REPORT

The State of Ransomware in Education 2026

Findings from an independent survey of 226 IT and cybersecurity leaders in the education sector across 17 countries whose organizations were hit by ransomware in the last year.

SOPHOS

Introduction

Welcome to the sixth edition of the annual Sophos State of Ransomware in Education report, which reveals the reality of ransomware for both lower education (including K-12, primary, and secondary schools — typically for students under 18 years old) and higher education (universities, colleges, and equivalent establishments — typically for students over 18 years old) providers in 2026.

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

Drawing on the real-world experiences of 226 education IT and cybersecurity leaders, 131 from lower education and 95 from higher education institutions hit by ransomware in the past year, this report offers unique insights into:

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

Note: Throughout this report, "overall survey" refers to results from respondents across all sectors surveyed. The 226 education sector respondents are part of a broader cohort of 2,158 respondents across 15 industry sectors.

About the survey

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

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

Key findings

- **Identity attacks, especially email-based, were high in education sectors.**
  - 77% of higher education and 71% of lower education victims confirmed their ransomware attack was also their most significant identity attack, both above the 67% overall survey (all-sectors) rate.
  - Malicious email was the leading technical root cause for ransomware attacks in lower education (31%) and higher education (29%).
  - Identity-based approaches (e.g., malicious email, phishing, compromised credentials, or brute force) initiated 85% of attacks across all education, above the 79% all-sectors rate.
- **Operational weaknesses in education were higher than the overall survey (all sectors).**
  - Higher education's defining gap was expertise: 53% said they lacked the skills to detect and stop the attack in time, versus 35% for the overall survey.
  - Lower education's biggest operational root causes were human error (52%), lack of protection (47%), unknown security gaps (42%), and lack of people or capacity (41%).
- **Encryption from ransomware attacks rose sharply in lower education.**
  - Lower education's data-encryption rate more than doubled, rising from 29% in 2025 to 61% in 2026.
  - 58% of education-sector attacks resulted in encrypted data, close to the 56% overall survey rate.
- **Education providers relied heavily on backups to restore data.**
  - 77% of lower education providers restored encrypted data from backups, above the 66% overall survey rate.
  - 69% of higher education providers also recovered using backups.
- **Education paid less than the overall survey but had more $5M+ ransom payments.**
  - Education's median ransom demand ran higher than the overall survey at $775,200 (versus $698,000), but its median ransom payment came in lower at $515,000 (versus $769,000 overall).
  - Education median ransom demands have gone down two years in a row, while payments increased by $15,000 from the 2025 report to 2026.
  - Education providers were more likely to pay $5 million or more (23% versus 16% in the overall survey).
- **Recovery cost more and took longer in education.**
  - Average recovery costs in education reached $2.26 million, above the $1.7 million overall survey figure.
  - Education's recovery costs have gone up since the 2025 report from $1.66 million to $2.26 million, with higher education costs increasing by more than $1 million.
  - 26% of education providers needed one to three months to fully recover from a ransomware attack, roughly double the 14% all-sectors rate.
  - Lower education had the largest share of long-term recoveries: 31% took a month or more to get back on their feet, more than any other sector.
- **The human toll on security teams intensified.**
  - 53% of higher education teams reported increased pressure from senior leaders, versus 40% across all sectors.
  - Around 39% of education teams reported staff absence due to stress or mental-health issues, versus 29% across all sectors.

Attack and defense methods

Root causes of attacks

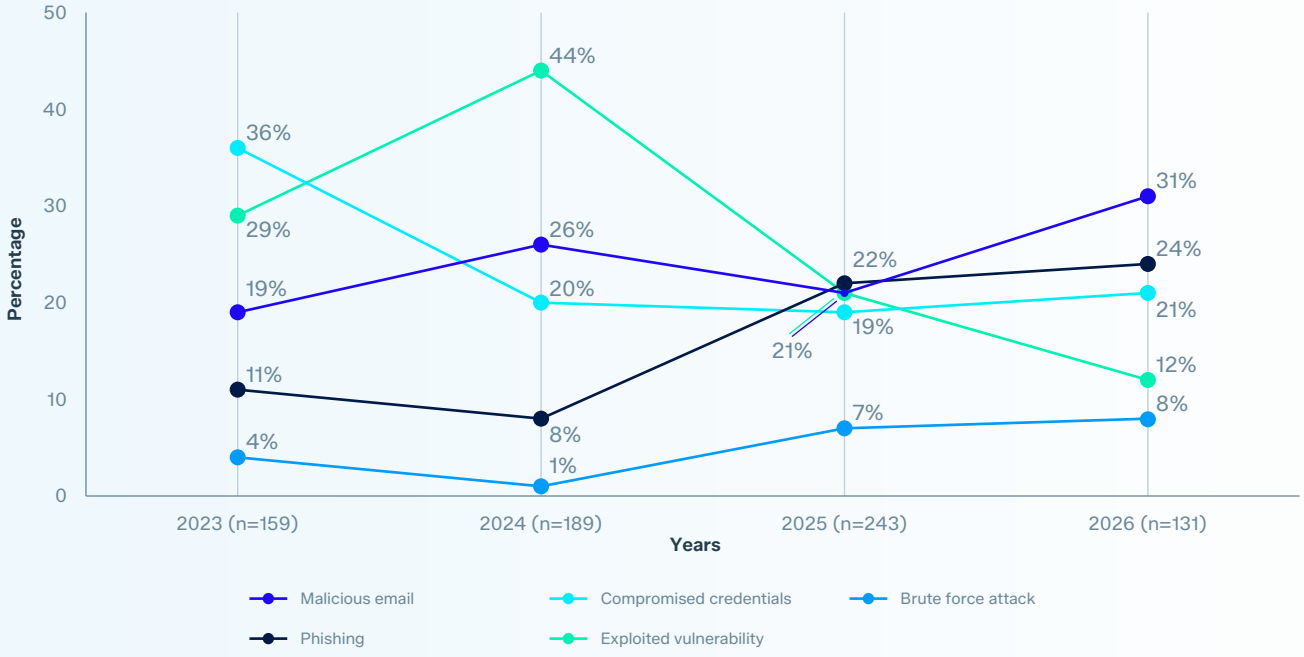
This year's education data reflects the same shift seen across all sectors: identity-based attacks are growing.

Malicious email was the most common technical root cause in lower education (31%), followed by phishing (24%) and compromised credentials (21%). Exploited vulnerabilities dropped to 12%, which reflects the general drop in the overall survey (all sectors) to 18%.

85%

The share of attacks on education providers that started with an identity-based approach (e.g., malicious email, phishing, compromised credentials, or brute force), above the 79% overall survey rate.

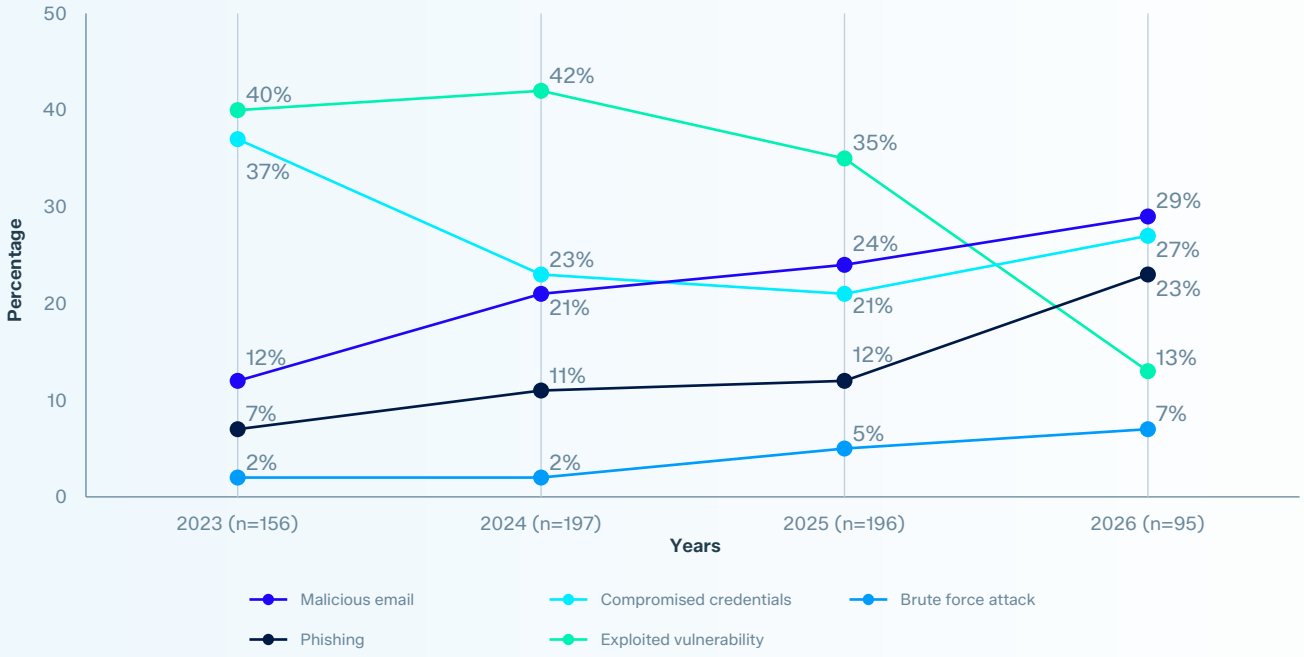
Technical root cause of ransomware attacks 2023–2026: Lower education



