SOPHOS

The State of Ransomware in Education 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity across 14 countries, including 600 from the education sector, conducted in January-February 2024.

A Sophos Whitepaper. July 2024

Introduction

The fifth annual Sophos study of the real-world ransomware experiences of organizations around the globe explores the full victim journey, from root cause to severity of attack, financial impact, and recovery time. Fresh new insights combined with learnings from our previous studies reveal the realities facing education providers today and how the impact of ransomware has evolved over the last five years.

This year's report also incorporates brand new areas of study, including an exploration of ransom demands vs. ransom payments. Plus, for the first time, it shines a light on the role of law enforcement in ransomware remediation for education providers.

A note on reporting dates

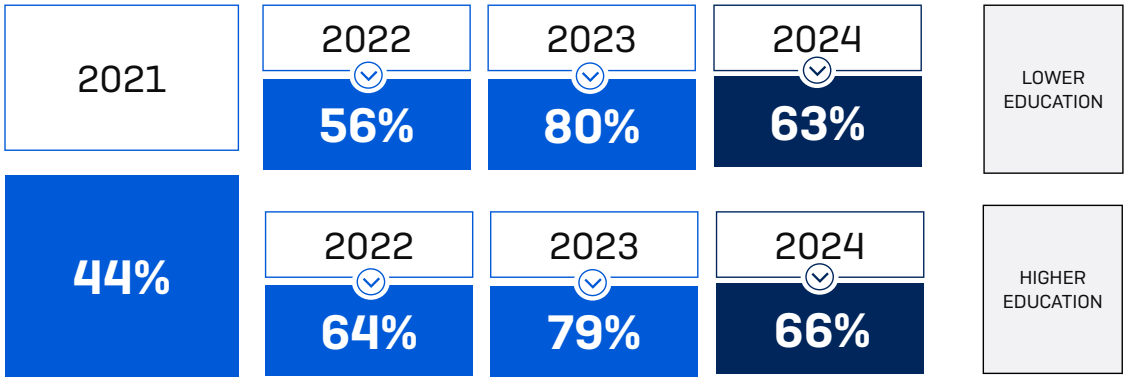
To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2024. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2023.

About the survey

The report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. 600 respondents were from educational organizations, split into 300 from lower education (catering to students up to 18 years) and 300 from higher education (for students over 18 years). All respondents represent organizations with between 100 and 5,000 employees. The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants were asked to respond based on their experiences over the previous year.

Rate of Ransomware Attacks in Education

63% of lower education and 66% of higher education organizations were hit by ransomware in the last year, a considerable decrease from the 80% and 79% reported in 2023, respectively. Nonetheless, the attack rates in education remain higher than the global cross-sector average, which came in at 59% this year, down from 66% in 2023.



In the last year, has your organization been hit by ransomware?
Yes. n=300 (2024)/ 200 (2023), 320 (2022) lower education organizations; n=300 (2024)/ 200(2023)/ 410 (2022) higher education organizations

The education sector no longer reports the two highest rates of attack, with the unwelcome top spot now held by *central/federal government* (68%), followed by *healthcare* and *energy, oil/gas and utilities* (both 67%).

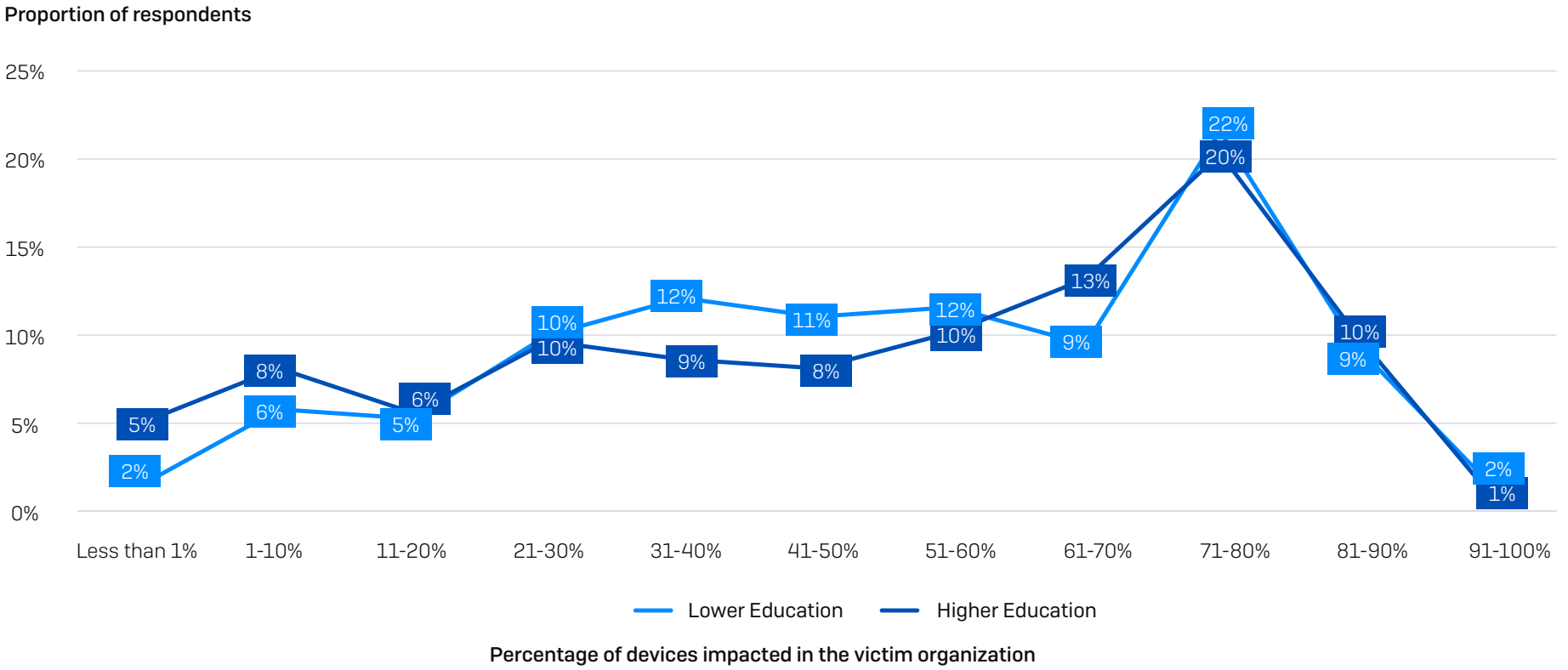
See the appendix for a detailed breakdown of the rate of ransomware attacks by industry.

Percentage of Computers Impacted in Education

On average, 52% of computers in lower education and 50% in higher education are impacted by a ransomware attack, slightly above the cross-sector average of 49%. Having a full environment encrypted is extremely rare. Only 2% of lower education organizations and 1% of higher education organizations reported that 91% or more of their devices were impacted. At the other end of the scale, while some attacks do impact only a handful of devices, this too is highly unusual – only 2% of affected lower education and 5% of higher education organizations said that fewer than 1% of their devices were affected.

Across all sectors globally, *IT, technology and telecoms* reported the smallest percentage of devices impacted (33%). The *energy, oil/gas and utilities* sector experienced the effects of an attack most broadly, with 62% of devices impacted, on average, followed by *healthcare* (58%). Both industries are challenged by higher levels of legacy technology and infrastructure controls than most other sectors, which likely makes it harder to secure devices, limit lateral movement, and prevent attacks from spreading.

See the appendix for a detailed breakdown of the percentage of computers impacted by industry.

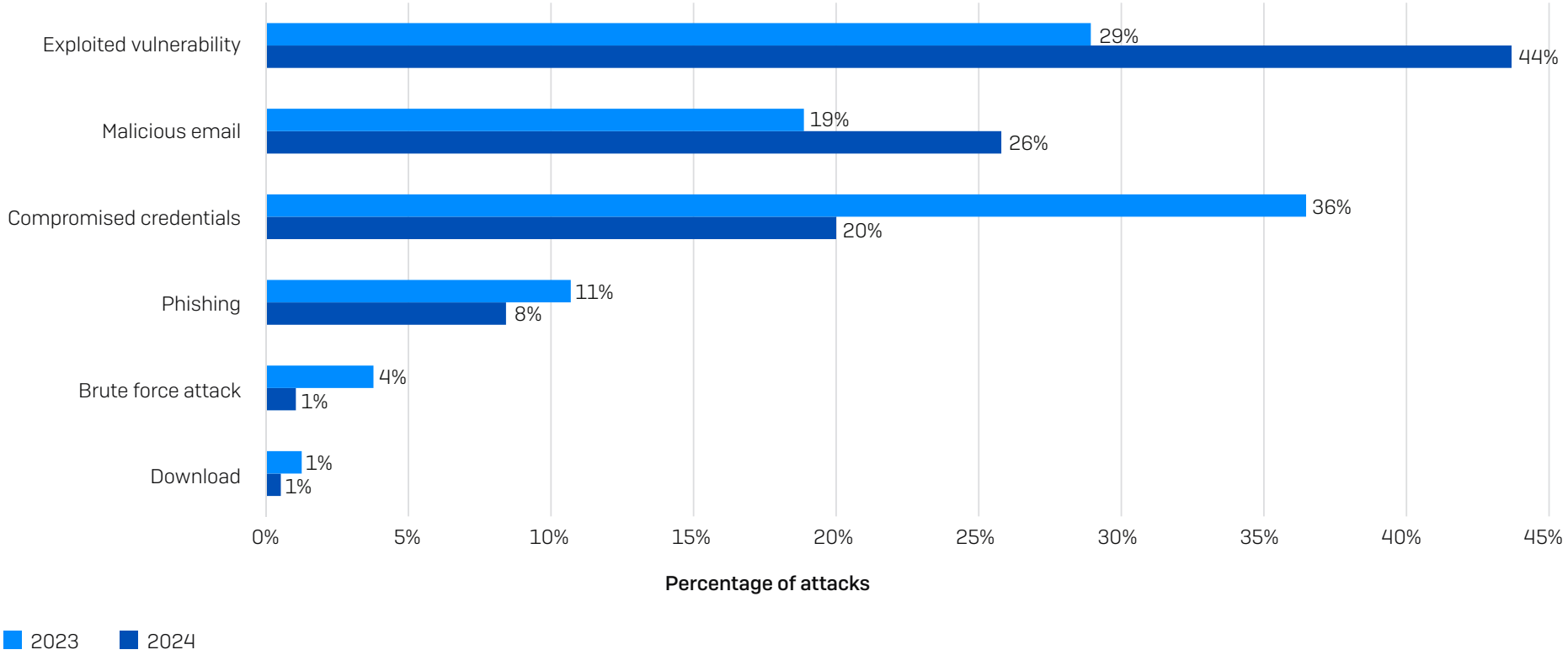


What percentage of your organization's computers were impacted by ransomware in the last year? n=190 lower education and 197 higher education organizations hit by ransomware.

