% decrease in demands of $1M or more. This suggests that attackers may be shifting to chase smaller, quicker payouts rather than targeting large sums.

Ransom payments by education providers

Much like the ransoms demanded, **the average (median) ransom payments** made by both higher and lower education providers **dropped considerably over the last year,** from among the highest in 2024 to among the lowest in 2025, indicating they may be pushing back more effectively against inflated demands.

The median ransom paid by lower education plummeted 88% from $6.60M in 2024 to $800K, while payments made by higher education providers fell from $4.41M in 2024 to just $463K — among four of the lowest payments recorded in this year's survey.

	2024	2025
Lower education	$6.60M (n=99)	$800K (n=35)
Higher education	$4.41M (n=92)	$463K (n=65)

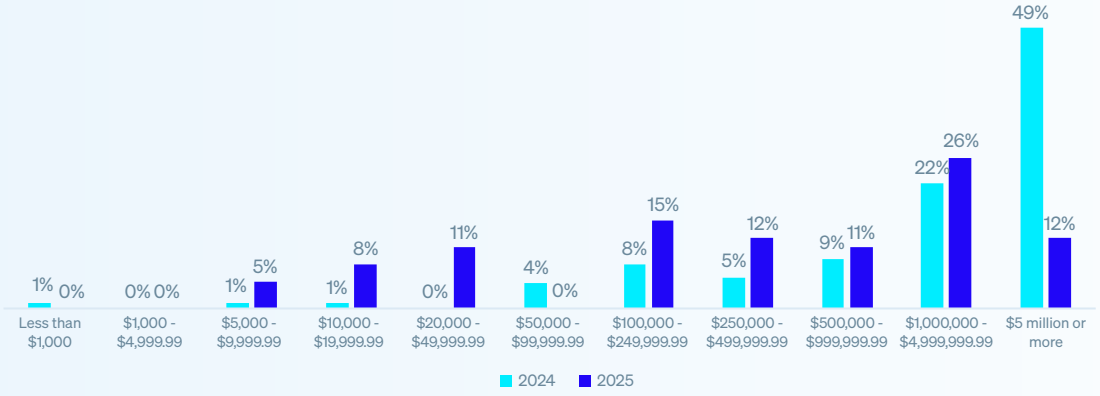
How much was the ransom payment that was paid to the attacker(s)? Base numbers in chart.

The decrease in ransom payments made by education providers is largely driven by a considerable reduction in high value payments of $5M or more, with lower education providers recording an 89% decrease and higher education providers recording a 75% decrease in payments of this size.

Chart 10: Ransom payments in lower education | Distribution banding

How much was the ransom payment that was paid to the attackers? n=35 (2025), 99 (2024)

Chart 11: Ransom payments in higher education | Distribution banding

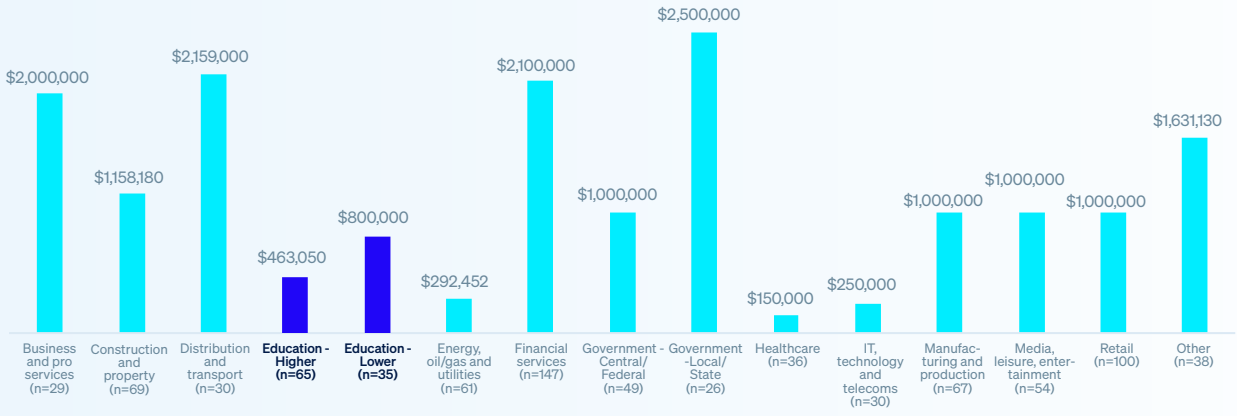


How much was the ransom payment that was paid to the attackers? n=65 (2025), 92 (2024)

Ransom payments by industry

Ransom payments varied considerably by industry, with state and local government organizations paying the highest average amount to attackers at $2.5 million. This may be due to critical service pressures, limited cyber resilience, and attackers exploiting their urgency to recover quickly. In contrast, healthcare providers paid the lowest at just $150,000.