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

Higher education providers also reported a drop in exploited vulnerabilities. That vector fell to 13% in the 2026 report, down from 35% in 2025. **Malicious email (29%) and compromised credentials (27%) are nearly joint-leading causes** with phishing close behind at 23%. Both lower and higher education sectors report email-based attacks as leading causes, which is consistent with the overall survey, where malicious email (26%) and phishing (24%) together account for half of all incidents.

Technical root cause of ransomware attacks 2023–2026: Higher education

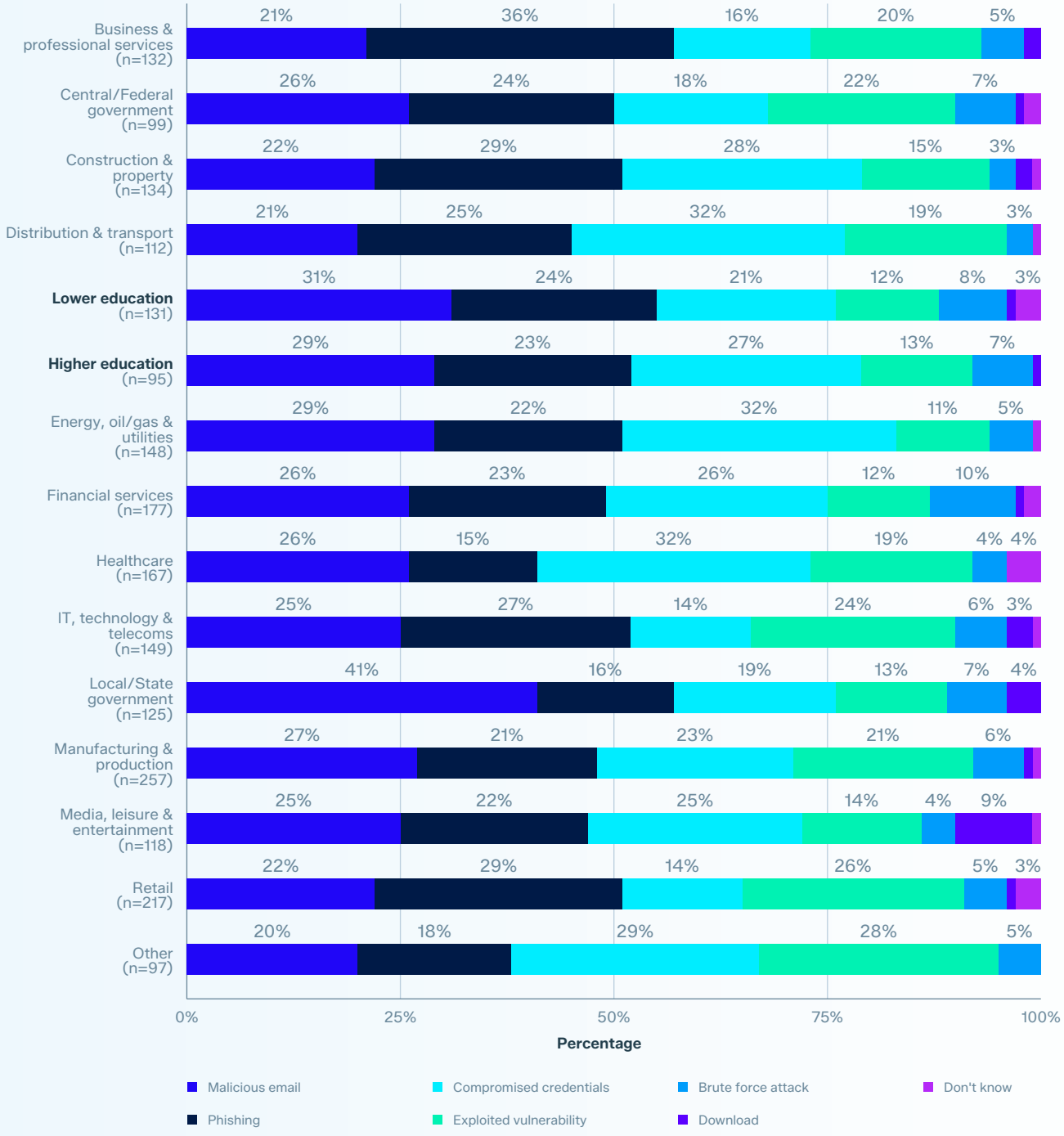


Do you know the root cause of the ransomware attack your organization experienced in the last year?
Downloads and "I don't know" excluded from chart for visual clarity. Percentages may not equal 100%. Base numbers in chart.

Taken together, **identity-based vectors (e.g., malicious email, phishing, compromised credentials, and brute force attacks) accounted for 85% of attacks on education providers, above the 79% overall survey rate**. Higher education was highest at 86%, and lower education followed at 84%. In other words, roughly six in seven attacks against education began with an identity-based approach, reinforcing why identity security is central to the sector's defenses.

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

Technical root cause by industry (2026)



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

What made organizations vulnerable

Education providers cited a broad mix of challenges with protection, resourcing, and security gaps. Across the three consolidated categories, resourcing issues (a lack of people or skills) were cited by 63% of education providers, followed by protection issues (62%) and security gaps (62%).

Why do you think your organization fell victim to the ransomware attack? n=226. Consolidated responses.

Combined education reported a higher rate than the overall survey on nearly every operational root cause, with known security gaps being the only exception. Splitting lower and higher education reveals two different weaknesses.

Higher education's defining weakness was expertise. 53% said they lacked the skills or knowledge to detect and stop the attack in time, compared with 35% for the overall survey, an 18-percentage-point gap and its single largest.

Lower education's weaknesses clustered around capacity and tooling. Human error was cited by 52% of lower education providers (versus 35% across all sectors), lack of protection by 47% of providers, and lack of people or capacity by 41% of providers.

Operational root causes: Lower & higher education vs. all sectors

Operational root cause	Lower education (n=131)	Higher education (n=95)	All sectors (n=2,158)
Lack of protection	47%	36%	36%
Unknown security gap	42%	38%	36%
Known security gap	33%	35%	36%
Lack of people/capacity	41%	37%	35%
Human error	52%	36%	35%
Lack of expertise	33%	53%	35%
Poor quality protection	38%	39%	33%

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

53%

The share of higher education victims who said they lacked the skills or knowledge to detect and stop the attack in time, 18 points above the overall survey and their single biggest weakness.

Viewed against other sectors, education struggled with lack of protection and expertise by comparison. The table below shows sectors placed in the column of the operational root cause they cited most.