Root Causes of Ransomware Attacks in Education

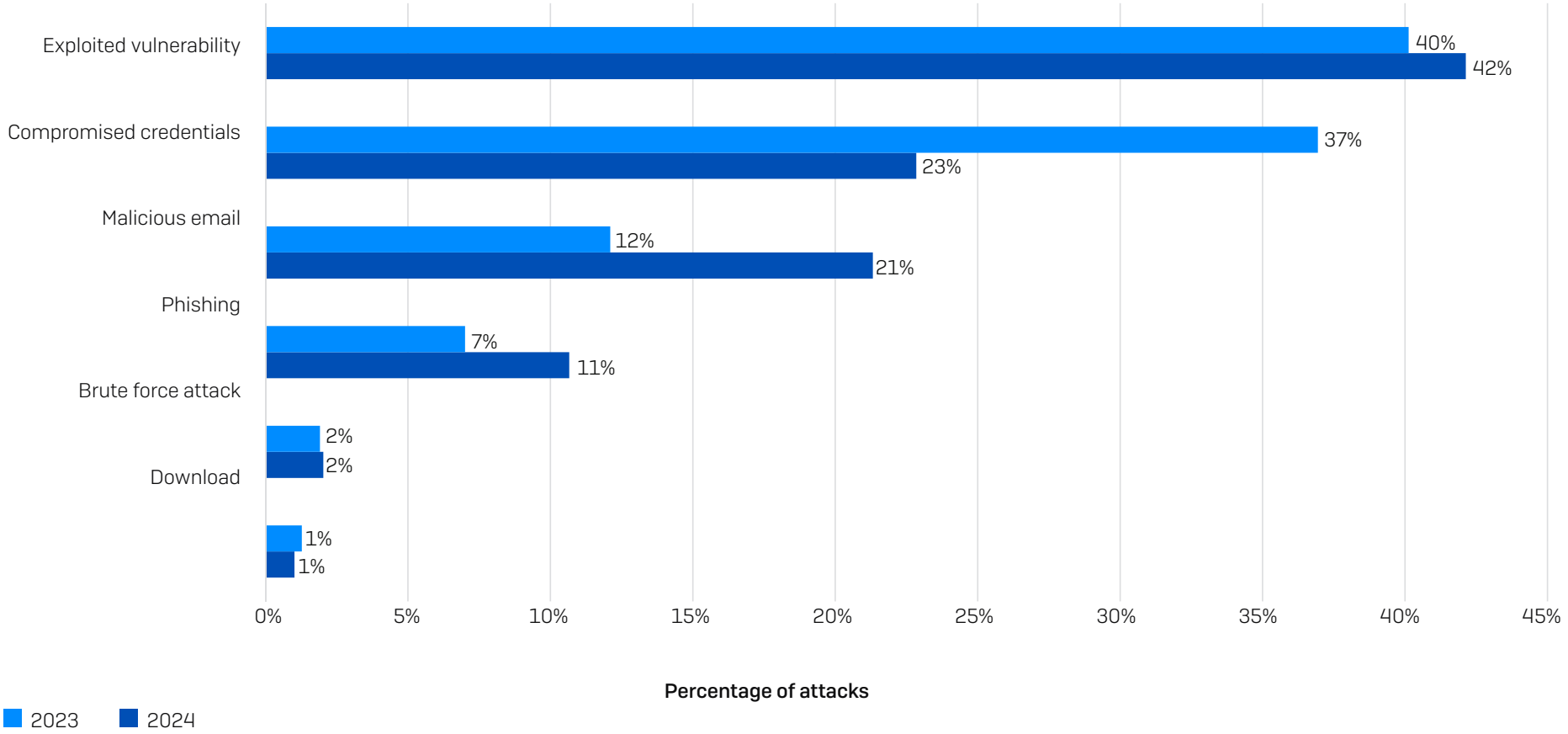
99% of lower education and all higher education organizations hit by ransomware were able to identify the root cause of the attack. Exploited vulnerabilities were the most common root cause of attacks in educational organizations (lower education (44%) and higher education organizations (42%)). Malicious emails (26%) ranked as the second most common attack method in lower education, whereas compromised credentials (23%) were the second most frequent entry method in higher education.

Root Cause of Ransomware Attacks in Lower Education



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n = 190 lower education organizations hit by ransomware.

Root Cause of Ransomware Attacks in Higher Education



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=197 higher education organizations hit by ransomware.

For the second year in a row, across all sectors globally, exploited vulnerabilities topped the list as the most common root cause (32%) of ransomware attacks, with compromised credentials in second place (29%).

Education organizations are particularly exposed to the risks of unpatched vulnerabilities, with only the *energy, oil/gas and utilities* sector reporting a greater percentage of attacks that started this way.

Government organizations are particularly vulnerable to attacks that start with abuse of compromised credentials: 49% *(state/local)* and 47% *(central/federal)* of attacks began with the use of stolen login data. *IT, technology and telecoms* and *retail* both reported that 7% of ransomware incidents began with a brute force attack – it may be that their reduced exposure to unpatched vulnerabilities and compromised credentials forces adversaries to focus, in part, on other approaches.

See the appendix for a detailed breakdown of the rate of the root cause of attack by industry.

Backup Compromise in Education

95% of educational organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. Of them, 71% were successful – the second highest rate of successful backup compromise across all sectors after the *energy, oil/gas and utilities* sector.

Educational organizations that had their backups compromised reported considerably worse outcomes than those whose backups were not breached:

- Ransom demands: Initial asks in lower education were, on average, 5X that of those whose backups weren't impacted ($4.72M vs. $850,000 median initial ransom demand). In higher education organizations, ransom demands were almost double that of those whose backups weren't impacted ($4.08M vs. $2.65M median initial ransom demand)
- Ransom payment rate: Lower education organizations whose backups were compromised were more than 3X as likely to pay the ransom to recover encrypted data (75% vs. 21%). Higher education organizations were more than 2X as likely to pay the ransom to recover encrypted data (75% vs. 35%)
- Recovery costs: Median overall recovery costs in lower education came in 5X higher than that of those that did not have backups compromised ($3,000,000 vs. $562,500). For higher education organizations, this was 4X higher than that of those that did not have backups compromised ($3,000,000 vs. $750,000).

Rate of Data Encryption in Education

85% of ransomware attacks on lower education and 77% on higher education organizations resulted in data encryption in our 2024 study, slightly higher than 81% and 73%, respectively, reported in the previous year and above the 2024 cross-sector average of 70%.

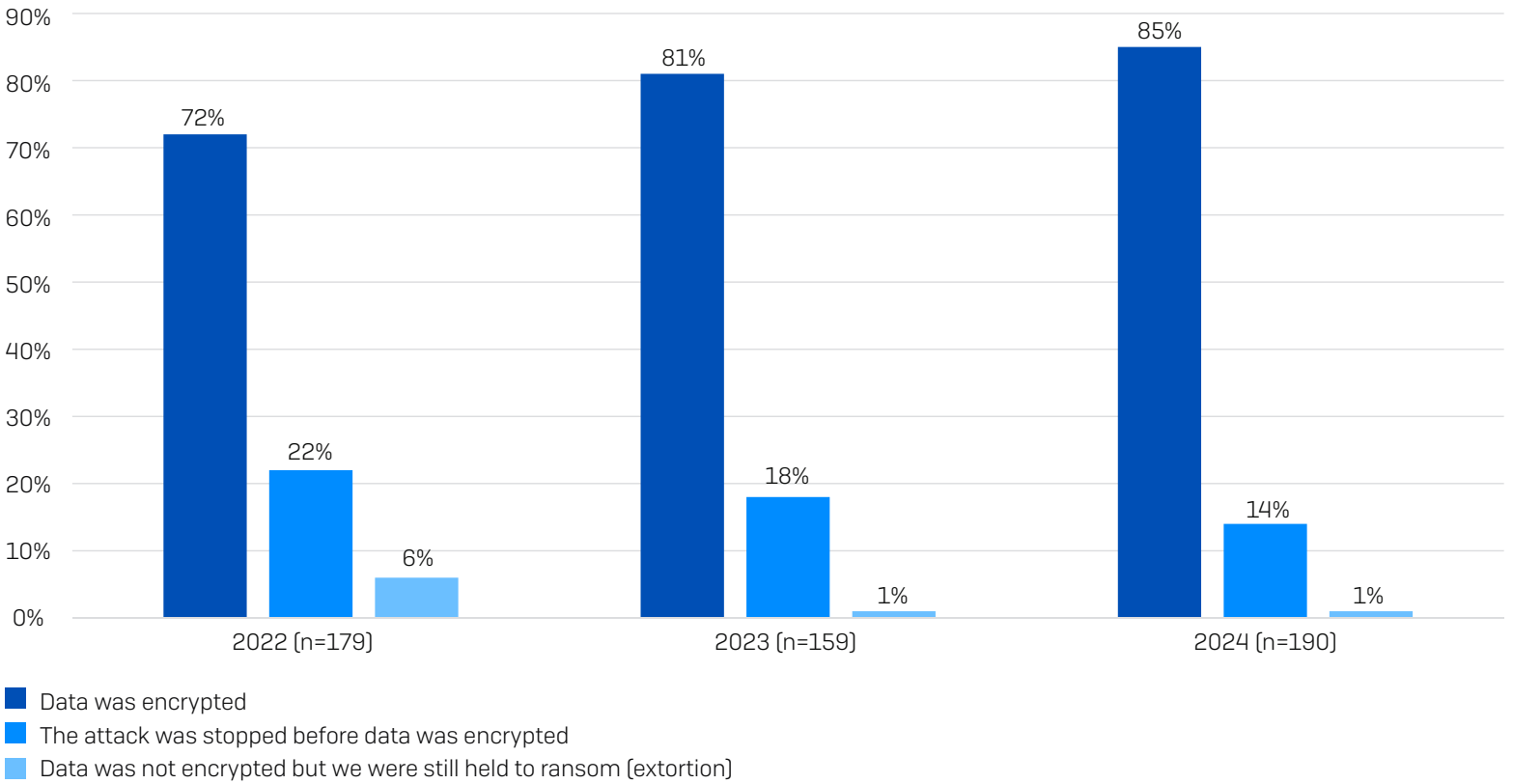
1% of lower education and 2% of higher education organizations also experienced an extortion-based attack, where the data was not encrypted, but they were held to ransom anyway.

For lower education, this is the second consecutive year of an increase in encryption rate, with only *state/local government* (98%) more likely to have data encrypted in an attack.

Financial services (49%), followed by *retail* (56%), reported the lowest rates of data encryption. *Distribution and transport* is the sector most likely to have experienced an extortion-based attack, with 17% saying that data was not encrypted, but they were held to ransom anyway – almost three times the rate of any other sector.

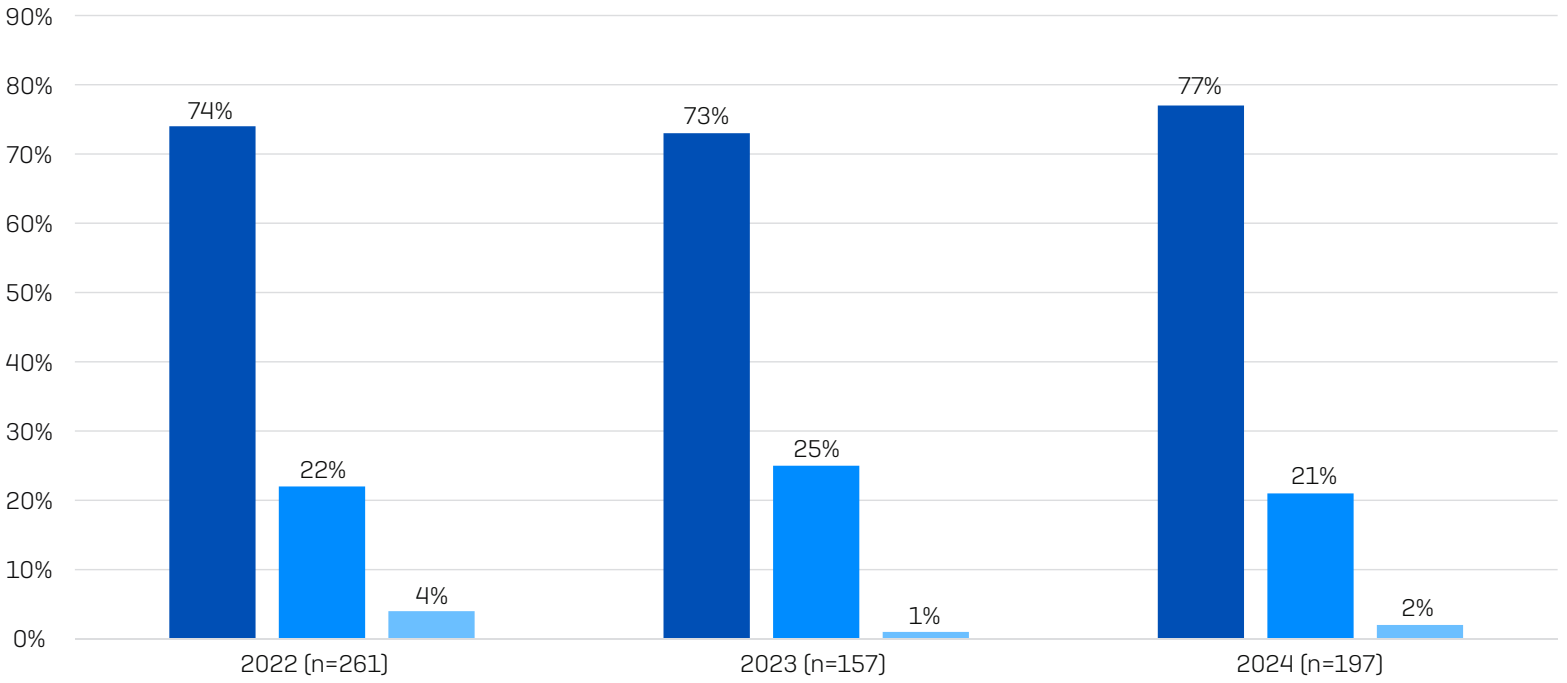
See the appendix for a detailed breakdown of the data encryption rates by industry.

