SOPHOS

The State of Ransomware in Education 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 400 from the education sector, conducted in January-March 2023.

A Sophos Whitepaper. July 2023

Introduction

Sophos' annual study of the real-world ransomware experiences of IT/cybersecurity leaders makes clear the realities facing educational organizations in 2023. It reveals the most common root causes of attacks and shines new light on how ransomware impacts the education sector. The report also reveals the business and operational impact of paying the ransom to recover data rather than using backups.

About the Survey

Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in organizations with between 100 and 5,000 employees across 14 countries in the Americas, EMEA, and Asia Pacific. The survey included 400 education respondents: 200 from lower education (up to 18 years) and 200 from higher education (above 18 years) and included both public and private sector education providers.

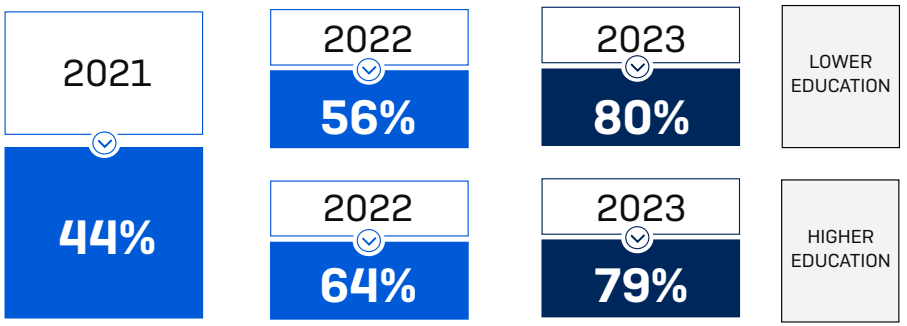
The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences over the previous year.

Rate of Ransomware Attacks in Education

The 2023 study revealed that the rate of ransomware attacks in education continues to rise. 80% of lower education providers and 79% of higher education providers reported that they were hit by ransomware in the last year, up from 56% and 64%, respectively, in our 2022 survey.

The 2023 rates of attacks are more than double than reported in our 2021 survey when 44% of education providers (combining lower and higher education) experienced a ransomware attack. This considerable increase in the attack rate makes clear that adversaries are now able to execute attacks at scale consistently, and ransomware is arguably the biggest cyber risk facing education providers today.

Cybercriminals have been developing and refining the ransomware-as-a-service model for several years. This operating model lowers the barrier to entry for would-be ransomware actors while also increasing attack sophistication by enabling adversaries to specialize in different stages of attacks. For more information on ransomware-as-a-service, read the Sophos 2023 Threat Report.



In the last year, has your organization been hit by ransomware? Yes. n=400 (2023), 440 (2022), 499 (2021)

This year the education sector reported the highest rates of ransomware attacks of all industries surveyed, suggesting that the sector is particularly exposed to attacks. IT, technology, and telecoms reported the lowest attack level (50%), indicating increased cyber readiness and defenses.

The rising rate of ransomware attacks in education is in contrast to the global cross-sector trend, which has remained flat: in both our 2023 and 2022 surveys, 66% of all respondents reported that their organization had been hit by ransomware in the previous year.

Root Causes of Ransomware Attacks in Education

Lower education reported compromised credentials (36%) and exploited vulnerabilities (29%) as the top two root causes of ransomware attacks. Emails (malicious emails or phishing) were the starting points for nearly one-third of the attacks (30%), suggesting that the lower education sector is highly exposed to email-based threats.

In higher education, exploited vulnerabilities (40%) were the most common root cause of ransomware attacks, with compromised credentials falling in second place at 37%. Together, they account for over three-quarters of ransomware attacks (77%) in higher education. Email-based attacks (malicious email or phishing) are a less common root cause but still drive almost one in five ransomware incidents (19%).

Across the full survey cohort, higher education was one of the sectors most likely to report exploited vulnerabilities as the root cause of attacks. At the same time, lower education was one of the sectors most likely to have attacks originating from compromised credentials.