Top "operational" root cause of ransomware attacks by sector

LACK OF EXPERTISE	UNKNOWN SECURITY GAP	KNOWN SECURITY GAP	LACK OF PEOPLE/ CAPACITY	LACK OF EXPERTISE	POOR QUALITY PROTECTION	HUMAN ERROR
We did not have the necessary cybersecurity products and services in place	We had a weakness in our defenses that we were not aware of	We had weakness(es) in our defenses that we were aware of but had not addressed	We did not have a sufficient number of cybersecurity experts monitoring our systems at the time of the attack	We did not have the skills or knowledge available to detect and stop the attack in time	Our cybersecurity products and services were not able to stop the attack	Our teams made a mistake/ failed to follow processes properly
Business & professional services (44%) Other (42%) Energy, oil/gas & utilities* (37%)	IT, technology & telecoms (42%) Construction & property (41%)	Financial services (44%) Energy, oil/gas & utilities* (37%) Manufacturing & production* (37%) Retail (38%)	Media, leisure & entertainment (43%) Local/State government (42%)	**Higher education (53%)** Healthcare (47%) Central/Federal government (43%)	Distribution & transport (38%)	**Lower education (52%)** Manufacturing & production* (39%)

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

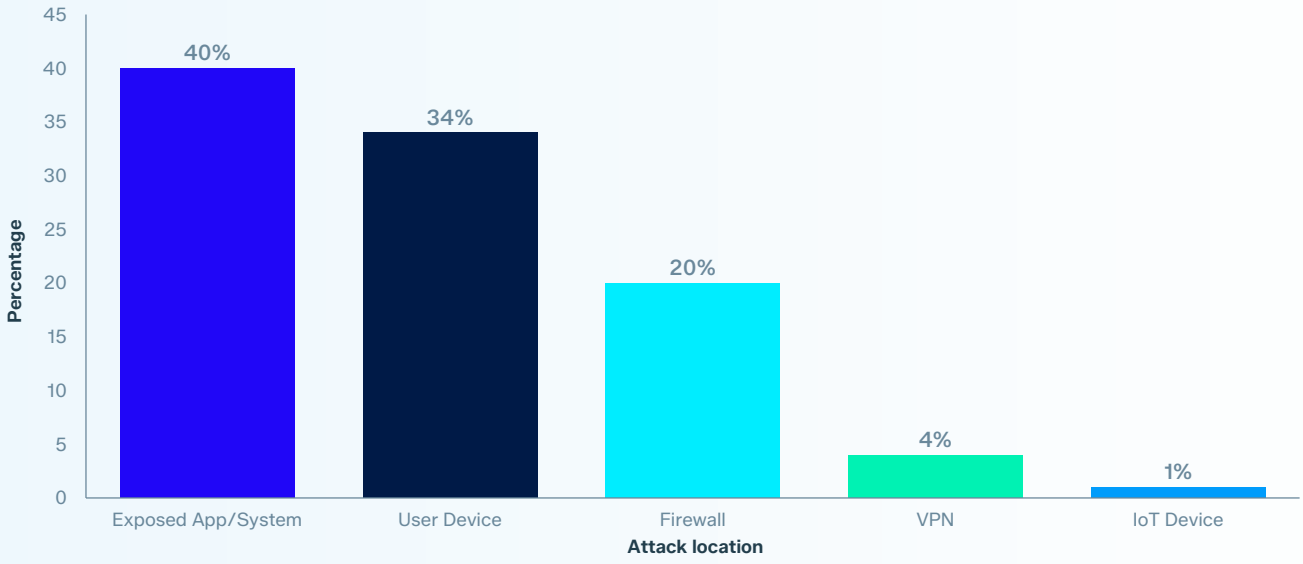
NEW RESEARCH

Where attacks start

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

For education, exposed applications and systems were the most common entry point (40%), followed by user devices (34%) and firewalls (20%). These figures track the overall survey closely (38%, 30%, and 21% respectively), so education shows no meaningful divergence here.

Where ransomware attacks start: Combined education



You said the root cause was an exploited vulnerability, compromised credentials, or a brute force attack. Where did this happen in your environment? Combined higher and lower education. n=99

NEW RESEARCH

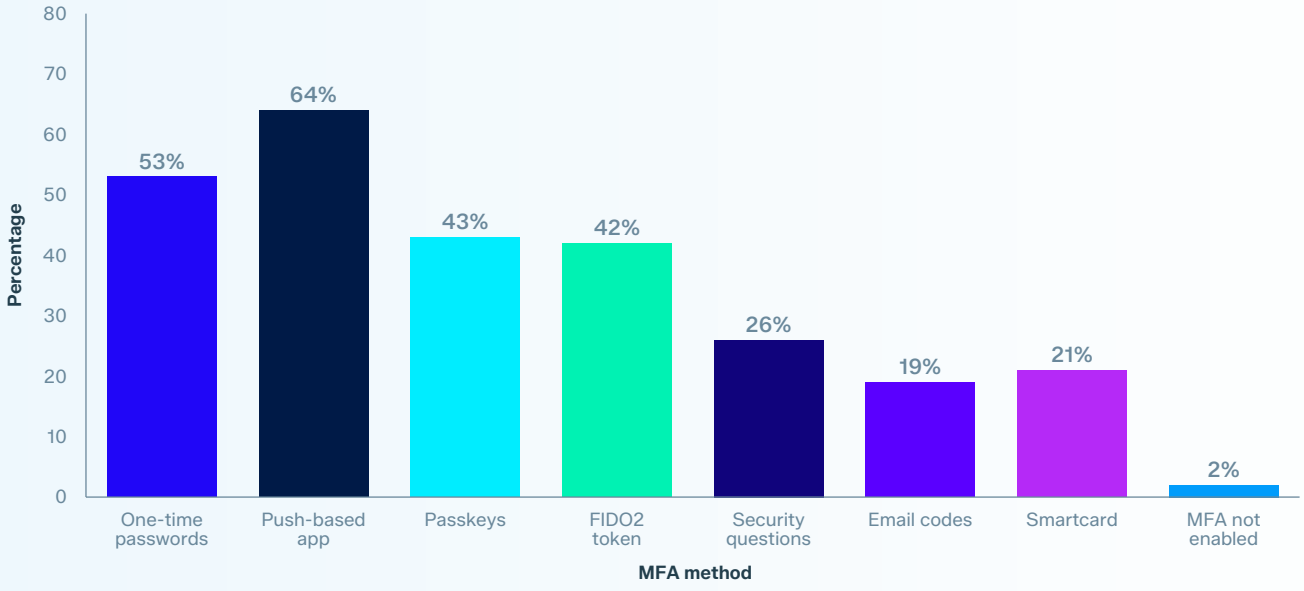
The role of multi-factor authentication (MFA)

We also examined the MFA methods in place at the time of the attack among education providers whose attack began with compromised credentials. Almost all victims in education had some form of MFA enabled (98%), echoing the overall survey finding (97%) that MFA was present in most credential-based attacks.

However, out of the education providers who were asked about MFA, 81% still had data encrypted despite MFA enablement. This suggests that either MFA was not comprehensively deployed across all critical systems, attackers found ways to bypass MFA protections, or the attack vectors didn't rely solely on credential compromise.

Push-based applications (64%) and one-time passwords (53%) were the most commonly deployed methods for education.

MFA methods enabled at the time of attack: Combined education



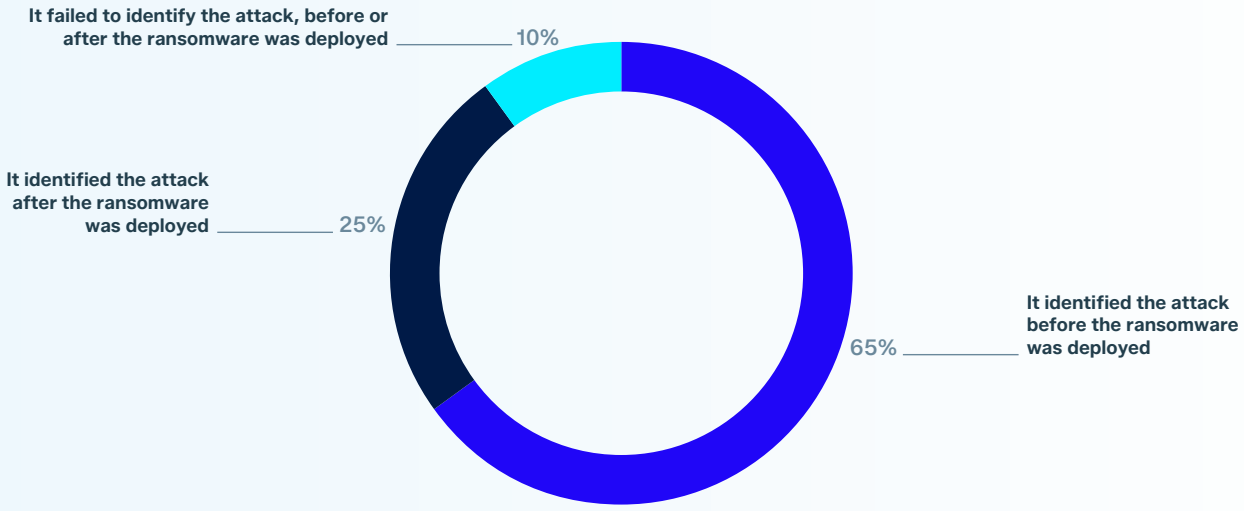
What type of multi-factor authentication was enabled at the time of the attack, if any? Multiple responses permitted. Base: The attack occurred due to compromised credentials. Combined higher and lower education. n=53.