Data Encryption in Lower Education



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

Data Encryption in Higher Education



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

Data Theft

Adversaries don't just encrypt data; they also steal it. In lower education, 22% of ransomware attacks where data was encrypted also resulted in data theft, down from 27% in our 2023 study. Higher education also experienced a drop in double-extortion, with cybercriminals stealing data in 18% of encryption events, considerably below the 35% reported last year. Data theft increases attackers' ability to extort money from their victims while also enabling them to further monetize the attack by selling the stolen data on the dark web.

Lower Education	Higher Education
22%	**18%**
of ransomware attacks where data was encrypted reported that data was also stolen	**of ransomware attacks where data was encrypted reported that data was also stolen**

Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes. Yes, and the data was also stolen (n=190 lower education organizations; n=197 higher education organizations)

Across sectors, the education sector is least likely to report data theft in an attack. Higher education reports the lowest overall propensity to have data encrypted and stolen, followed by lower education, which shares the second spot with *healthcare* (both 22%). The *IT, technology and telecoms* sector has the highest propensity (53%) to have data exfiltrated as well as encrypted, followed by *energy, oil/gas and utilities* (50%).

Data Recovery

98% of lower education and 97% of higher education organizations that had data encrypted got their data back. Of them, 62% in lower education paid the ransom to get encrypted data back, while 75% restored encrypted data using backups. At the same time, 67% of higher education organizations paid the ransom to restore data, whereas 78% used backups.

Across sectors, higher education reported the second-highest propensity to use backups for data restoration along with *state/local government* organizations. *Central/federal government* ranks first in terms of backup use at 81%. Higher education also ranks second-highest in terms of the propensity to pay the ransom to restore encrypted data, whereas lower education organizations rank third. *Media, leisure and entertainment* has the highest propensity to pay the ransom (69%).

28% of lower education and 25% of higher education organizations used other means to get data back – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.

Data Recovery in Lower Education

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
75%	62%	28%

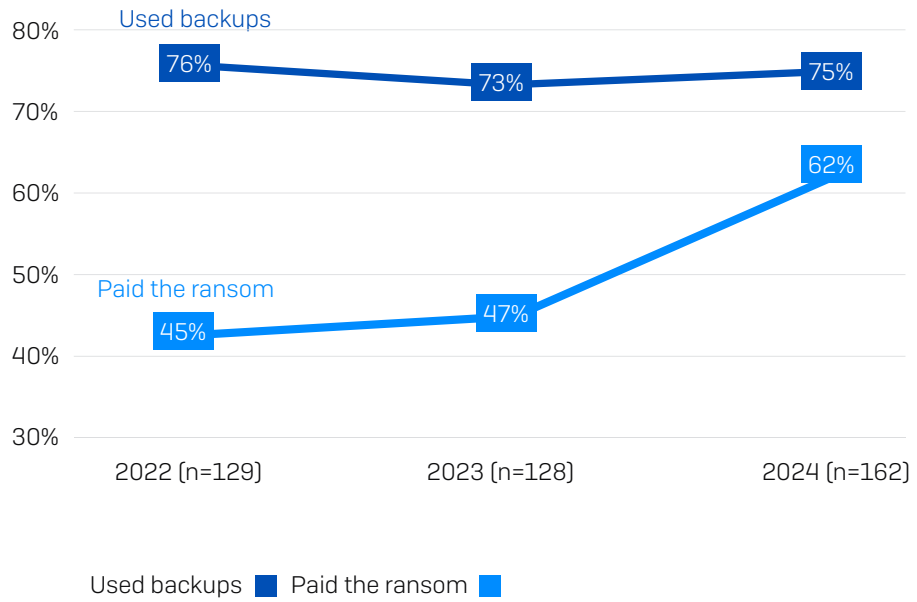
Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data (Lower education n=162)

Data Recovery in Higher Education

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
78%	67%	25%

Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data (Higher education n=152)

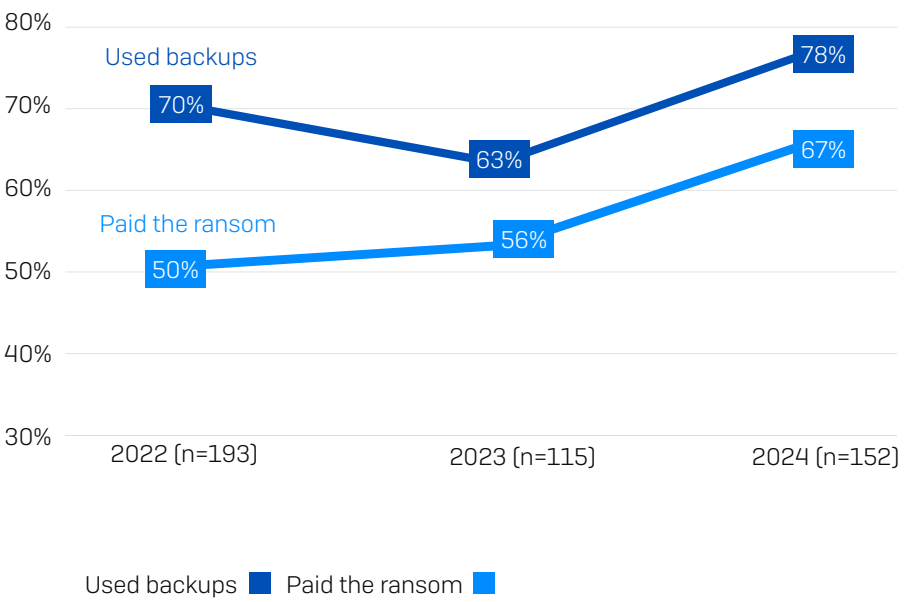
Data Recovery in lower education



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.

The last three-year view of the education sector reveals an increase in backup use. In our 2023 study, higher education was among the bottom three sectors globally for backup use, jumping to second place in 2024, alongside *local/state government*. Unfortunately, the propensity to pay the ransom has progressively increased for both lower and higher education organizations in the last three years.

Data Recovery in higher education



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.

A notable change over the last year is the increase in the propensity for victims to use multiple approaches to recover encrypted data (e.g., paying the ransom and using backups). This time, 65% of lower education and 69% of higher education organizations that had data encrypted reported using more than one method, almost three times the rates reported in 2023 (23% in lower education and 22% in higher education organizations.)

See the appendix for a detailed breakdown of the data recovery method by industry.

Ransom Demands

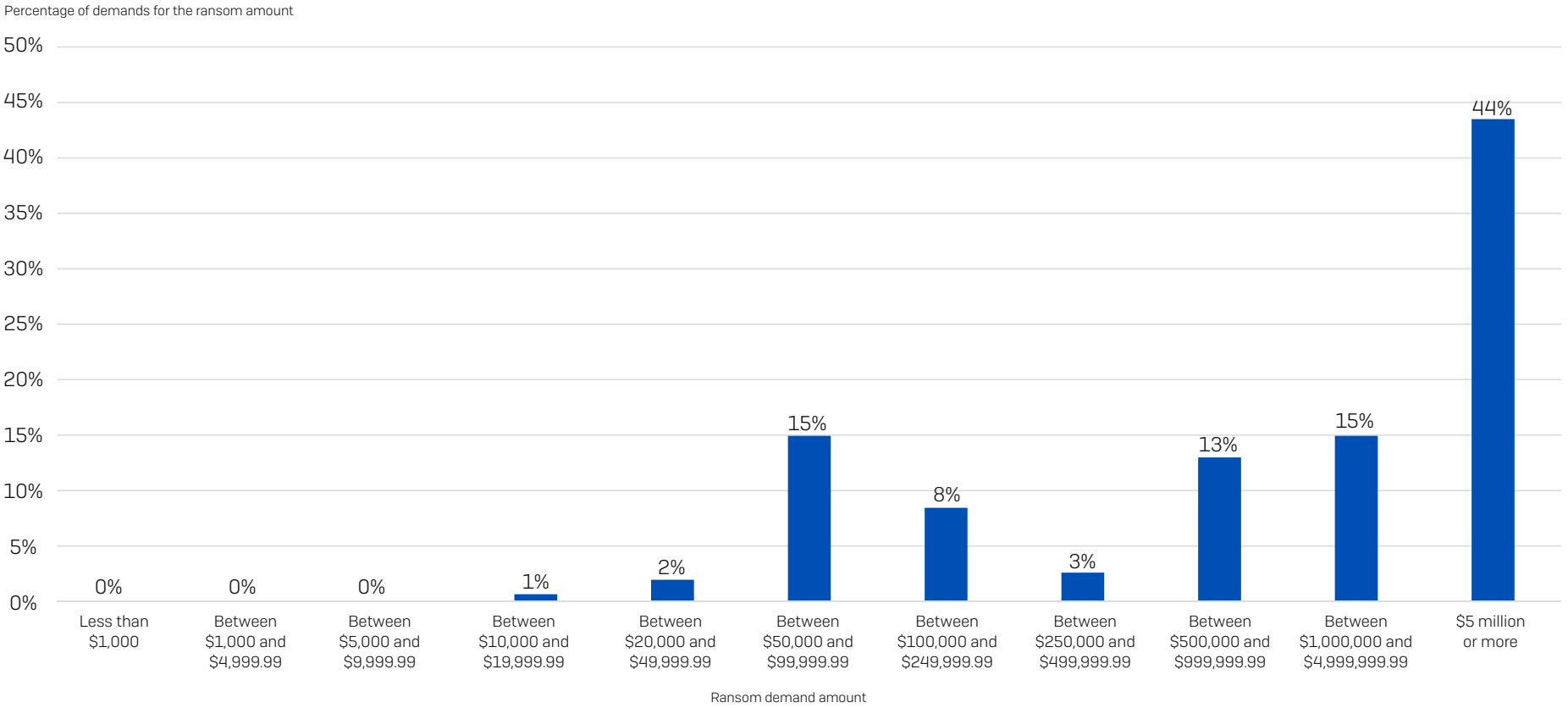
This year, for the first time, we included both ransom demands and payments in this report. Of the 154 lower education organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was $3.9M (median) and $5.9M (mean). 58% of ransom demands made to lower education organizations are for $1M or more, with approximately half of the demands (44%) for $5M or more.

Across 130 higher education organizations, the average initial ransom demand was $3.6M (median) and $4.8M (mean). 67% of ransom demands made to higher education organizations are for $1M or more, with more than one-third of the demands (35%) for $5M or more.

These huge demands are not exclusive to the education sector, with all named sectors (excluding "other") reporting median ransom demands of $1M or higher. *Central/federal government* reported the highest median ($7.7M) and mean ($9.9M) demands, whereas *retail* and *IT, technology and telecoms* received the lowest median demands ($1M), followed by *construction* ($1.1M)

See the appendix for a detailed breakdown of ransom demands by industry.