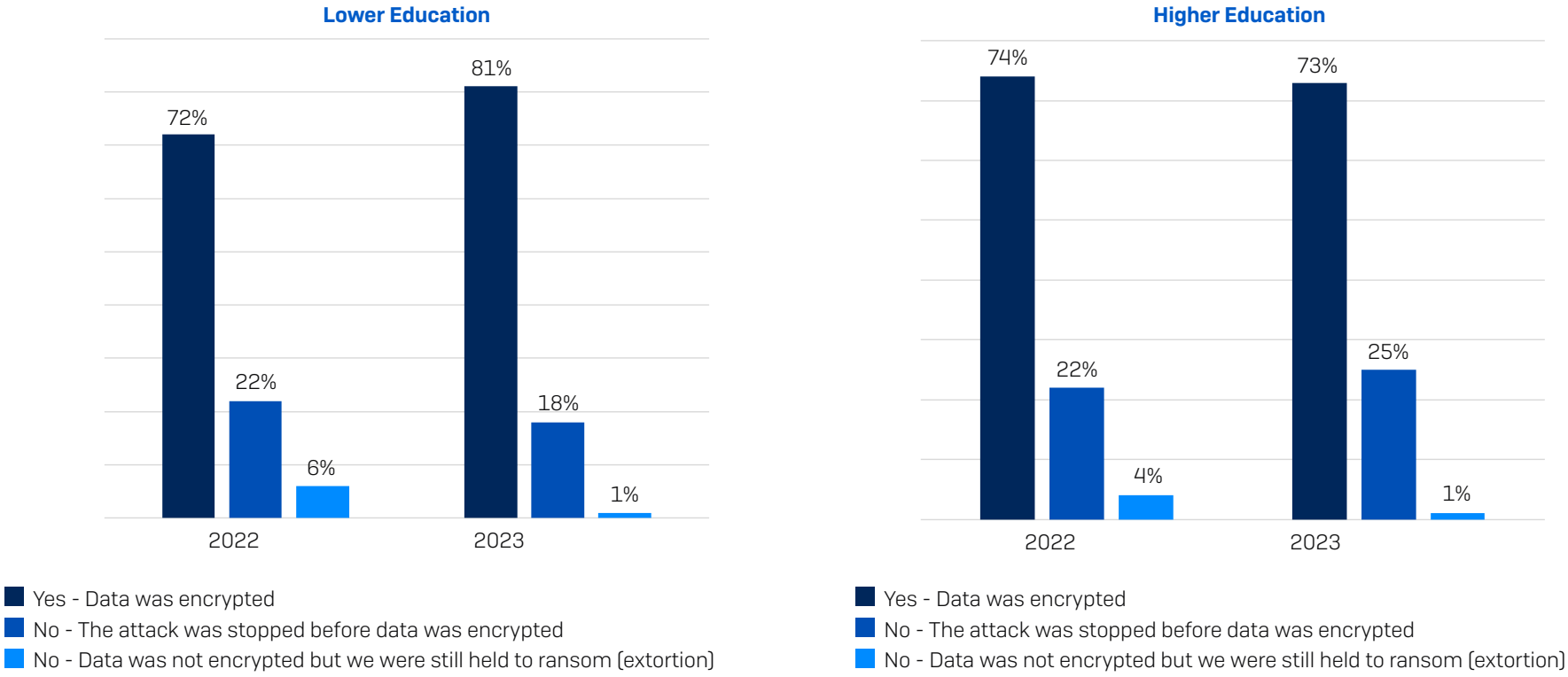
	LOWER EDUCATION (n=159)	HIGHER EDUCATION (n=157)	CROSS-SECTOR AVERAGE (n=1,974)
Exploited vulnerability	29%	40%	36%
Compromised credentials	36%	37%	29%
Malicious email	19%	12%	18%
Phishing	11%	7%	13%
Brute force attack	4%	2%	3%
Download	1%	1%	1%

Rate of Data Encryption in Education

Data encryption in the education sector has continued to rise: the percentage of attacks that resulted in data being encrypted in lower education organizations has gone up from 72% in 2022 to 81% in the 2023 survey. In higher education, the data encryption rate reported in the 2023 survey is 73%, similar to the 74% reported last year. This high encryption rate likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

18% of attacks in lower education were stopped before the data was encrypted, down from 22% in 2022. However, higher education reported an increase in the rate of attacks stopped before data encryption, up from 22% in 2022 to 25% in 2023. The rate of extortion-only attacks in lower and higher education organizations combined dropped from 5% in the last survey to 1% in this year's survey.

Across all sectors, 76% of attacks resulted in data encryption, and 21% were stopped before data was encrypted. The highest frequency of data encryption (92%) was reported by business and professional services.



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Selection of answer options. Lower education n= 159 (2023), 179 (2022), Higher education n=157 (2023), 261 (2022)

Of the lower education organizations that had data encrypted, 27% said their data was also stolen. This figure rises to 35% in higher education. This "double dip" approach by adversaries is becoming more commonplace as they look to increase their ability to monetize attacks. The threat of making stolen data public can be used to extort payments, and the data can also be sold. The high frequency of data theft increases the importance of stopping attacks as early as possible before information can be exfiltrated.

Percentage of ransomware attacks where data was encrypted that also had data stolen

Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes/Yes, and the data was also stolen n=128 (lower ed), 115 (higher ed)

Data Recovery Rate in Education

It is encouraging to note that all higher education and 99% of lower education organizations that had data encrypted were able to get data back, above the cross-sector average of 97%.

In lower education, 73% used backups for data recovery, while almost half (47%) paid the ransom. These figures represent a small but worrying change from our 2022 study, when 76% used backups and 45% paid the ransom.