NEW RESEARCH

The role of firewalls

For education, firewalls identified most attacks, but they didn't always help stop them. 65% of providers said their firewall identified the attack before the ransomware was deployed, 25% said it identified the attack afterward, and 10% said it did not identify the attack at all. This reflects the overall survey (61%, 32%, and 7%) with a slight shift toward the two ends of the spectrum.

What role did your firewall play in identifying the attack?



What role did your firewall play in identifying the attack? Combined higher and lower education. n=226.

Among those early-detection cases, victims in education still had their data encrypted 51% of the time.

Firewalls are doing a good job of collecting data to identify attacks, but attacks still aren't being stopped at the same rate they're being identified. Firewalls often log the data needed to detect and stop an attack, but they may not be connecting deeply enough with other systems to recognize the threat and respond in time.

NEW RESEARCH

The identity-ransomware connection

One of the survey's clearest findings is the direct link between identity attacks and ransomware. Across all sectors, two-thirds of ransomware victims (67%) confirmed the incident was the same event as their most significant identity attack. However, education sits above that mark: 71% in lower education and 77% in higher education (73% combined education).

Although not all the attacks resulted in data encryption, the finding shows a strong overlap between identity attacks and ransomware in education.

Ransomware attack was also their most significant identity-related attack

Did your organization experience a ransomware attack that was also an identity attack? Organizations hit by ransomware. Bases in charts.

73%

The share of education victims whose ransomware incident was the same event as their most significant identity attack, above the 67% overall survey rate.

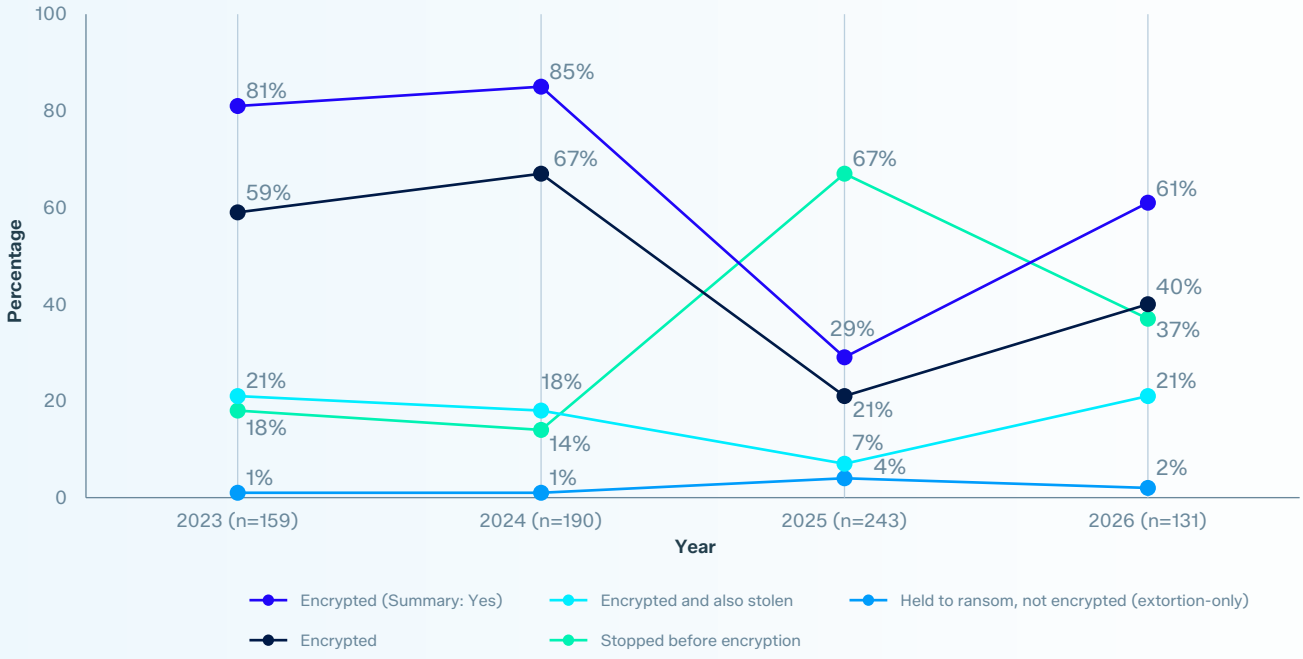
Data encryption and recovery

Data encryption rate

The findings from the 2025 State of Ransomware in Education Report showed very positive outcomes for lower education. Unfortunately, this year's report shows lower education regressing back closer to its prior trend.

After lower education's encryption rate fell to 29% in the 2025 report, the lowest of any sector that year, **the share of attacks against lower education that succeeded in encrypting data more than doubled to 61% in 2026** (above the 56% overall survey rate). Only 37% of attacks were stopped before encryption by lower education this year, down from 67% in last year's report.

Data encryption rate over time: Lower education

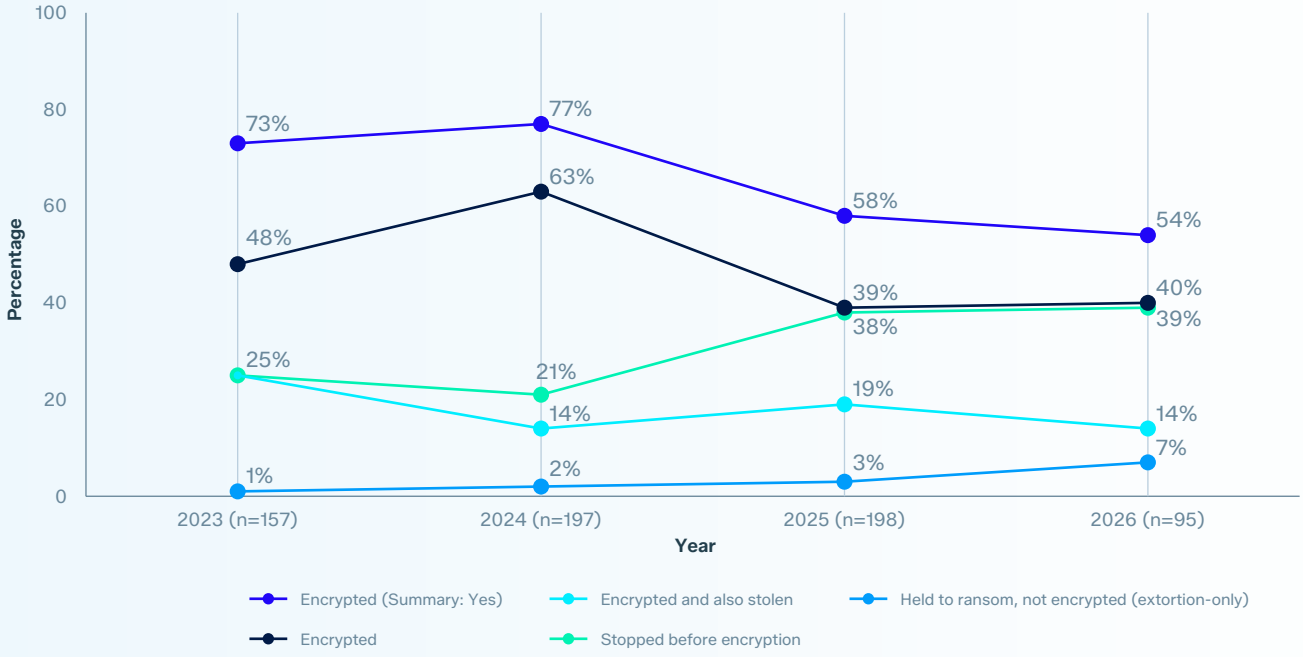


Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.
The "Encrypted (Summary: Yes)" line in this chart is the sum of "Encrypted" and "Encrypted and also stolen" answers.