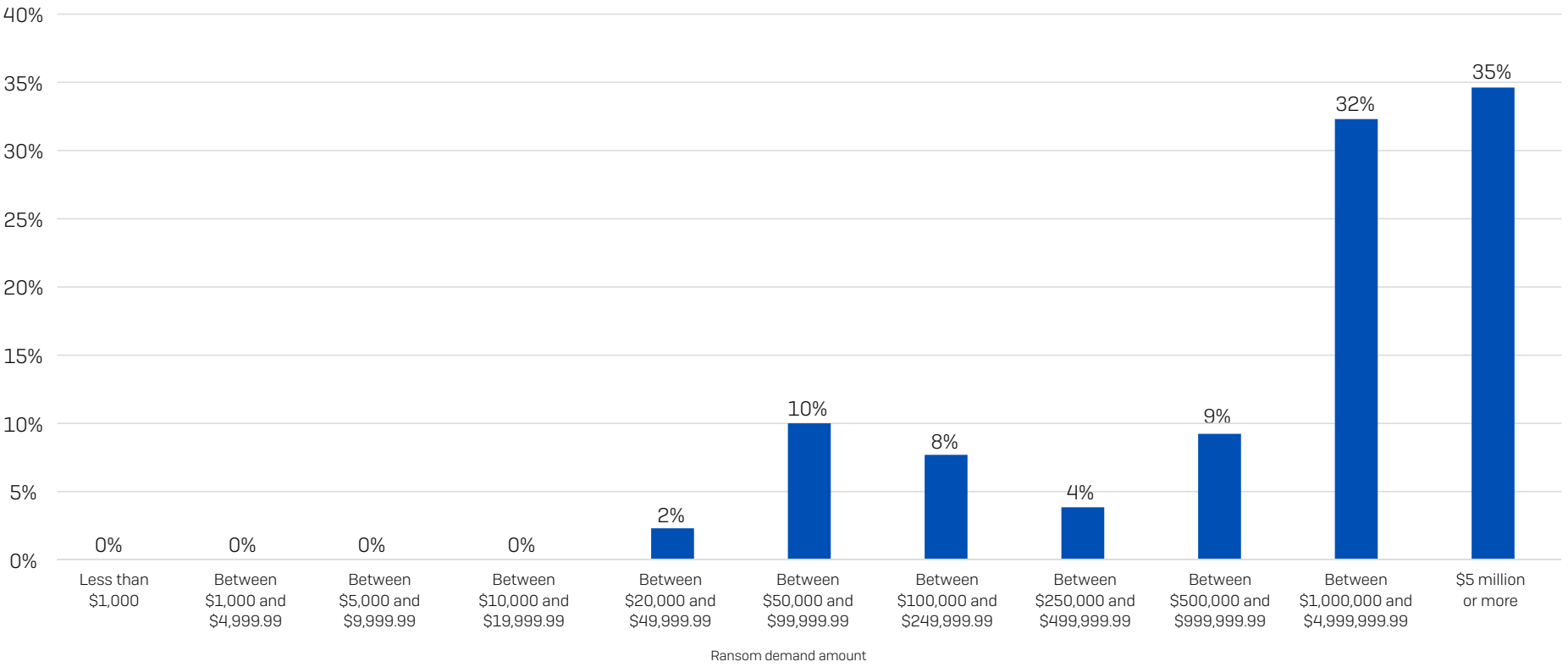
Ransom demand in lower education



How much was the ransom demand from the attacker(s)? n=154

Ransom demand in higher education

Percentage of demands for the ransom amount



How much was the ransom demand from the attacker(s)? n=130

Ransom Payments

99 lower education and 92 higher education respondents whose organizations paid the ransom shared the actual sum paid.

Lower education:

- Median payment: $6.6M
- Mean payment: $7.5M

Higher education:

- Median payment: $4.4M
- Mean payment: $5.9M

Ransom payments vary considerably by industry. Lower education, joint with *central/ federal government,* paid the highest median ransom, followed by higher education. *IT, technology and telecoms* reported the lowest median ransom payment ($300,000), followed by *distribution and transport* ($440,000).

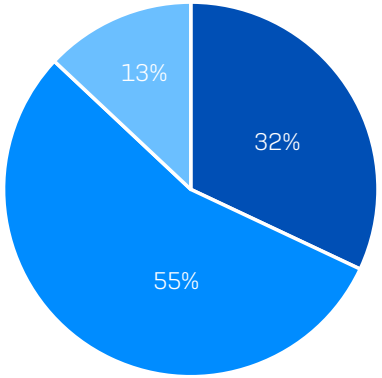
See the appendix for a detailed breakdown of average ransom payment by industry.

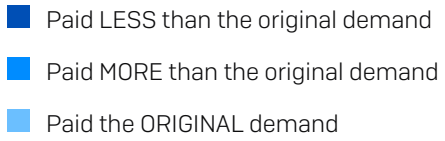
Propensity to Negotiate Ransom Amounts in Education

The study has revealed that education victims don't typically pay the initial sum demanded by the attackers: only 13% said their payment matched the original request. 32% of lower education and 20% of higher education respondents paid less than the original demand, while 55% of lower education and 67% of higher education organizations paid more. Overall, higher education is the sector most likely to pay more than the original demand.

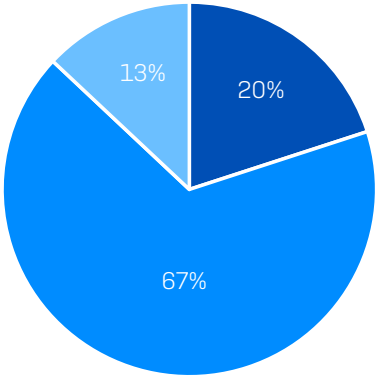
The sectors most likely to pay more than the original demand are those with a high proportion of public sector organizations. It may be that these industries are less able to access professional ransom negotiators to help reduce their costs. They may also have a greater need to recover the data "at any cost" due to their public remit. Either way, it's clear that there is room for negotiation between the original demand and the eventual payment.

Propensity to negotiate ransom amount in lower education





Propensity to negotiate ransom amount in higher education



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=99 lower education organizations, n=92 higher education organizations

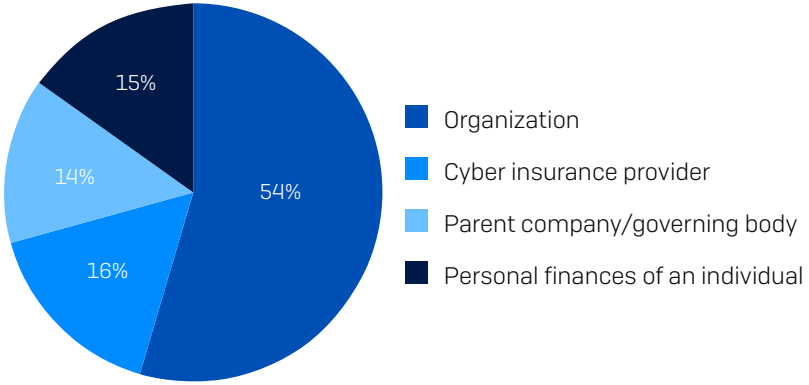
See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

Source of Ransom Funding in Education

Who provides the money for the ransom is an area of considerable interest, and the study has revealed a number of insights in this area:

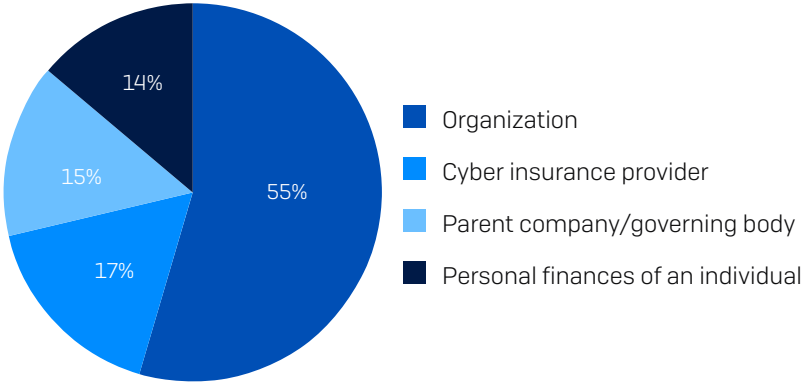
- Funding the ransom is a collaborative effort, with lower and higher education respondents reporting multiple sources of monies in 64% and 62% of cases, respectively
- The primary source of ransom funding in lower education is the organization itself, covering 54% of the payment on average; the organization's parent company and/or governing body typically provides 14%.
- The primary source of ransom funding in higher education is again the organization itself, covering 55% of the payment on average; the organization's parent company and/or governing body typically provides 15%.
- Insurance providers are heavily involved in ransom payments: 16% of total ransom payment funding comes from insurance providers in lower education organizations and 17% comes from insurance providers in higher education organizations.

Source of Ransom Payment Funding in Lower Education



From which of the following source(s) was the money to fund the ransom payment obtained? n=100

Source of Ransom Payment Funding in Higher Education



From which of the following source(s) was the money to fund the ransom payment obtained? n=102

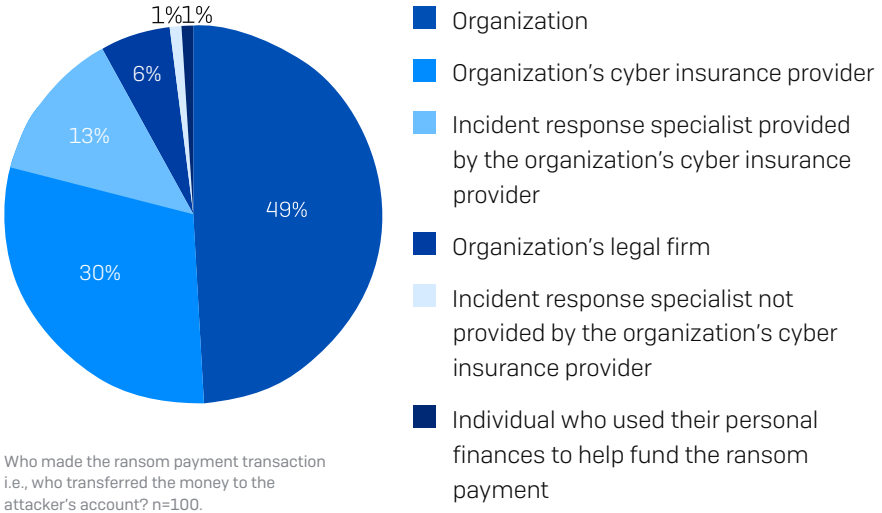
Ransom Transaction Execution

While multiple bodies can contribute to the ransom, funds are typically transferred in a single payment by one party.

In the lower education sector, the victim organization made almost half (49%) of the transactions. Insurance providers transferred the funds for 43% of ransom payments, either directly (30%) or through their appointed incident response specialist (13%). 6% were executed by the victim's legal firm. Only 14% of transfers were made by incident response specialists, whether appointed by the insurance provider (13%) or another party, typically the victim (1%).

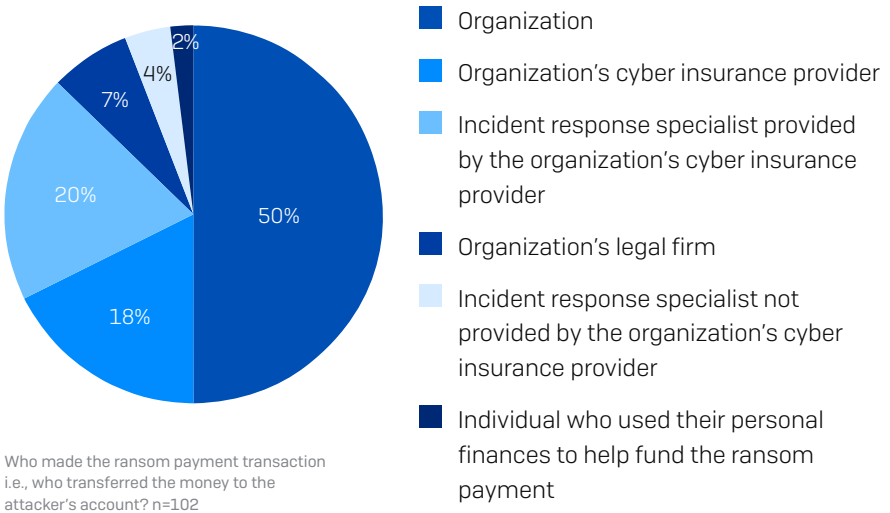
In the higher education sector, the victim organization made half (50%) of the transactions. Insurance providers transferred the funds for 37% of ransom payments, either directly (18%) or through their appointed incident response specialist (20%). 7% were executed by the victim's legal firm. Almost one-quarter (24%) of transfers were made by incident response specialists, whether appointed by the insurance provider (20%) or another party, typically the victim (4%).