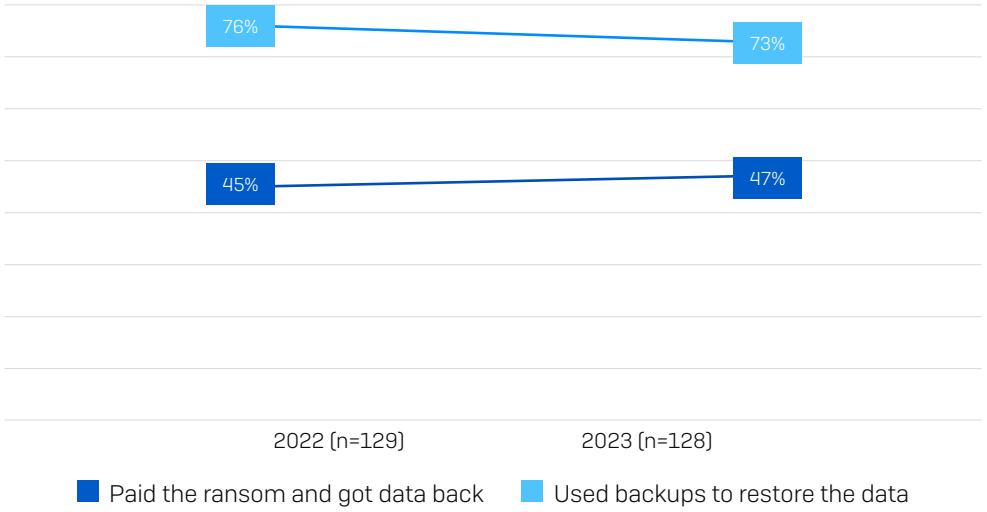
Higher education was among the bottom three sectors globally for backup use, with only two-thirds (63%) reporting the use of backups for data recovery. Only media, leisure and entertainment, and distribution and transport reported lower backup rates. The sector also reported one of the highest rates of ransom payments for data recovery, with 56% paying up to get data back.

	LOWER EDUCATION	HIGHER EDUCATION	CROSS-SECTOR AVERAGE
Got data back	99%	100%	97%
Used backups to restore data	73%	63%	70%
Paid the ransom to get data back	47%	56%	46%
Used other means to get data back	2%	3%	2%

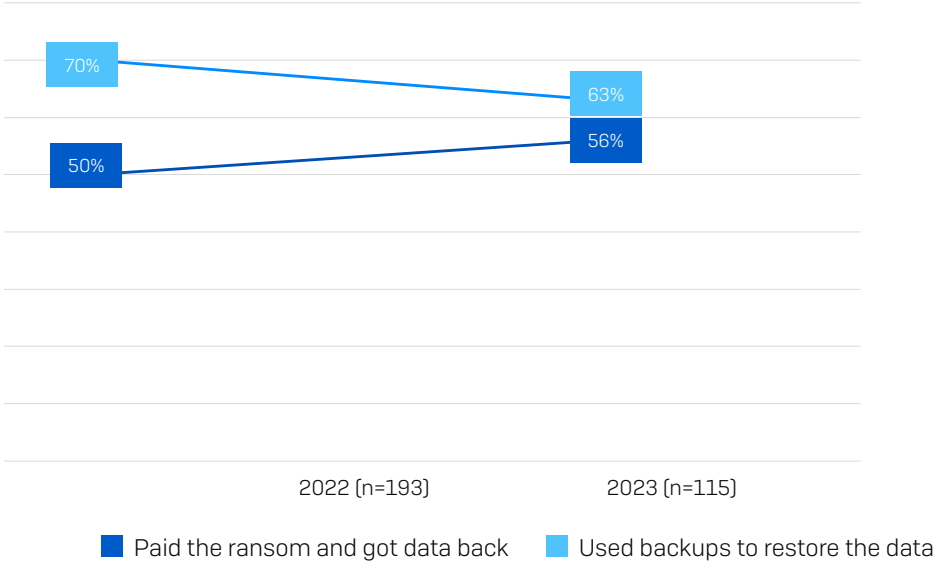
Paying the ransom and using backups were not mutually exclusive, and almost a quarter of education sector respondents (lower education: 23%; higher education: 22%) reported using multiple means to recover encrypted data.

Globally, the rate of ransom payments remained flat year on year, coming in again at 46%, while the use of backups dropped from 73% in our 2022 study to 70% in the 2023 report.

Ransom Payment and Backup Use for Data Recovery: Lower Education



Ransom Payment and Backup Use for Data Recovery: Higher Education



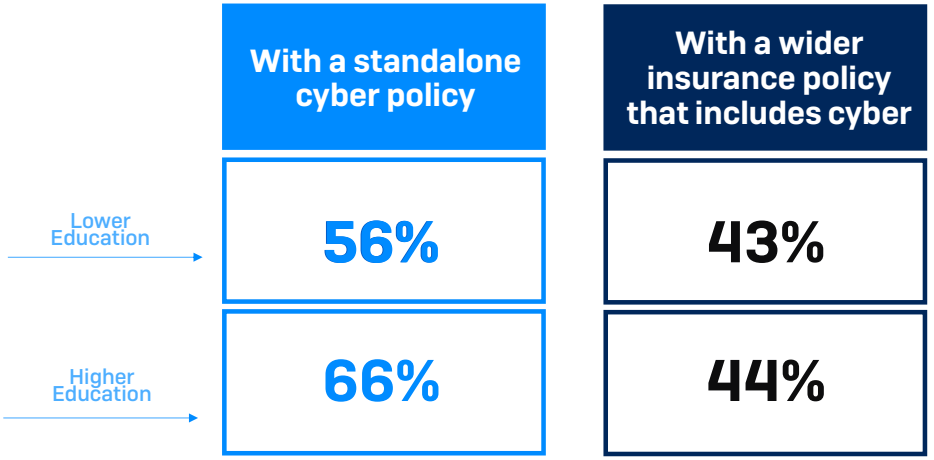
Did your organization get any data back? Yes, we paid the ransom and got data back, Yes, we used backups to restore the data. Base numbers in chart

The Impact of Insurance on Data Recovery

While the overall rate of data recovery was 99% in lower education and 100% in higher education, the methods used to recover data varied according to insurance coverage. Organizations with standalone policies reported a higher propensity to pay the ransom than those with cyber as part of broader insurance coverage.