Double extortion (where data is both encrypted and also stolen) resurged in lower education, climbing from 7% in 2025 to 21% in 2026, which is in line with its pre-2025 levels. These attacks give attackers a second point of leverage. Extortion-only attacks **(held to ransom without encryption)** fell slightly from 4% to 2% for lower education.

Higher education was steadier. Its encryption rate eased slightly to 54% in 2026, from 58% in 2025, keeping it close to the overall survey.

Data encryption rate over time: Higher education



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.
The "Encrypted (Summary: Yes)" line in this chart is the sum of "Encrypted" and "Encrypted and also stolen" answers.

For higher education, extortion-only attacks rose to 7%, up from 3% in 2025, which is worth watching even at a small share.

The 2026 picture also returns education to its longer-term pattern. In 2023 and 2024, the rate of data encryption in lower education was higher than that of higher education; 2025 was the exception, when lower education's rate briefly cratered. This year's 61% encryption rate for lower education versus 54% for higher education restores the long-term trend.

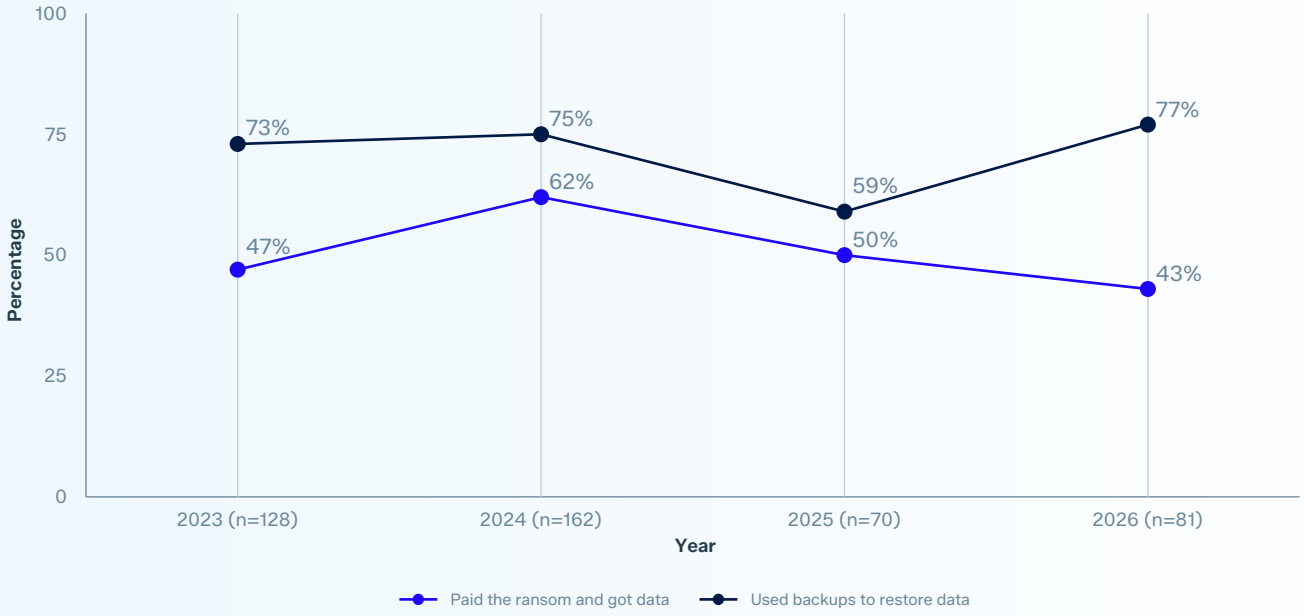
How organizations recovered encrypted data

Backups were education's strongest recovery lever in 2026. After dipping in 2025 (lower education 59%, higher education 47%), backup-based recovery rebounded this year. **77% of lower education and 69% of higher education providers restored data from backups**, both above the 66% overall survey rate. The rebound suggests education has renewed its investment in backup infrastructure and is rebuilding resilience against ransom demands.

77%

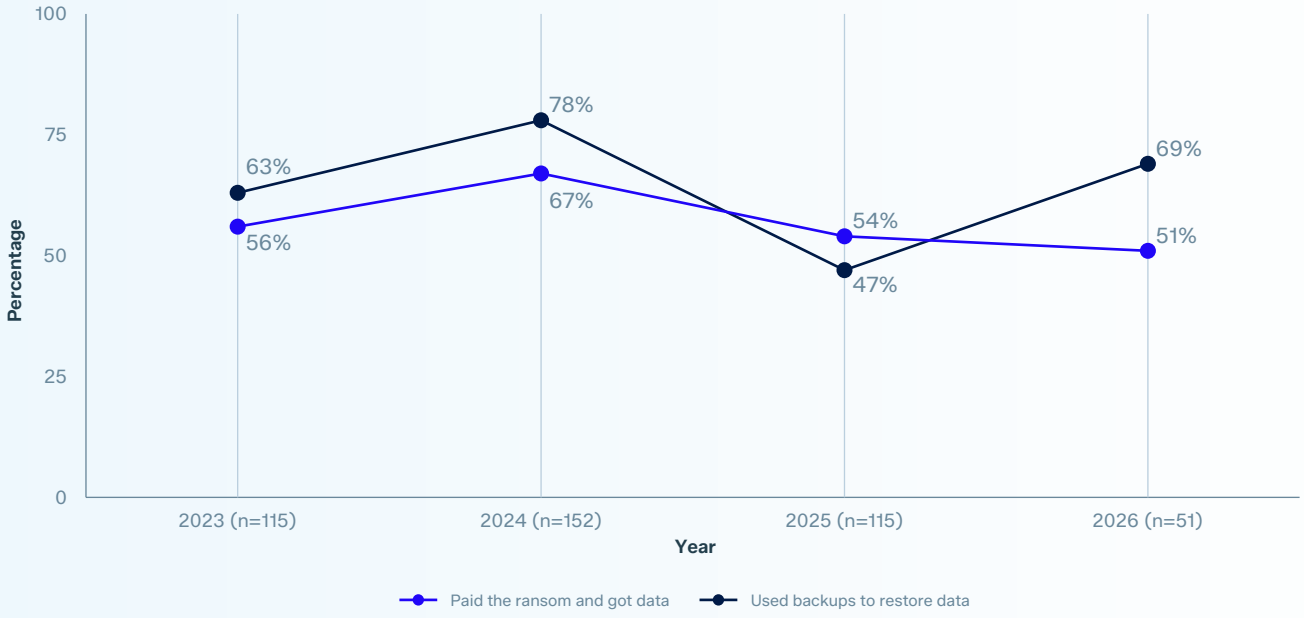
The share of lower education providers that restored encrypted data from backups in 2026, above the 66% overall survey rate.

Data recovery methods over time: Lower education



How did your organization get the data back? Multiple responses permitted. Base numbers in chart.

Data recovery methods over time: Higher education



How did your organization get the data back? Multiple responses permitted. Base numbers in chart.

At the same time, education is paying ransoms less frequently. **The share of providers that paid the ransom and got data back has declined for two straight years**, from 62% (2024) to 50% (2025) to 43% (2026) in lower education, and from 67% to 54% to 51% respectively in higher education.

With backup restoration rising and payment-based recovery falling, education is recovering more on the strength of its own capabilities than on the attackers' cooperation.