Chart 13: Ransom payments by industry

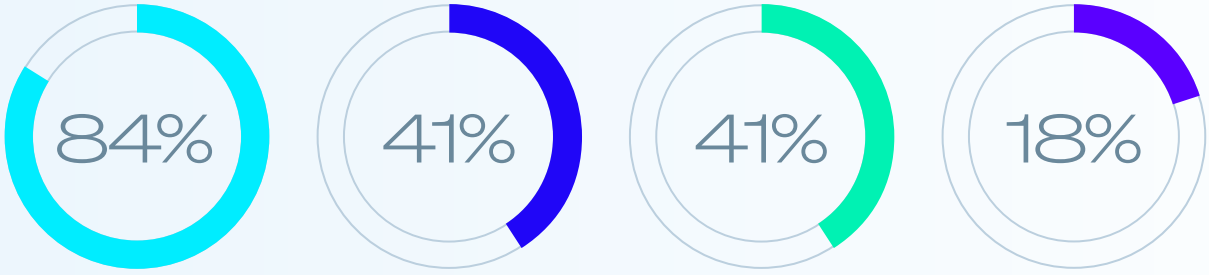


How much was the ransom payment that was paid to the attackers? Base numbers in chart.
Note: Business and pro services and Government – Local/State have low base numbers, so findings should be considered indicative only.

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

34 lower education providers that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, 84% of the initial ransom demand – a welcome drop from the 115% recorded in 2024. Overall, 41% paid less than the initial request (notably below the cross-sector average of 53%), 18% paid more, and 41% matched the initial demand.

34 lower education providers that paid the ransom shared both the initial demand and their actual payment, revealing that:



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

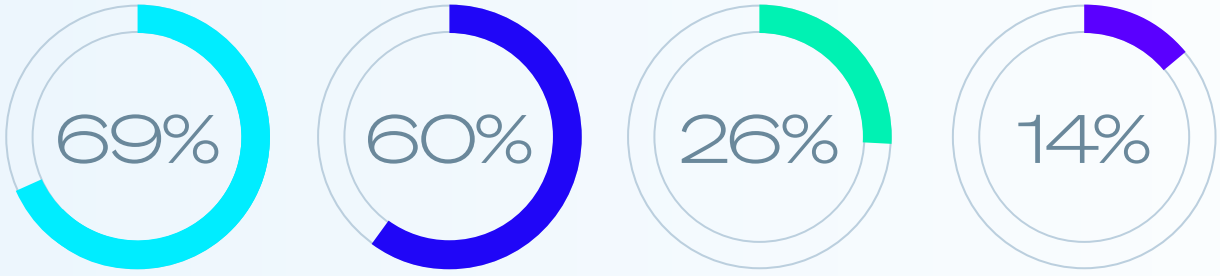
of payments were for **less** than the initial ransom demand

of payments **matched** the initial ransom demand

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

65 higher education providers that paid the ransom shared both the initial demand and their actual payment, revealing that they paid, on average, just 69% of the initial ransom demand — a considerable drop from the 122% recorded in 2024 and the lowest rate recorded in this year's survey. Overall, 60% paid less than the initial ask (notably above the cross-sector average of 53%), 14% paid more, and 26% matched the initial demand.

65 higher education providers that paid the ransom shared both the initial demand and their actual payment, revealing that:



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

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

of payments **matched** the initial ransom demand

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

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

This year, for the first time, we have explored why some education providers pay less than the initial demand, shining new light on a critical area when dealing with a ransomware attack.

15 **lower education** organizations* that **paid less** than the initial demand revealed that:

- 67%: The attackers reduced their demand to encourage us to pay (the highest percentage against this factor in this year's survey).
- 60%: We paid the ransom quickly, so we got a discount.
- 53%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement).
- 53%: A third party negotiated a lower amount with the attackers.
- 33%: We negotiated a lower amount with the attackers.

**Please note: Due to a very low base number, findings are indicative only.*

39 **higher education** providers that **paid less** than the initial demand explained how they were able to lower their payment:

- 59%: We negotiated a lower amount with the attackers (the highest percentage recorded against this factor in this year's survey).
- 46%: We paid the ransom quickly, so we got a discount.
- 44%: The attackers reduced their demand to encourage us to pay.
- 41%: A third party negotiated a lower amount with the attackers.
- 38%: The attackers reduced their demand due to external pressures (e.g., from the media or law enforcement).

Between lower and higher education providers, the reasons they paid less than the initial ask vary significantly. Lower education providers mainly attributed paying less than the initial ask to **attackers reducing their demands to encourage payment**, whereas higher education providers cited **successful negotiations** as the key factor behind paying less. This may have been a factor behind why higher education providers reported among the lowest ransom payments in this year's survey.