Executor of Ransom Payment Transfer in Lower Education



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=100.

Executor of Ransom Payment Transfer in Higher Education



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=102

Recovery Costs in Education

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, lower education organizations reported a mean cost of $3.76M to recover from a ransomware attack, more than double the $1.59M reported in our 2023 survey; higher education organizations reported a mean cost of $4.02M, almost four times higher than the $1.06M reported in 2023.

In contrast, the cross-sector average showed a 50% increase in recovery costs, coming in at $2.73M in 2024, an increase of almost $1M from 2023 ($1.82M).

	2022	2023	2024
Lower Education	$1.58M	$1.59M	$3.76M
Higher Education	$1.42M	$1.06M	$4.02M

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.)? n=190 (2024)/159 (2023)/ 179 (2022) lower education organizations; n=197 (2024)/ 157 (2023)/ 261 (2022) higher education organizations N.B. 2022 question wording also included "ransom payment".

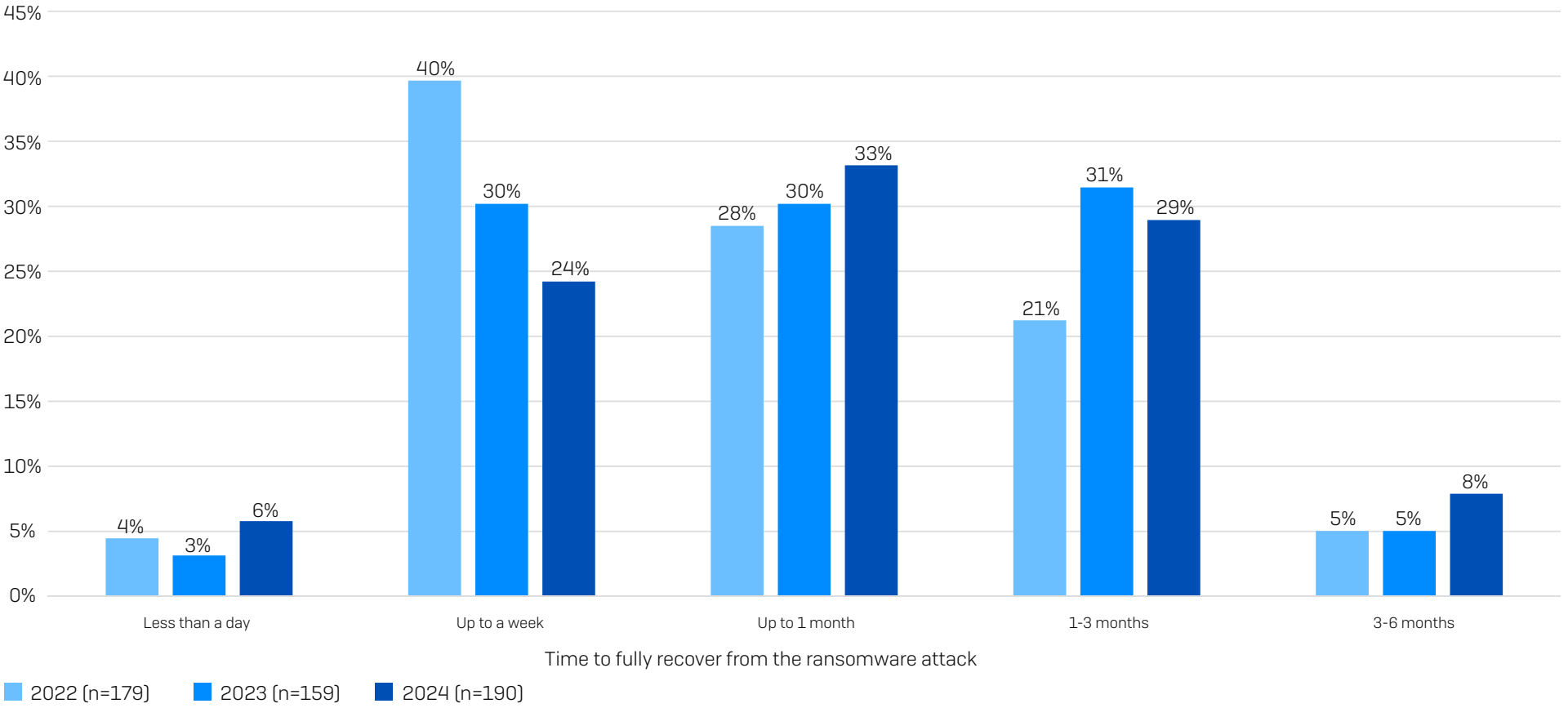
The median recovery cost data for lower education organizations revealed a 4X increase, from $750,000 in 2023 to $3,000,000 in 2024. Higher education organizations reported an 8X increase from $375,000 in 2023 to $3,000,000 in 2024. These figures are considerably above the cross-sector average, where median recovery costs doubled from $375,000 to $750,000 over the last year.

Recovery Time in Education

The time taken to recover from a ransomware attack has largely remained steady in lower education, whereas it has increased for higher education organizations over the last year. Our 2024 research revealed:

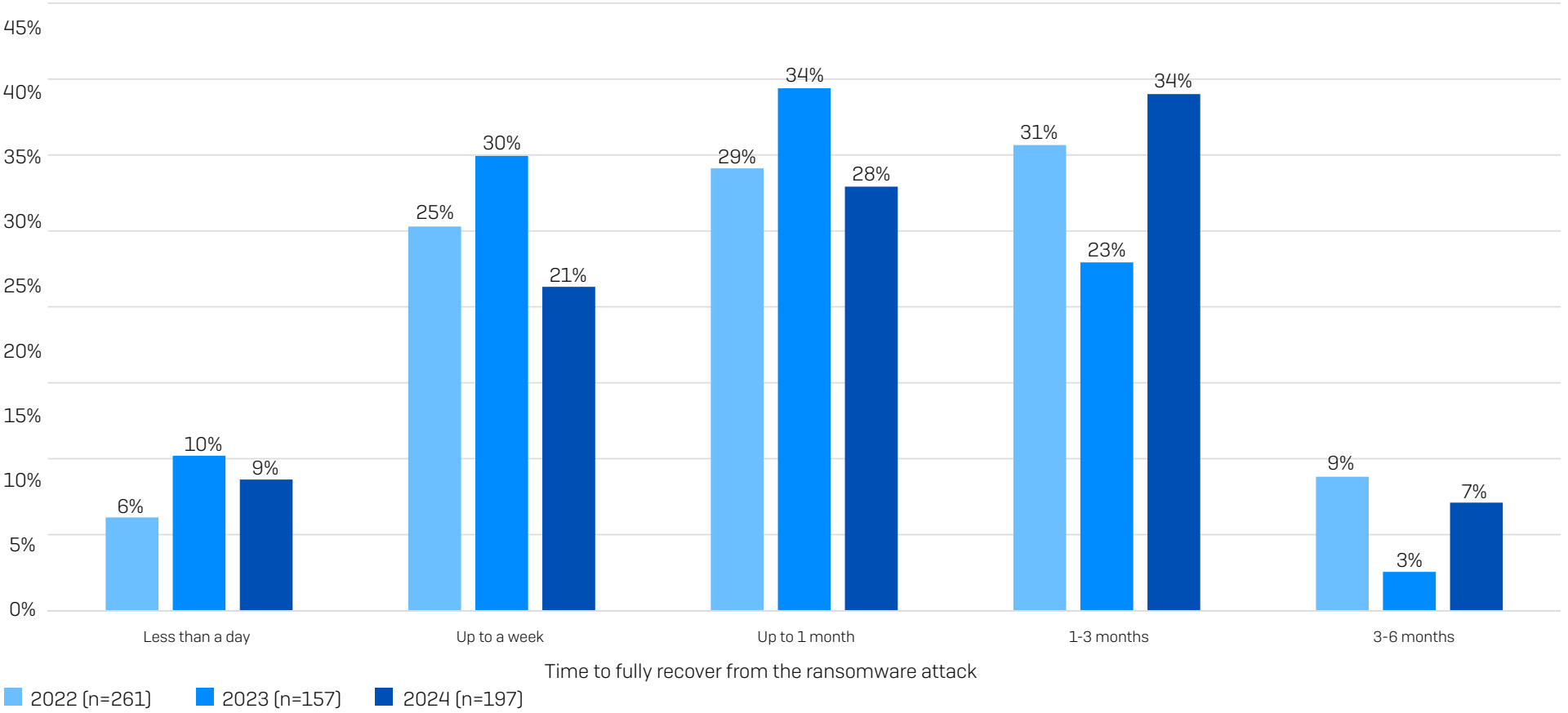
- 30% of ransomware victims in both lower and higher education were fully recovered in a week or less, down from last year's 33% (lower) and 40% (higher).
- 37% of lower education organizations took more than a month to recover, similar to the 36% reported in 2023.
- In higher education organizations, 41% took more than a month to recover, compared to 25% in 2023.

Recovery Time in Lower Education



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

Recovery Time in Higher Education



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

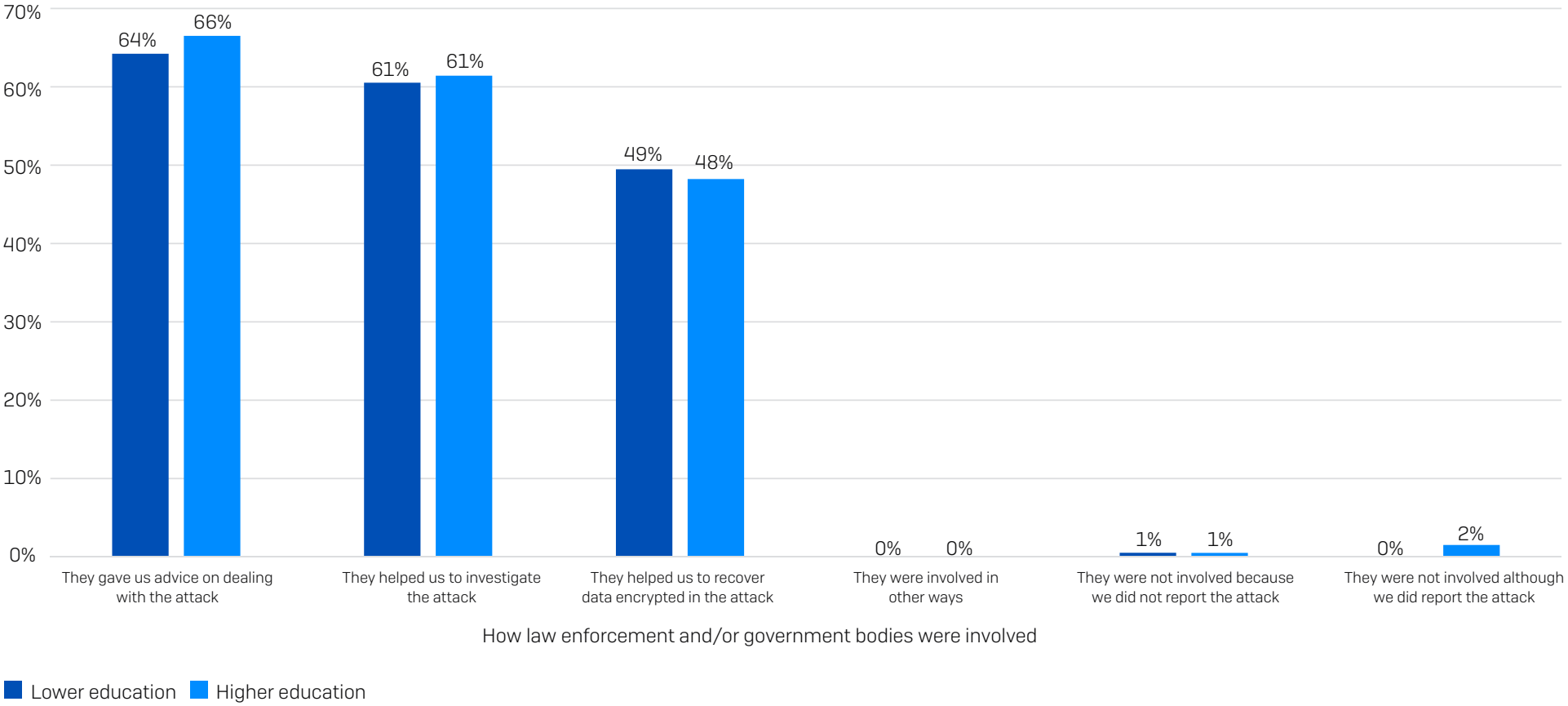
Involvement of Law and Order in Education

The nature and availability of official support when dealing with a ransomware attack vary on a country-by-country basis, as do the tools to report a cyberattack. US victims can leverage the Cybersecurity and Infrastructure Security Agency (CISA); those in the UK can get advice from the National Cyber Security Centre (NCSC); and Australian organizations can call on the Australian Cyber Security Center (ACSC), to name but a few.