Ransom demands and payments

Ransom demands

Education faced steeper ransom demands compared to other sectors in the overall survey. The median ransom demand made to an education institution was $775,200, above the $698,000 median for all sectors. The distribution skewed high as well: **half of ransom demands (50%) were for $1 million or more, and a quarter (25%) were for $5 million or more**, compared with 46% and 23% respectively across the all-sectors sample.

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

Median ransom demand

	2025	2026
Education	$0.98M (n=185)	$0.78M (n=132)
All sectors	$1.32M (n=1,700)	$0.70M (n=1,214)

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

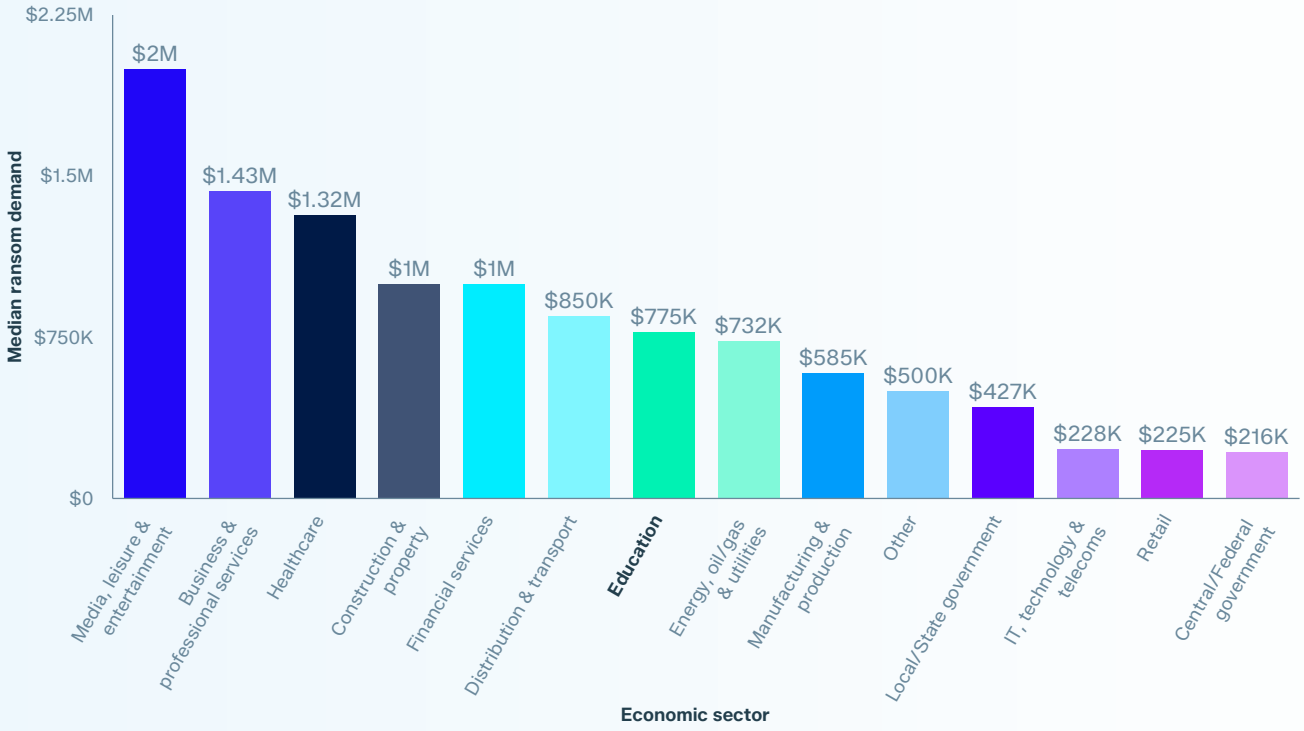
Against other sectors, education sits in the middle of the field. Its median ransom demands run below the highest-demand sectors, such as media, leisure and entertainment ($2 million) and business and professional services ($1.43 million), but well above lower-demand sectors like central government ($216,500) and retail ($225,000).

$775.2K

The median ransom demand made to education providers—higher than the $698,000 overall survey median.

Half of all education ransom demands were for $1 million or more.

Median ransom demands by sector



How much was the ransom demand from the attacker(s)? Base: organizations whose data was encrypted. n=1,141

The year-over-year trends are good and bad. Combined education's median demand fell from $976,000 in 2025 to $775,200 in 2026. This decrease was largely driven by lower education, where the median demand dropped from $1.03 million to $737,600, while higher education ran counter to that trend, with its median demand rising from $697,086 to $889,200.

Ransom payments

Education's higher demands did not translate into higher payments. **Though they saw higher demands, the median ransom payment by education was less compared to other sectors in the overall survey**. The median ransom payment made by an education institution was $515,000, below the $769,000 overall survey median.

Education's payments clustered away from the top band but included a larger share of $5M+ payments. 39% of education payments were $1 million or more, below the 44% overall survey figure. Yet 23% were $5 million or more, above the 16% overall survey rate. When education pays, it usually pays less than other sectors, but a meaningful minority pay very large sums.

Median ransom payment

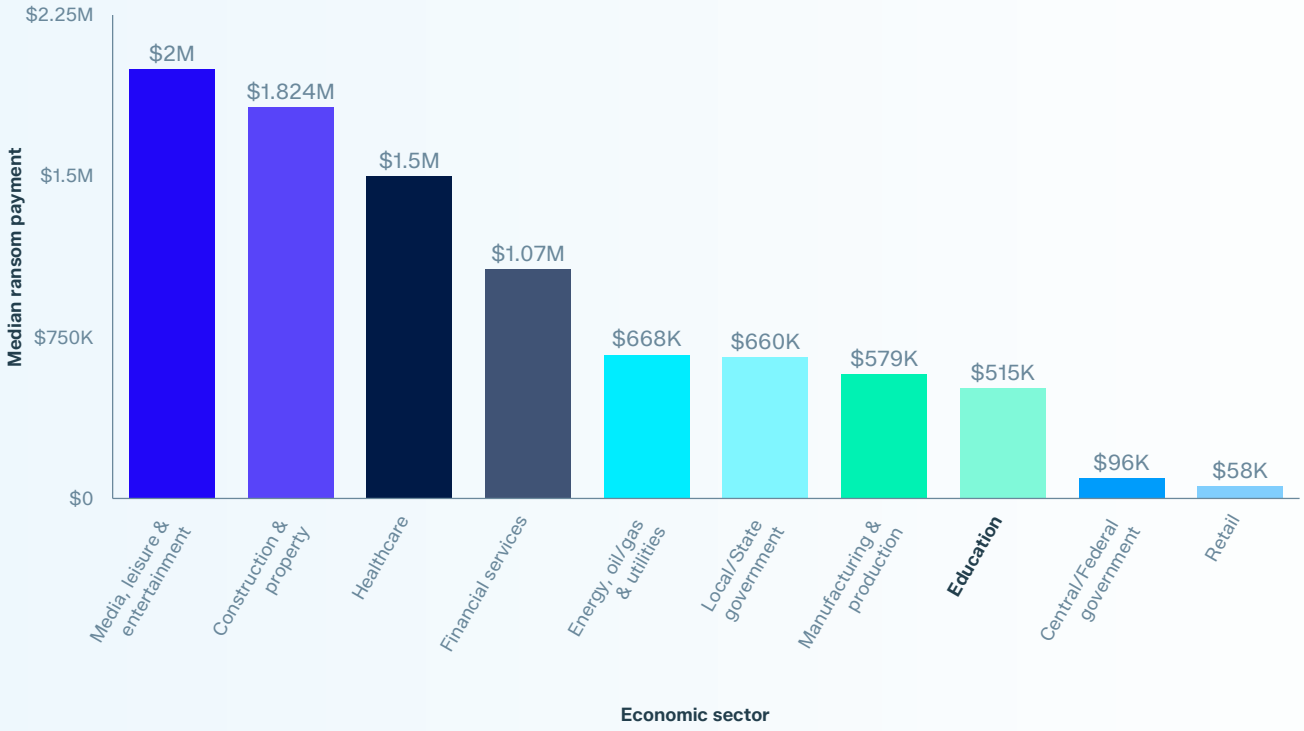
	2025	2026
Education	$0.50M (n=100)	$0.52M (n=62)
All sectors	$1.00M (n=847)	$0.77M (n=587)

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

$515K

The median ransom paid by education providers - lower than the $769,000 overall survey median, despite higher ransom demands.