Of those that had data encrypted and had a standalone cyber insurance policy, 56% in lower education and 66% in higher education paid the ransom. In contrast, the ransom payment rate was 43% (lower education) and 44% (higher education) for those with broader insurance policies that included cyber.

Percentage of ransomware victims that paid the ransom

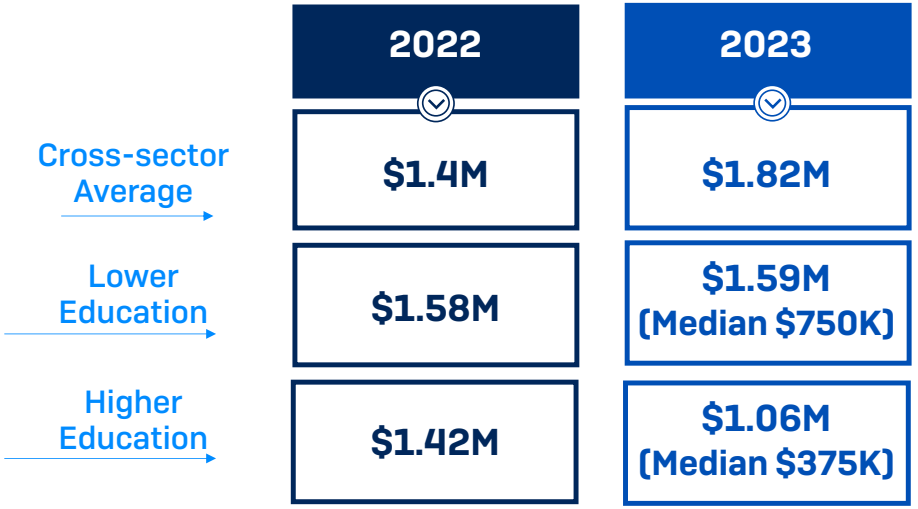


Did your organization get any data back? Yes, we paid the ransom and got data back. n=125 lower education organizations that were hit by ransomware in the last year and had data encrypted (50 standalone policy, 75 cyber as part of wider policy) n=114 higher education organizations that were hit by ransomware in the last year and had data encrypted (59 standalone policy, 55 cyber as part of wider policy)

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Across all sectors, excluding any ransoms paid, organizations reported an estimated mean cost to recover from ransomware attacks of $1.82 million, an increase from the $1.4 million reported in 2022 (which included ransom payments) and in line with the $1.85 million including ransom reported in 2021.

While the cross-sector recovery costs increased over the last year, in lower education, they have remained level ($1.59M in 2023 vs. $1.58M in 2022). The median recovery cost in lower education was $750K in 2023. In higher education, recovery costs have dropped considerably from the $1.42M reported last year to just over $1 million in 2023, and the median recovery cost is coming to $375K.



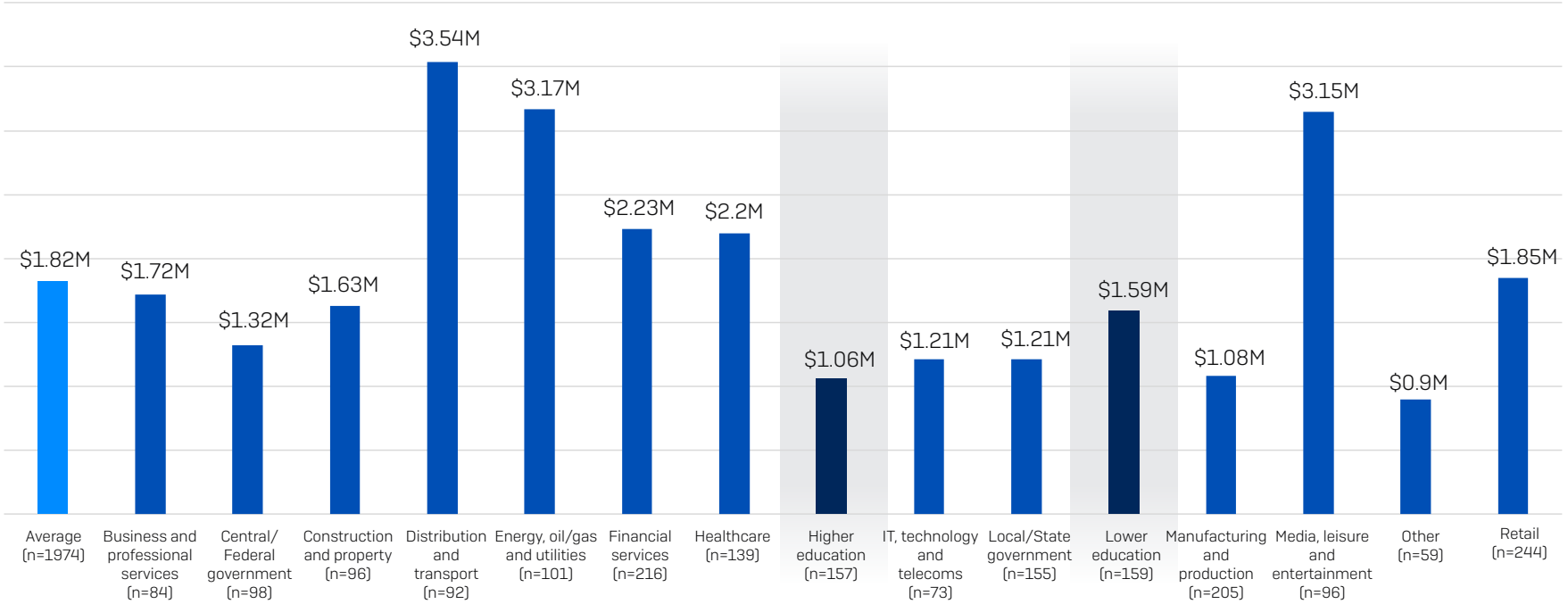
What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? Cross-sector: n=1,974 (2023)/ 3,702 (2022); Lower education: n=159 (2023)/ 179 (2022); Higher education: n= 157 (2023)/261 (2022)