Reflecting the normalization of ransomware, 99% of lower education and 98% of higher education organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack.

64% of lower education and 66% of higher education organizations reported that they received advice on dealing with the attack, 61% of both lower and higher education organizations got help investigating the attack, and 49% and 48%, respectively, said they received help recovering data encrypted in the attack.

Involvement of Law Enforcement/ Official Bodies in Education



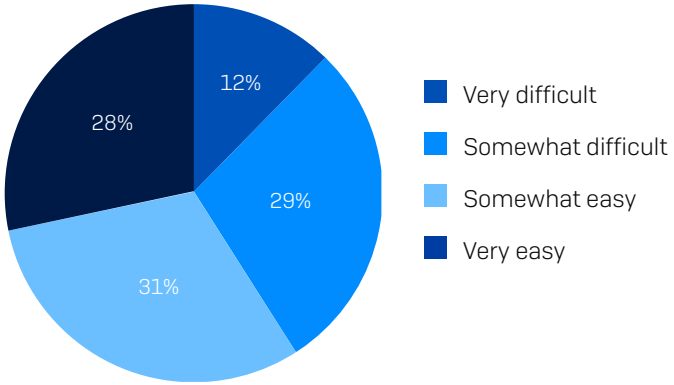
If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? n= 190 lower and 197 higher education organizations

Ease of Engagement in Education

59% of lower education and 63% of higher education organizations that engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (28% very easy and 31% somewhat easy in lower education; 27% very easy and 36% somewhat easy in higher education).

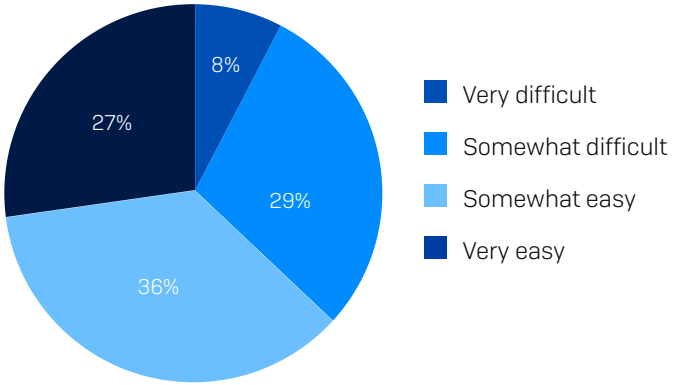
12% in lower education and 8% in higher education said the process was very difficult, while 29% in both lower and higher education described it as somewhat difficult. While it is encouraging that some found the process easy, there is clearly room to improve the engagement experience for the sector.

Ease of Engagement with Official Bodies in Lower Education



How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=188 (not showing "don't know" responses).

Ease of Engagement with Official Bodies in Higher Education



How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=196 (not showing "don't know" responses).

Conclusion

Ransomware remains a major threat to education organizations of all sizes around the globe. While the attack rate in education has dropped in the last year, two-thirds of education organizations are hit by ransomware attacks, which is a cause for concern. Furthermore, the cost of recovering from an attack has more than tripled in the education sector in the last year. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace.

Prevention. The best ransomware attack is the one that didn't happen because the adversaries couldn't get into your organization. With over 40% of attacks in the education sector starting with the exploitation of unpatched vulnerabilities, it's important to take control of your attack surface and deploy risk-based prioritization of patching. The use of MFA to limit credential abuse should also be a priority for every single organization. Ongoing user training on how to detect phishing and malicious emails remains essential.

Protection. Strong foundational security, including endpoint, email, and firewall technologies, is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure they are well-defended, including dedicated anti-ransomware protection to stop and roll back malicious encryption. Security tools need to be correctly configured and deployed to provide optimal protection, so look for solutions that deploy out of the box with straightforward posture controls. Protection that is complicated and hard to deploy can easily increase risk rather than reduce it.

Detection and response. The sooner you stop an attack, the better. Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypt your data will considerably improve your outcomes.

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. Regularly practice restoring data from backups to ensure speed and fluency should you need to execute in the aftermath of an attack.

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

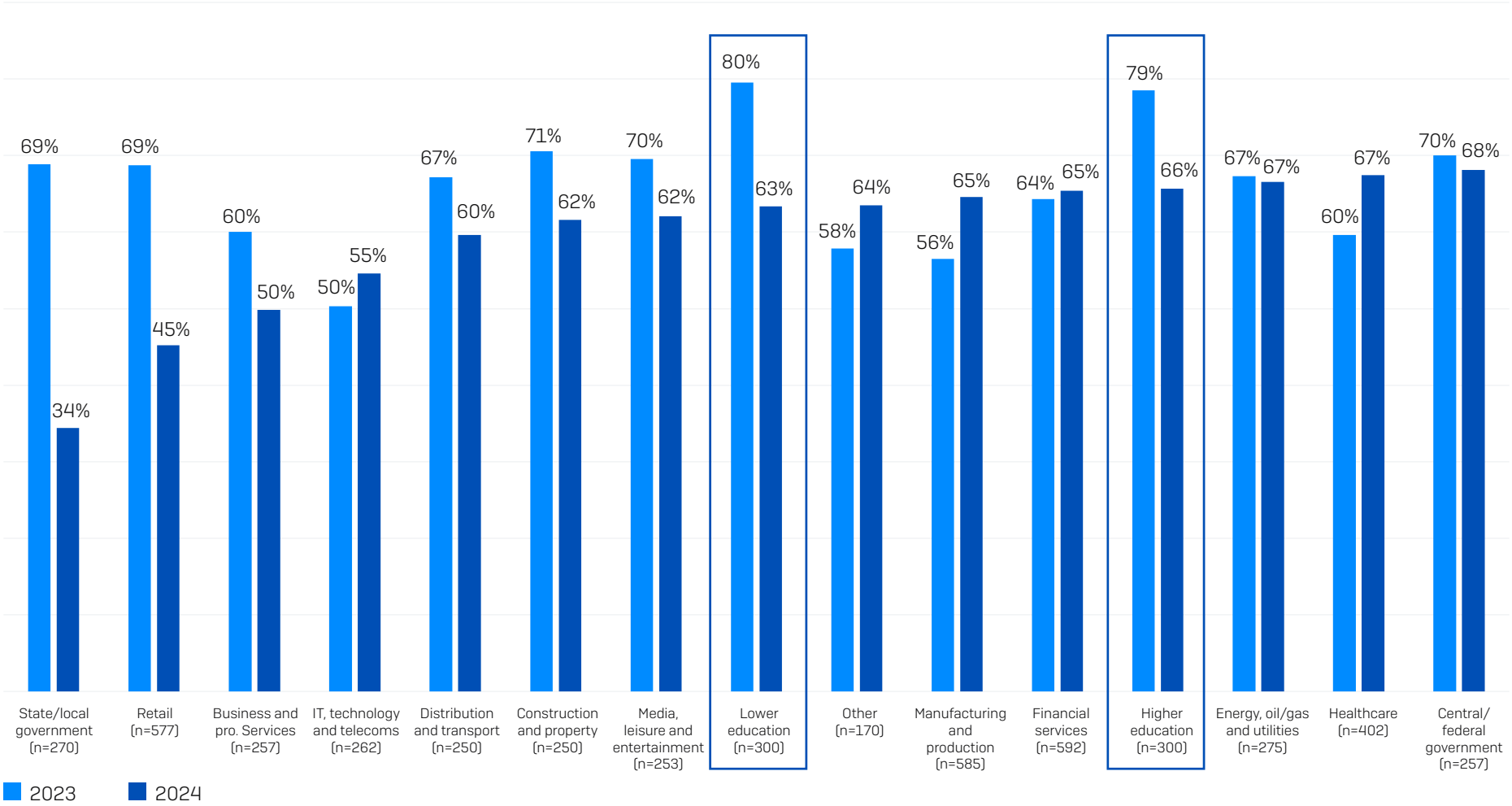
About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions in all business sectors and all major markets. For more information, visit www.vansonbourne.com

Appendix

Rate of Ransomware Attacks by Industry

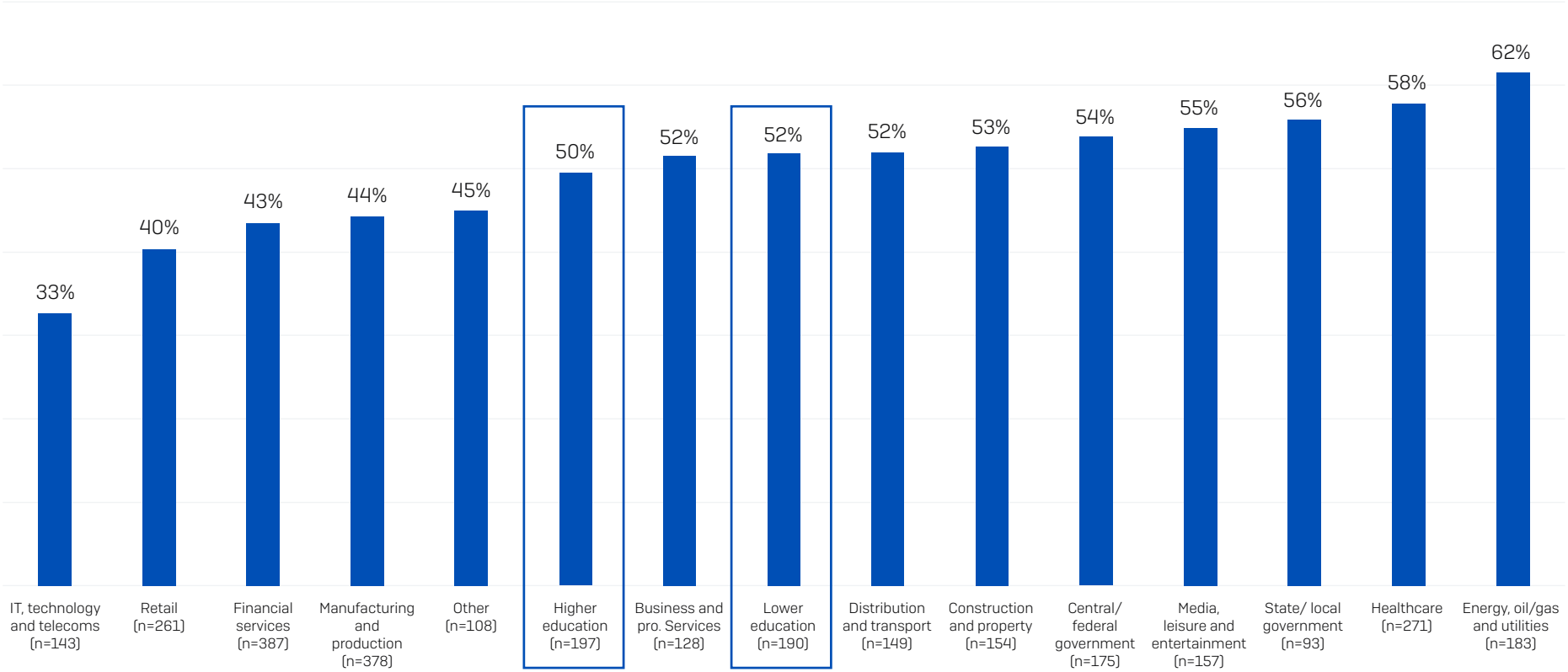
Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2024) n=3,000 (2023). 2024 industry base numbers in chart.