Median ransom payments by sector



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

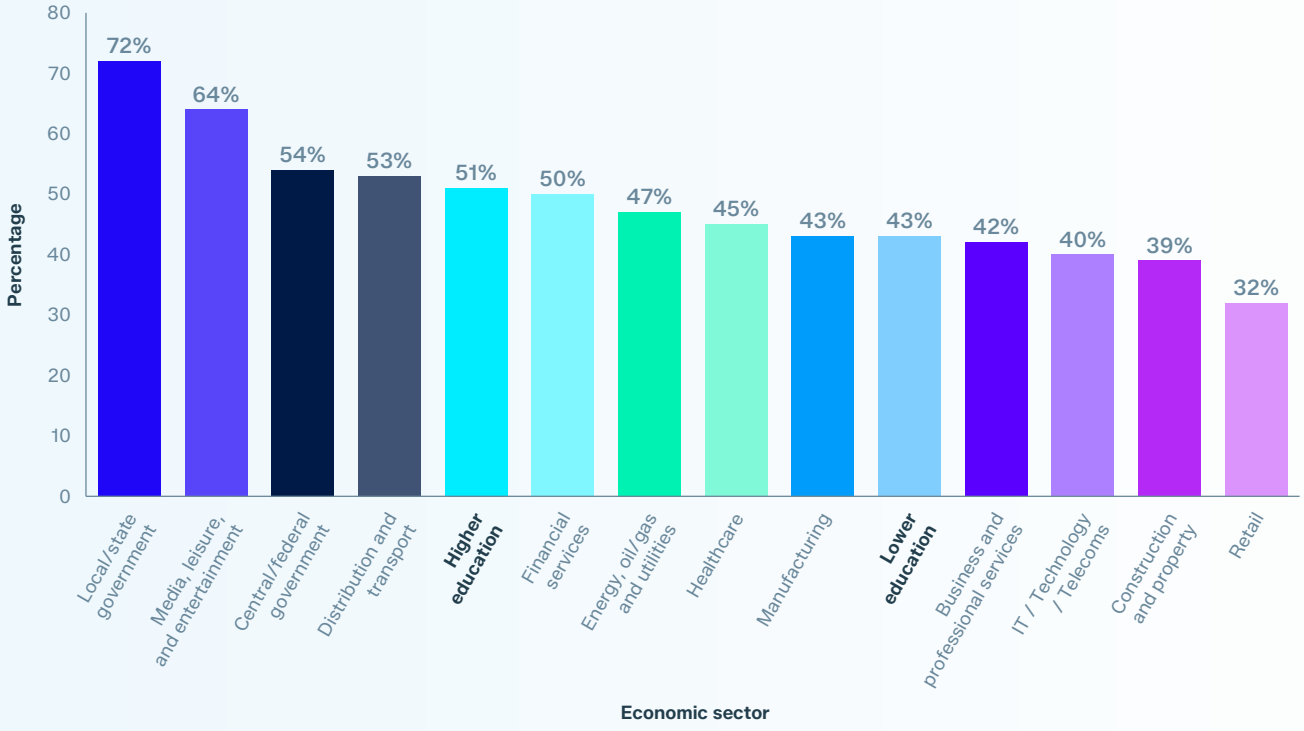
Year-over-year trends were also mixed for ransom payments. Combined education's median payment was essentially flat, edging up slightly from $500,000 in 2025 to $515,000 in 2026. Lower education's median payment fell sharply over the same period, from $800,000 to $320,000. The slight rise at the combined level was therefore driven by higher education.

Because fewer than 30 higher education institutions reported a payment figure this year (n=27), we cannot show a reliable standalone trendline for higher education payments, so we recommend using the combined education payment trends.

Percentage of organizations that paid the ransom, by sector

Propensity to pay ransoms differed between the two education cuts. 51% of higher education victims paid the ransom, above the 48% overall survey rate, while 43% of lower education victims paid the ransom, resisting payment more often than the overall survey.

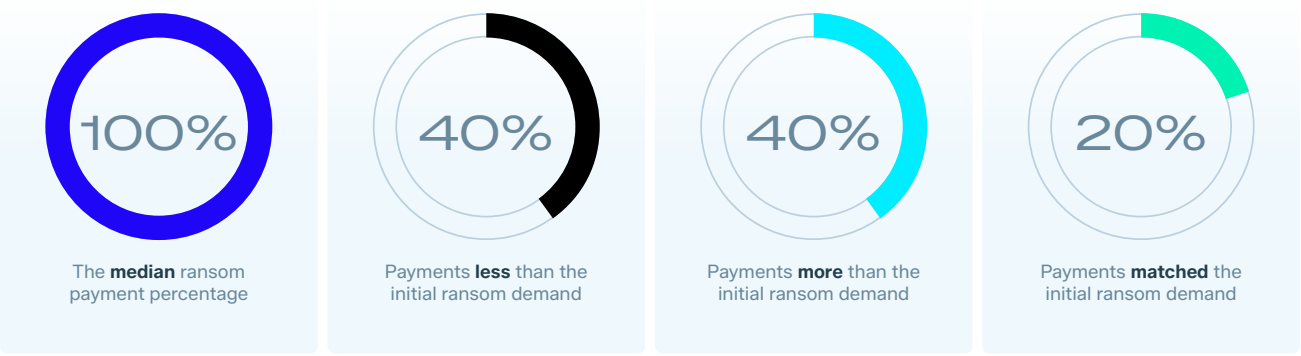
Percentage who paid the ransom by sector



How did your organization get the data back? Base: organizations whose data was encrypted. n=1,214

Actual payments versus initial demands

Among education institutions that paid the ransom, 40% paid less than the initial demand, 40% paid more, and 20% paid exactly what was demanded. The median institution paid 100% of the demand, up from 82% in 2025. So, while a substantial share of institutions negotiated their payment down, an equal share ended up paying more than what was first demanded.



Thinking about the ransom payment made, was it lower than, the same as, or higher than the initial ransom demand? Excluding outliers. Combined higher and lower education. n=58.

Business and human impact

Ransomware recovery costs

Education faced an above-average recovery bill. **The average (mean) cost to rectify a ransomware attack, excluding any ransom paid, was $2.46 million in lower education and $1.99 million in higher education**, both above the $1.7 million overall survey average.

Lower education carried the heaviest burden for two years running. Its average recovery cost edged up from $2.28 million in 2025 to $2.46 million in 2026, making it the most expensive education sector and well above the overall survey ($1.7 million).

Average (mean) recovery cost

	2025	2026
Lower education	$2.28M (n=243)	$2.46M (n=131)
Higher education	$0.90M (n=198)	$1.99M (n=95)
All sectors	$1.53M (n=3,400)	$1.70M (n=2,158)

What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack? Average (mean), excluding any ransom paid. Base numbers in chart.

Higher education is where the gap widened most sharply. Its average recovery cost more than doubled, from $0.90 million in 2025 to $1.99 million in 2026. In the 2025 report, higher education had recorded one of the lowest recovery costs of any sector. This year it converged upward toward lower education. Both education cuts now sit above the overall survey average, which itself rose modestly from $1.53 million to $1.7 million.

$1.09M

The increase in average ransomware recovery costs for higher education from 2025 to 2026.