N.B. 2022 question wording also included 'ransom payment'

This suggests that as ransomware rates increase, higher education organizations are getting better at recovering from an attack and are able to do so at a lower cost.

Recovery costs in education organizations were much below the cross-sector average of $1.82M. Distribution and transport paid the highest recovery cost ($3.54), almost double what most other organizations paid.

Recovery Cost After the Most Significant Ransomware Attack (in 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.)? Base numbers in chart.

Recovery Cost by Data Recovery Method

The research confirms that backups are a cheaper way to recover encrypted data than paying the ransom.

Across all sectors, the median recovery cost for those that used backups ($375,000) is half that of those that paid the ransom ($750,000). Similarly, the mean recovery cost is almost $1 million lower for those that used backups.

While lower education reported a mean recovery cost of $1.59M, for organizations that paid the ransom, it soared to $2.18M. Conversely, recovery costs dropped to $1.37 million for those that used backups.

In higher education, which had a mean $1.06M recovery cost, paying the ransom resulted in a recovery cost of $1.31M, while using backups brought the recovery cost average to just under $1M.

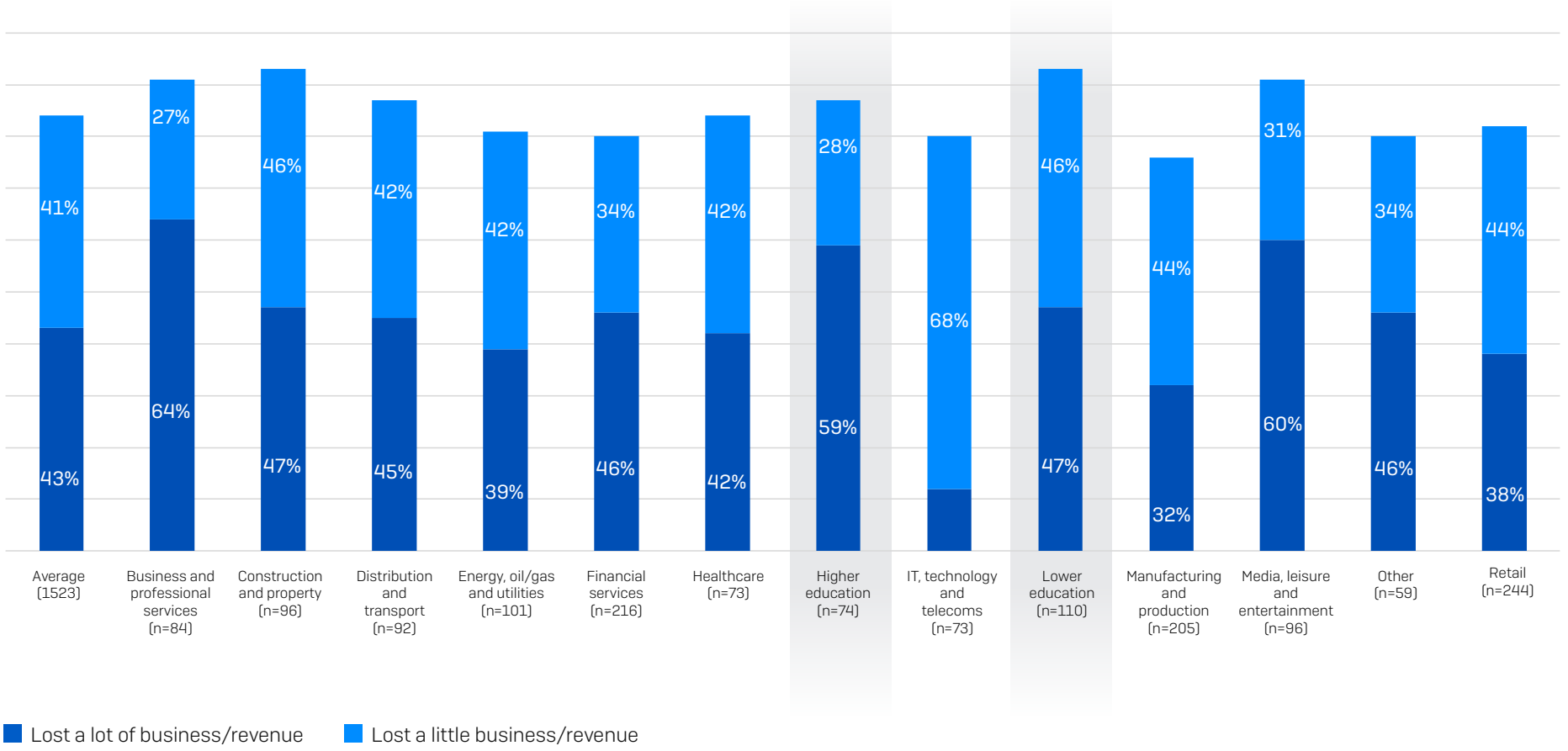
	Paid the ransom and got data back	Used backups to restore data
Cross-sector Average	**$2.6M**	**$1.62M**
Lower Education	**$2.18M**	**$1.37M**
Higher Education	**$1.31M**	**$0.98M**