Finally, both lower and higher education reported multiple factors (three and two, respectively) behind their lower ransom payment, further emphasizing the complex, multi-faceted situation that ransomware victims face.

Business consequences of ransomware

Recovery costs in education

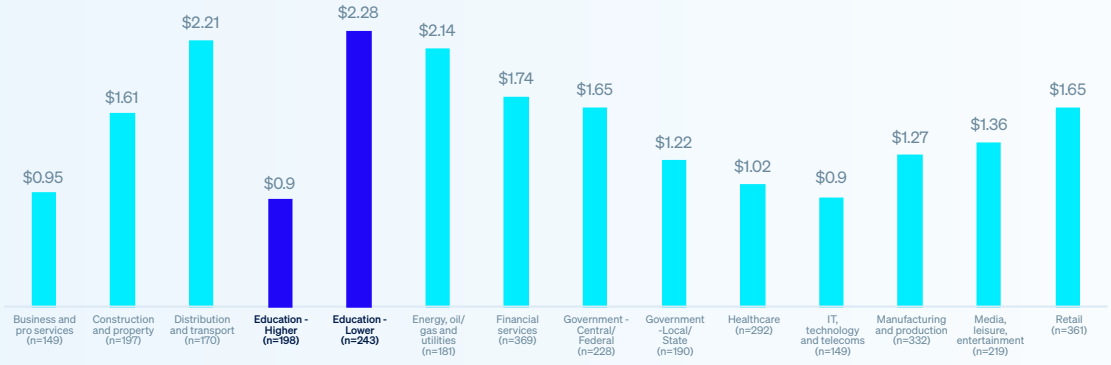
In 2025, average (mean) recovery costs (excluding any ransom payment) for education providers dropped sharply. Higher education saw a 77% fall to $0.90M (the joint lowest recovery cost of all industries surveyed). In stark contrast, despite a 39% reduction of the $3.76M recorded in 2024, lower education providers experienced the highest average recovery cost of all industries surveyed at $2.28M. This is potentially due to the limited IT resources and outdated/fragmented systems typical within the sector.

	2023	2024	2025
Lower education	$1.59M (n=159)	$3.76M (n=197)	$2.28M (n=243)
Higher education	$1.06M (n=157)	$4.02M (n=190)	$0.90M (n=198)

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 chart.

When looking at an industry split, recovery costs vary considerably. Behind lower education, distribution and transport organizations reported the highest average cost to rectify incidents at $2.21 million. Meanwhile, the IT, technology and telecoms sector reported the joint lowest cost at $0.90 million alongside higher education.

Chart 12: Ransomware recovery cost split by industry (USD, millions)



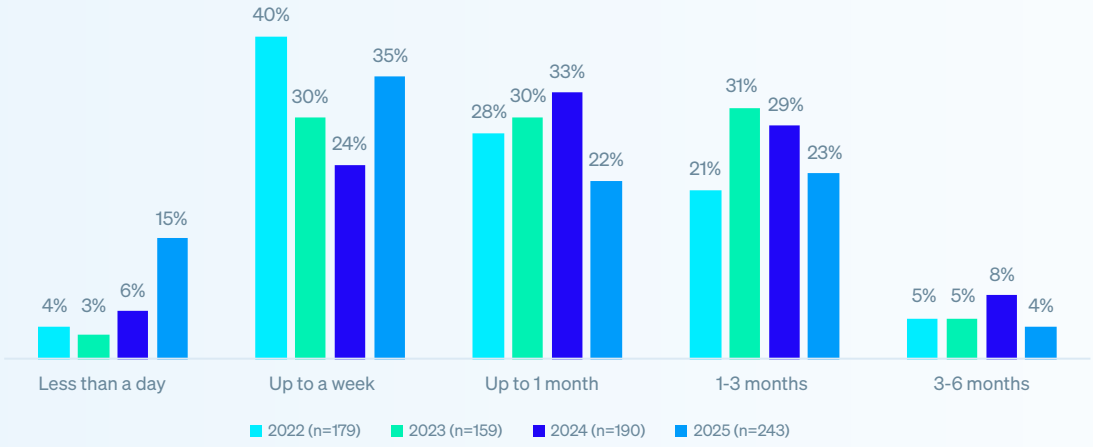
What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made? Base numbers in the chart.

Recovery time in education

The data reveals that, in 2025, **education providers are recovering faster from ransomware attacks.** Half of lower education providers and 59% of higher education providers fully recovered within a week (both up considerably from the 30% recorded in 2024). Meanwhile, the proportion taking one to three months to recover dropped to 23% for lower education and 14% for higher education, down from 29% and 34%, respectively.