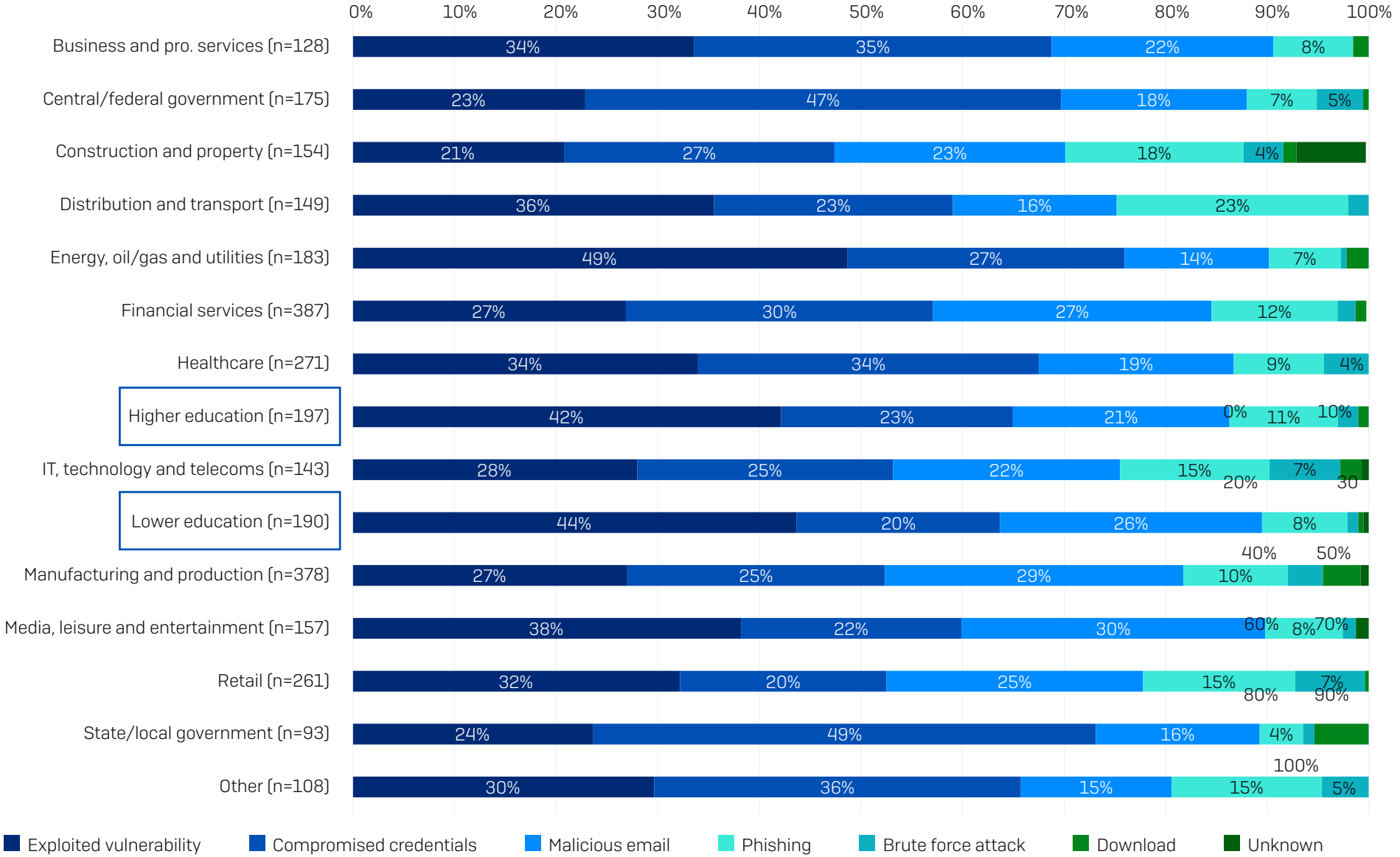
Percentage of Computers Impacted by Industry

Percentage of devices impacted



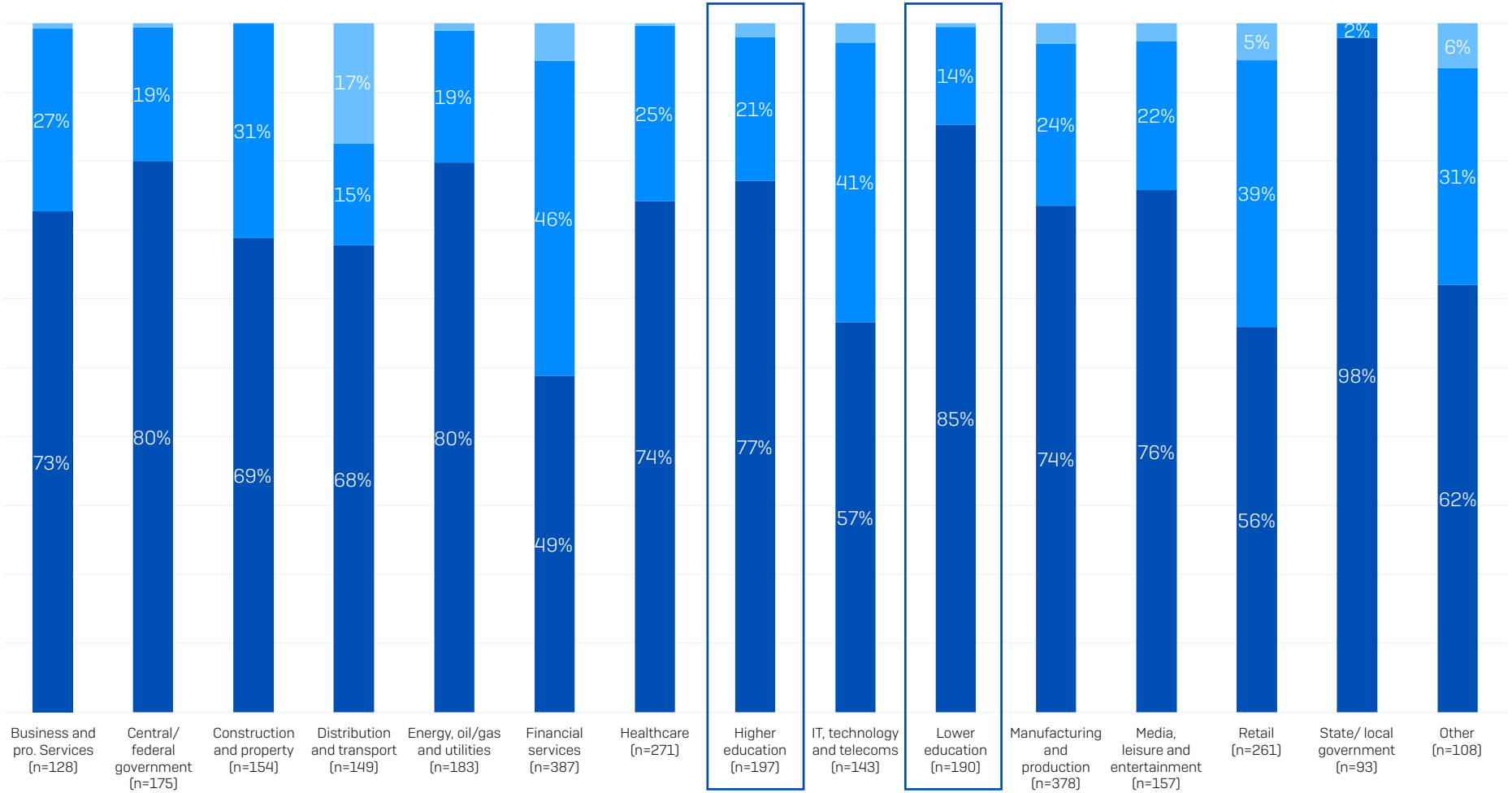
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

Root Cause of Attack by Industry



Do you know the root cause of the ransomware attack your organization experienced in the last year? n=2,974 organizations hit by ransomware.