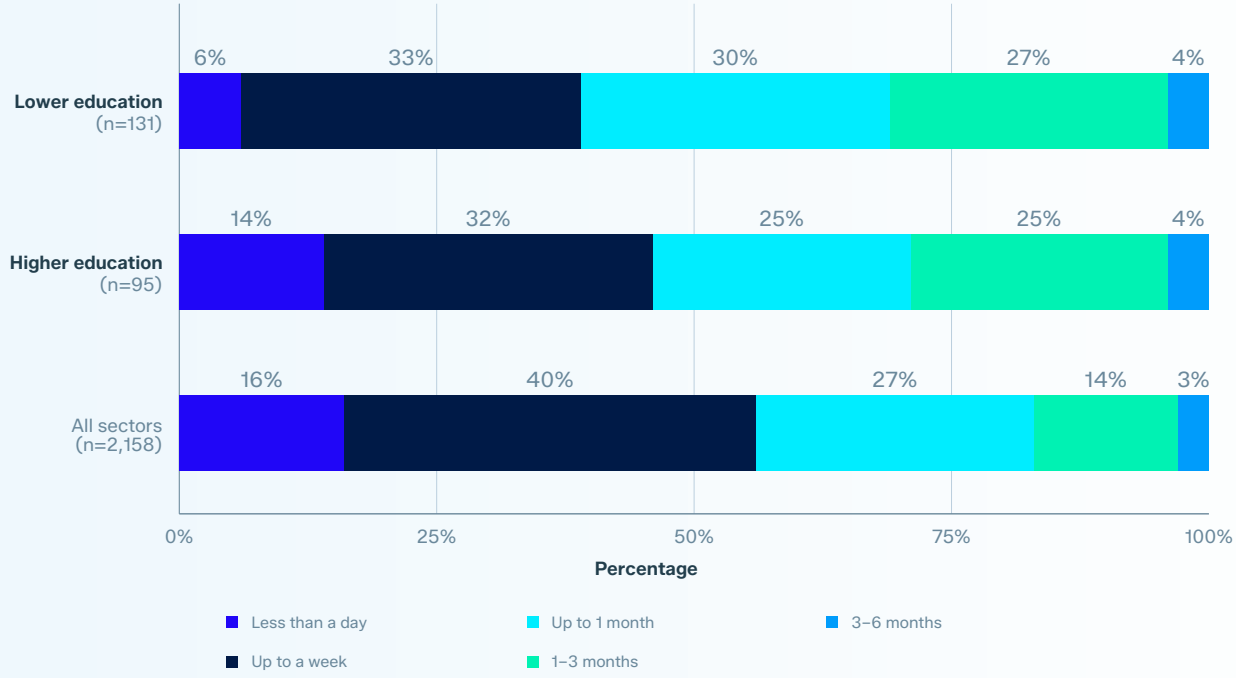
Recovery time

Education providers not only paid more to recover, they also took longer to do so. The clearest divide is in the one-to-three-month recovery band: 27% of lower education and 25% of higher education institutions needed that long to fully recover, compared to just 14% of the overall survey. **Education was nearly twice as likely to face a recovery lasting a month or more**.

31%

The share of lower education institutions that needed at least a month to recover, more than any other sector.

How long it took to recover from ransomware



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

The fast end of the scale tells the same story in reverse. Only 6% of lower education institutions recovered in less than a day, versus 16% of the overall survey and 14% of higher education.

No sector had a larger share of long recoveries than lower education, where 31% of institutions needed at least a month to fully bounce back.

Human impact of ransomware

The human toll on people in education was higher than the overall survey, and each educational sector felt it differently. For higher education, the defining pressure came from above: 53% of teams reported increased pressure from senior leaders, 13 points above the 40% overall survey rate. Changes to the team or organizational structure were also more common in higher education (43% versus 32% across all sectors).

Lower education's experience centered on recognition and workload. Nearly half of lower education teams (49%) reported increased recognition from senior leaders, above the 36% overall survey rate. Recognition can be a positive, but increased workload is not. 43% in lower education cited an ongoing increase in workload, versus 31% across all sectors. The attention cut both ways: more visibility, but also a heavier and more sustained load.

53%

The percentage of higher education IT and security teams that faced increased pressure from senior leaders after an attack, versus 40% across the overall survey.

Human impact of ransomware

Repercussion	Lower education (n=81)	Higher education (n=51)	All sectors (n=1,214)
Increased anxiety or stress about future attacks	40%	33%	41%
Increased pressure from senior leaders	48%	53%	40%
Increased recognition from senior leaders	49%	29%	36%
Changes to team/ organizational structure	33%	43%	32%
Change of team priorities/focus	33%	35%	32%
Feelings of guilt that the attack was not stopped	31%	25%	31%
Ongoing increase in workload	43%	31%	31%
Staff absence due to stress/ mental health issues	40%	39%	29%
Team's leadership was replaced	27%	29%	21%

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

Staff wellbeing suffered across both cuts. 39% of higher education and 40% of lower education teams reported staff absence due to stress or mental-health issues, well above the 29% overall survey rate.

Leadership turnover was also elevated, with 29% of higher education and 27% of lower education teams seeing their leadership replaced after the attack, compared with 21% overall.

Recommendations

Strengthen identity security as a ransomware defense. 73% of education ransomware victims confirmed their ransomware incident was the same event as their most significant identity attack, a higher share than the overall survey's 67%, underscoring the tight link between identity compromise and ransomware in this sector. Education providers should prioritize identity threat detection and response (ITDR), enforce multi-factor authentication across all access points, and regularly audit both human and non-human identity credentials.

Enable MFA comprehensively, specifically phishing-resistant MFA. The survey showed that 98% of education providers with compromised credentials had enabled MFA in some capacity at the time of their attack, but their encryption rates were still high. MFA alone is not enough to stop attacks, and it needs to be comprehensively enabled rather than left on for the SaaS apps that force it and off for VPN logins, firewall admin consoles, and legacy apps.

Strengthen endpoint protection for AI frontier models. Even though reports of exploited vulnerabilities fell in this report, Sophos experts expect exploits to climb again as organizations struggle to keep up with patches for vulnerabilities found by frontier AI. 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 across education, and especially acute in higher education, where lack of in-house expertise stood out as a defining weakness. Dealing with AI-augmented threats will put even more strain on these areas as security teams try to stay current with fast-changing AI technology. Unless you can confidently staff a security operations team in-house, look to an external specialist to fill the gap, either a 24/7 MDR vendor or a managed services provider. Vendors that resolve more incidents end-to-end with AI and automation act as a force multiplier that helps close skills and capacity gaps.

Invest in backup and recovery infrastructure. Backups were the dominant recovery route for both lower and higher education (77% and 69%, both above the overall survey). 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. Exploited vulnerabilities remain a major attack vector and are likely to increase as frontier AI models find new weaknesses faster. Education providers should maintain aggressive patching cadences and focus on mitigations including segmentation, zero trust network access, and MFA/continuous authentication deployments.

Reduce exposure via the firewall and leverage firewall telemetry to detect attacks early. The 2026 data showed firewalls are good at spotting the signs of ransomware, with 65% having enough data to identify an attack before the ransomware was detonated. But even in those early detection cases, victims in education still had their data encrypted 51% of the time, because the firewall often can't confirm or stop an attack without telemetry from other control points. Ensure your firewall receives rapid, ideally automated, updates and minimize internet-facing services like admin access and user portals. Connect firewalls to XDR and MDR so firewall telemetry helps detect ransomware attacks before payloads deploy. A cybersecurity defense system, where controls share signal, is the answer.

Recommended actions at a glance:

1. Segmentation to slow attackers down
2. ZTNA to replace legacy VPNs and contain app exploits
3. Identity threat detection and response (ITDR) to harden identity infrastructure
4. Phishing-resistant MFA as the destination rather than the starting line
5. Disciplined patching of internet-facing devices
6. 24/7 detection and response

Conclusion

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

There are signs of progress: ransom demands are declining, backup-based recovery has surged to near-record levels, and ransom payments by education providers are low compared to other sectors.

At the same time, the challenges that remain are significant. Over half of ransomware attacks against education still succeed in encrypting data, average recovery costs run to $2.26 million per incident (higher than the overall survey), and lower education had the largest share of recoveries lasting a month or longer.

Identity is where education's exposure concentrates. A greater share of education providers confirmed their ransomware incident was the same event as their most significant identity attack compared to the overall survey. For a sector where recovery is already slower and costlier, that tight coupling makes identity infrastructure the highest-leverage place to invest.

Education providers also need to prepare for the defining cybersecurity challenge of the next decade: AI-augmented threats. The data already hints at why: 62% of education organizations cited a security gap, known or unknown, as a factor in their attack, and 63% 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.

There's a deeper signal in this year's root-cause data, too. The perceived root-cause mix is equalizing; across all sectors, education included, no single vector dominates. That makes focusing defenses too narrowly on any one root cause risky, because attackers are succeeding through multiple vectors.

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

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

SOPHOS

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

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

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

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

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

2026-08-25 EN (DD)