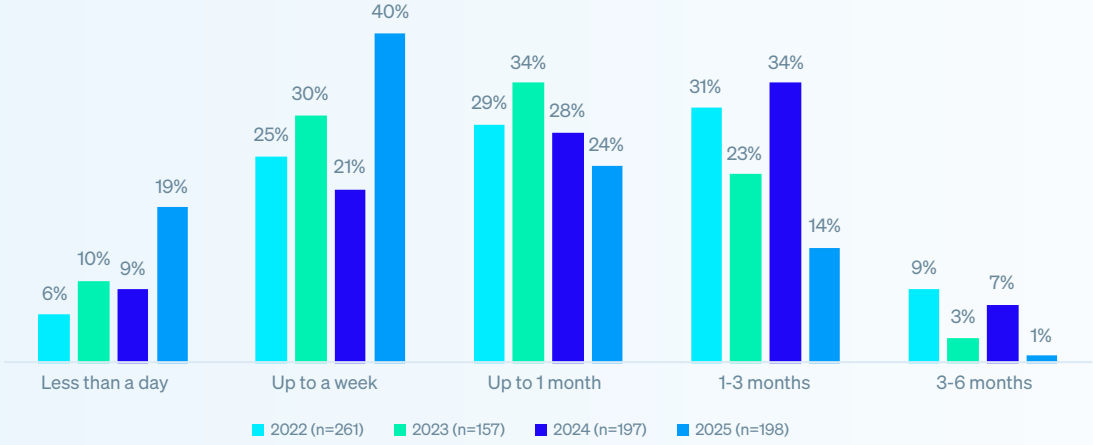
Overall, 95% of victims within the education sector fully recovered within three months, underscoring growing resilience and recovery capabilities across the sector.

Chart 13: Recovery time for lower education providers from ransomware attacks 2022 - 2025



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

Chart 14: Recovery time for higher education providers from ransomware attacks 2022 - 2025



Unsurprisingly, education providers that had data encrypted typically were slower to recover than those that were able to stop the encryption: 13% that had data encrypted were fully recovered in a day, compared to 19% of those where the adversaries did not encrypt the data.

Human consequences of ransomware

The survey makes clear that having data encrypted in a ransomware attack has significant repercussions for IT/cybersecurity teams in the education sector, with all respondents saying their team has been impacted in some way.

Chart 15: The consequences on IT/cybersecurity teams of having data encrypted

Lower education		Higher education	
41%	Increased **pressure** from senior leaders	53%	Increased **pressure** from senior leaders
40%	Ongoing increase in **workload**	50%	Changes to **team / organizational** structure
37%	Increased **anxiety or stress** about future attacks	40%	Increased **anxiety or stress** about future attacks
37%	Feelings of **guilt** that the attack was not stopped	37%	Ongoing increase in **workload**
36%	Increased **recognition** from senior leaders	36%	Feelings of **guilt** that the attack was not stopped
34%	Change of **team priorities / focus**	34%	Increased **recognition** from senior leaders
29%	Changes to **team / organizational** structure	33%	Our team's **leadership** was replaced
26%	Staff absence due to **stress / mental health** issues	31%	Changes to **team / organizational** structure
26%	Our team's **leadership** was replaced	31%	Staff absence due to **stress / mental health** issues

What repercussions has the ransomware attack had on the people in your IT/ cybersecurity team, if any? n=70 (Lower education), 115 (Higher education)

Recommendations

Although education providers have experienced several changes in their encounters with ransomware over the last year, it remains a significant threat. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace with ransomware and other threats. Leverage the insights in this report to fortify your defenses, sharpen your threat response, and limit ransomware's impact on your business and people. Focus on these four key areas to stay ahead of attacks:

- **Prevention**. The most successful defense against ransomware is one where the attack never happens because adversaries couldn't breach your organization. Take steps to eliminate the technical and organizational root causes highlighted in this report.
- **Protection**. Strong foundational security is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption.
- **Detection and response.** The sooner you stop an attack, the better your outcomes. Around-the-clock threat detection and response is now an essential layer of defense. If you lack the resources or skills to deliver this in-house, look to work with a trusted managed detection and response (MDR) provider.
- **Planning and preparation.** Having an incident response plan that you are well-versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Be sure to make quality backups and regularly practice restoring data from them to accelerate recovery if you do get hit.

To explore how Sophos can help you optimize your ransomware defenses, speak to an advisor, or visit www.sophos.com.

Learn more about ransomware and how Sophos can help you defend your organization.

Sophos delivers industry leading cybersecurity solutions to businesses of all sizes, protecting them in real time from advanced threats such as malware, ransomware, and phishing. With proven next-gen capabilities your business data is secured effectively by products that are powered by artificial intelligence and machine learning.

2025-10-06 WP (NP) CRE-2426

SOPHOS