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.)? Cross-sector: n=694 that paid the ransom and got data back and 1,053 that used backups to restore the data;
n=60 (ransom)/94 (backups) in lower ed and n=64 (ransom)/73 (backups) in higher ed

Business Impact

The education sector is particularly exposed to the impacts of ransomware, with private sector organizations reporting some of the highest levels of lost business/ revenue because of an attack. Overall, 59% of higher education organizations said they lost a lot of business/revenue, behind only business and professional services and media, leisure, and entertainment.

Similarly, although lower education was less likely to lose a lot of business/revenue, it is the industry that is most likely to have lost some business/revenue (94% - combined proportion of those losing either a little or a lot) due to the attack.



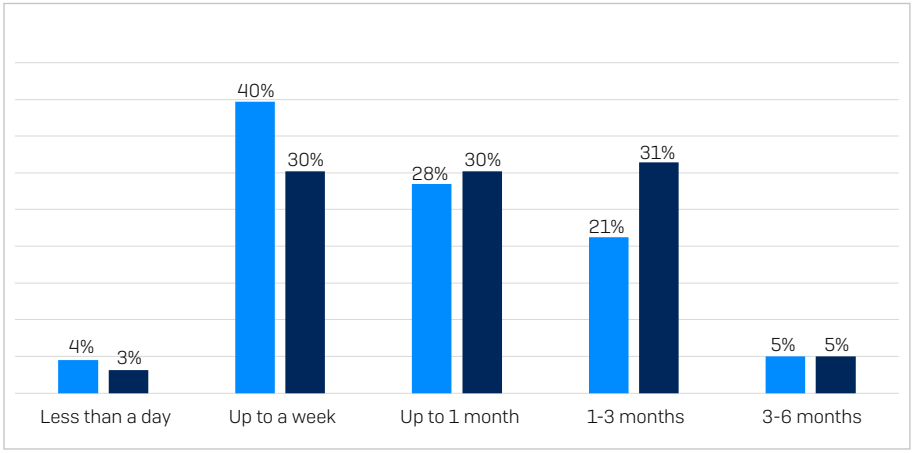
Did the ransomware attack cause your organization to lose business/revenue? Yes, we lost a lot of business/ revenue, Yes, we lost a little business/ revenue.
Private sector organizations that were hit by ransomware, base numbers in chart

Recovery Time

Lower education organizations have got a little slower at recovering from a ransomware attack, with 33% recovering within the week in this year's study compared to 44% last year. The percentage of organizations that took more than a month to recover increased to 36% (with rounding) from 26% (with rounding) year over year, reflecting the increased pressures and greater staffing shortages in the sector.

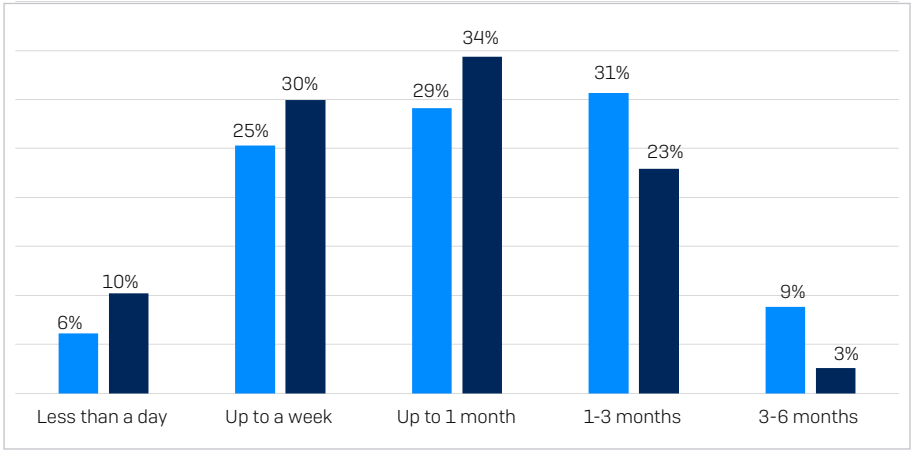
Conversely, higher education has got quicker at recovering, with 40% fully recovering within a week compared to 31% in last year's survey. Similarly, the percentage of organizations that took more than a month for recovery went down from 39% in the previous year to 25% in this year's survey.