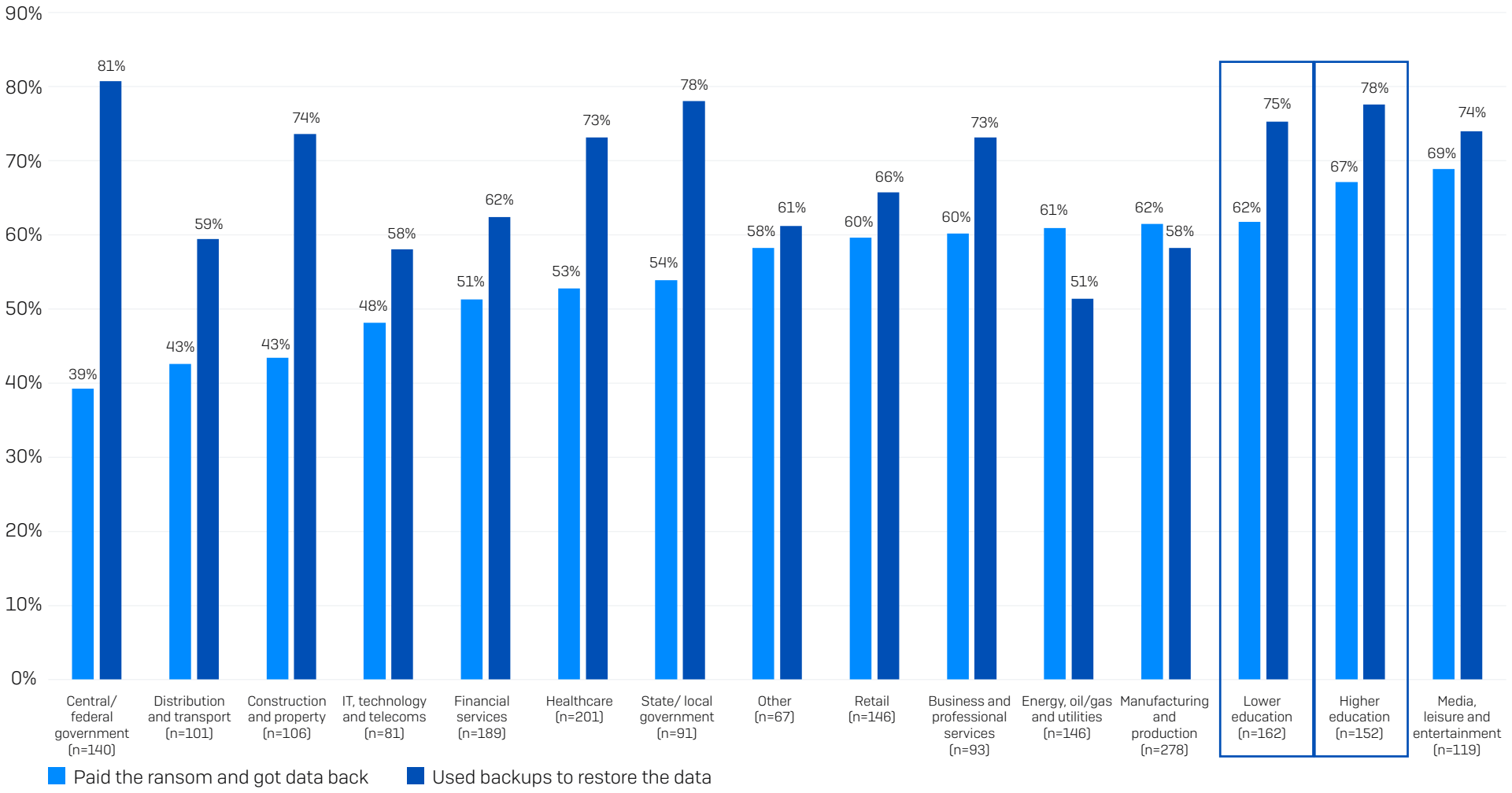
Data Encryption Rate by Industry



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

Data Recovery Method by Industry

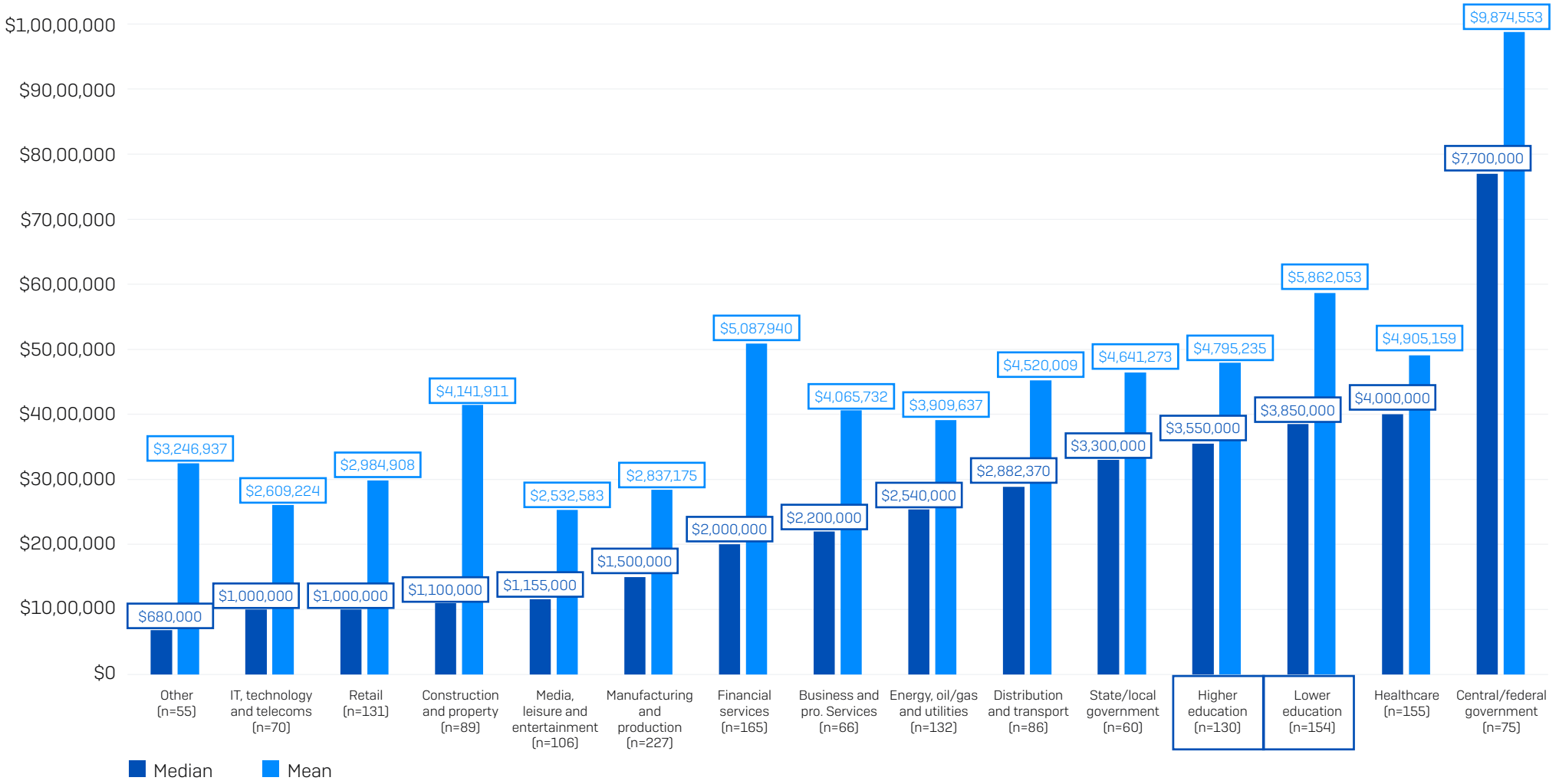
Percentage that got encrypted data back that used the recovery method



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. Ordered by propensity to pay the ransom.

Ransom Demand by Industry

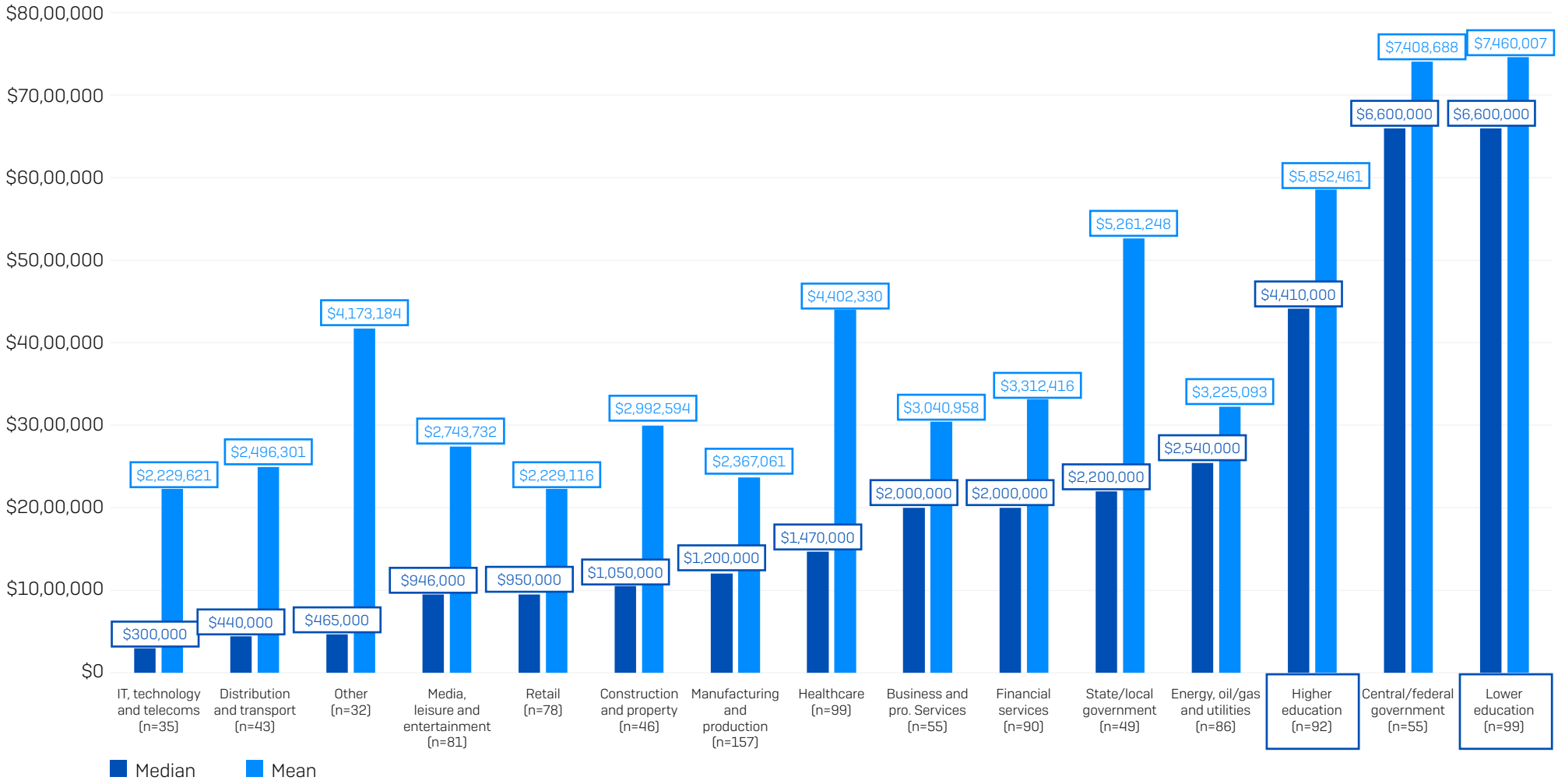
Ransom demand



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

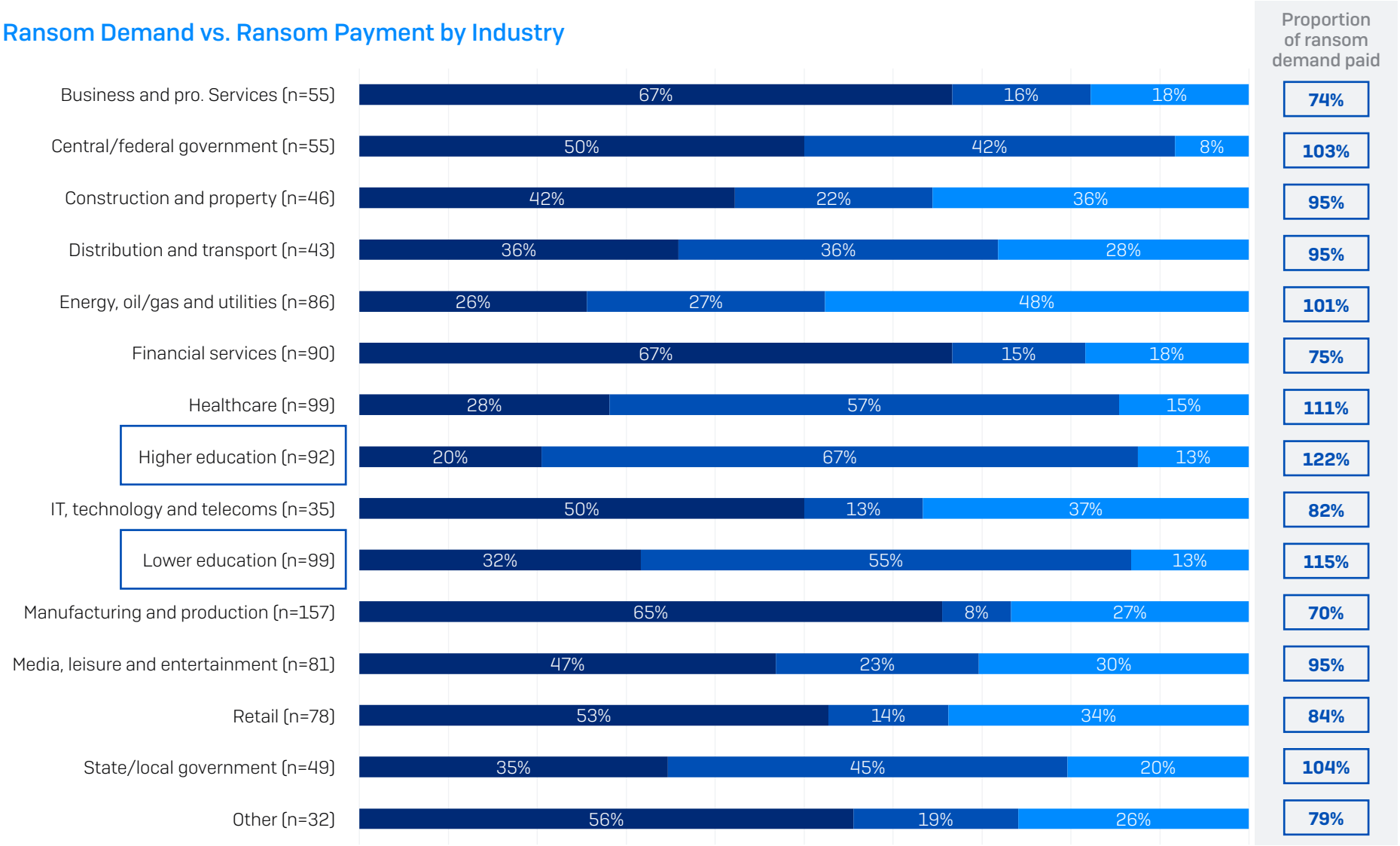
Ransom Payment by Industry

Ransom payment



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

Ransom Demand vs. Ransom Payment by Industry



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

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.

2024-07-11 WP-EN (PS)

SOPHOS