Recovery Time in Lower Education: 2022 vs. 2023



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

Recovery Time in Higher Education: 2022 vs. 2023



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

Recovery time by data recovery method

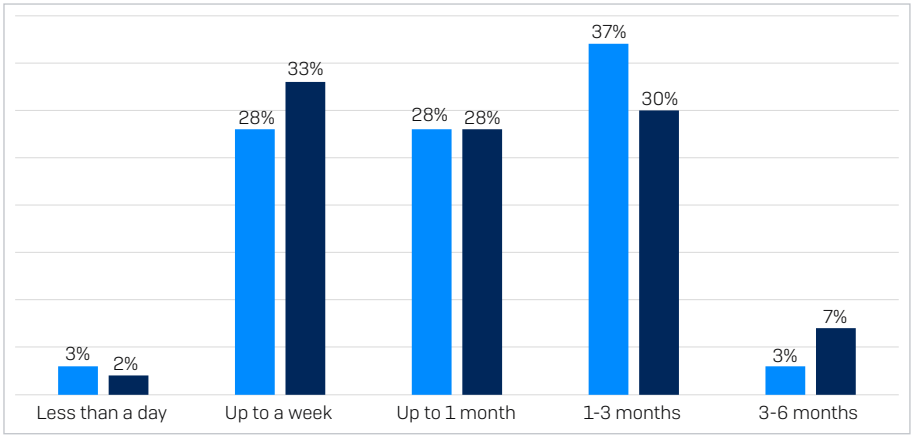
The research reveals that educational organizations that use backups to recover their data recover from attacks more quickly than those that pay the ransom.

Over one-third of lower education organizations that used backups (35%) recovered within a week, compared with 32% of those that paid the ransom.

While these two response options were not mutually exclusive, and some respondents will have both paid the ransom and used backups, the recovery advantages of backups are clear.

There is a similar pattern in higher education. 79% that used backups fully recovered within a month, compared to 63% that paid the ransom. 38% of organizations paying the ransom took over a month to recover compared to 21% who used backups and recovered in this time.

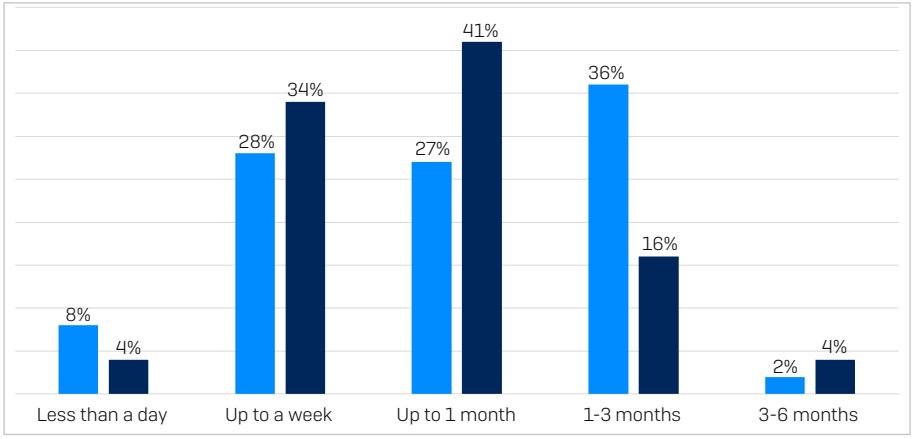
Recovery Time by Data Recovery Method in Lower Education



Paid the ransom and got data back (n=60)
Used backups to restore the data (n=94)

How long did it take your organization to fully recover from the ransomware attack? Organizations that paid the ransom and/or used backups to recover data. Base numbers in chart

Recovery Time by Data Recovery Method in Higher Education



Paid the ransom and got data back (n=64)
Used backups to restore the data (n=73)

How long did it take your organization to fully recover from the ransomware attack? Organizations that paid the ransom and/or used backups to recover data. Base numbers in chart

Conclusion

Ransomware remains a major threat, with the education sector reporting the highest attack rate across all industries in 2023. As adversaries continue to hone their attack tactics, techniques, and procedures (TTPs), defenders struggle to keep pace, resulting in increased encryption rates: over three-quarters of educational organizations (81% in lower education; 73% in higher education) hit by ransomware had their data encrypted. In addition, 27% in lower education and 35% in higher education reported that their encrypted data was also stolen.

Concerningly, the use of backups to recover encrypted data in education dropped in the last year, while the ransom payment rates increased year over year. In fact, higher education reported one of the highest uses of ransom payments for data recovery in the 2023 survey. The good news is that all (100%) higher education and 99% of lower education organizations that had data encrypted could recover data after the attack, above the cross-sector average of 97%.

The organization's insurance position had an impact on the method of data recovery in education. Educational providers with a standalone cyber insurance policy were more likely to pay the ransom to recover data than those with cyber as part of a broader business policy.

Education organizations were among those who spent the least to recover from an attack: lower education reported a mean recovery cost of $1.59M, and higher education reported a recovery cost of $1.06M, with both figures coming in well below the cross-sector average of $1.82M.

For education providers operating in the private sector, ransomware has a major business impact. 94% of lower education and 88% of higher education organizations hit by ransomware reported that they lost business/revenue as a result of the attacks.

With the growth of the ransomware-as-a-service business model, Sophos does not anticipate a drop in attacks in the coming year.

Organizations should focus on:

1. Further strengthening their defensive shields with:

   - Security tools that defend against the most common attack vectors, including endpoint protection with strong anti-exploit capabilities to prevent exploitation of vulnerabilities and zero trust network access (ZTNA) to thwart the abuse of compromised credentials.
   - Adaptive technologies that respond automatically to attacks disrupting adversaries and buying defenders time to respond.
   - 24/7 threat detection, investigation, and response, whether delivered in-house or in partnership with a specialist Managed Detection and Response (MDR) service provider.

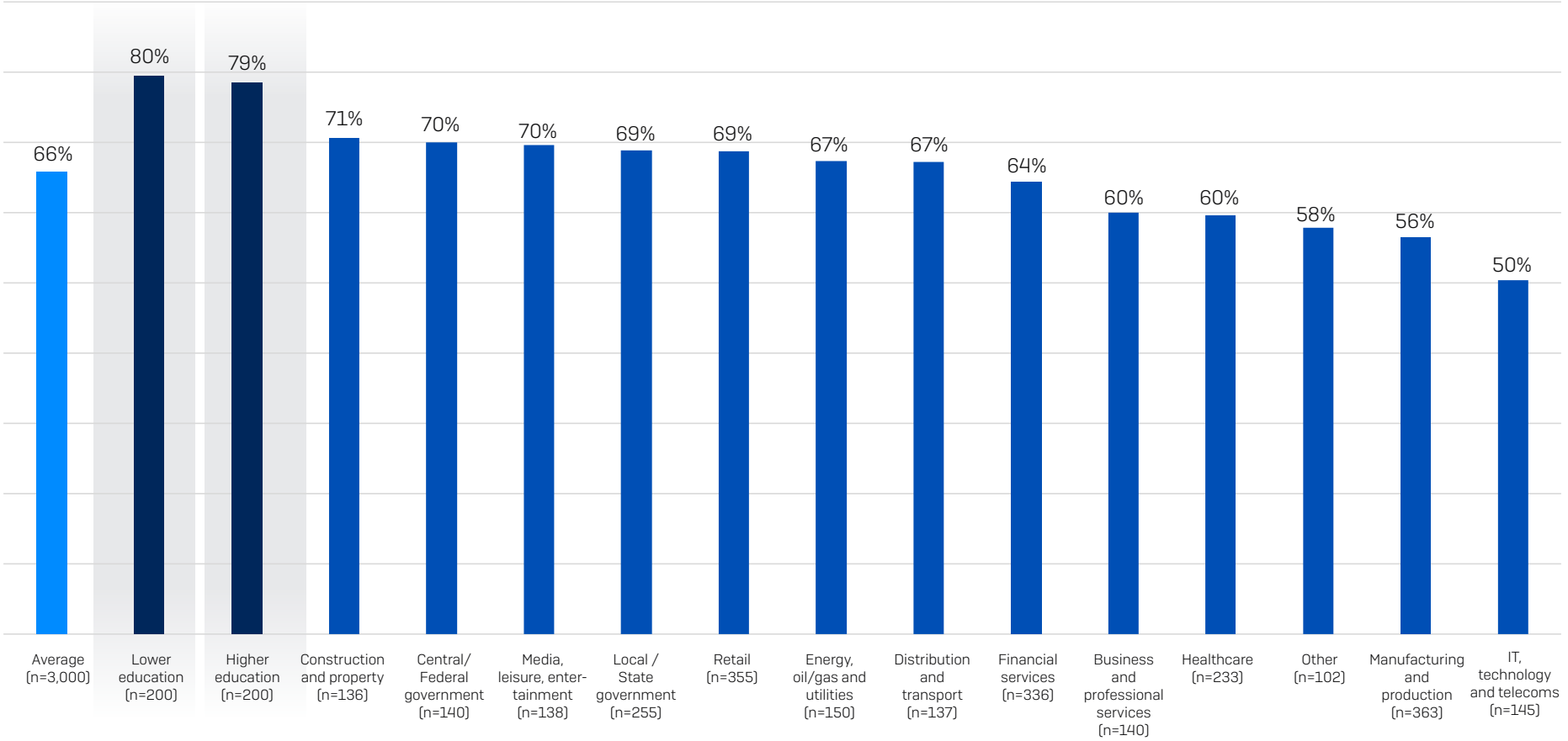
2. Optimizing attack preparation, including making regular backups, practicing recovering data from backups, and maintaining an up-to-date incident response plan

3. Maintaining good security hygiene, including timely patching, and regularly reviewing security tool configurations

Additional Charts

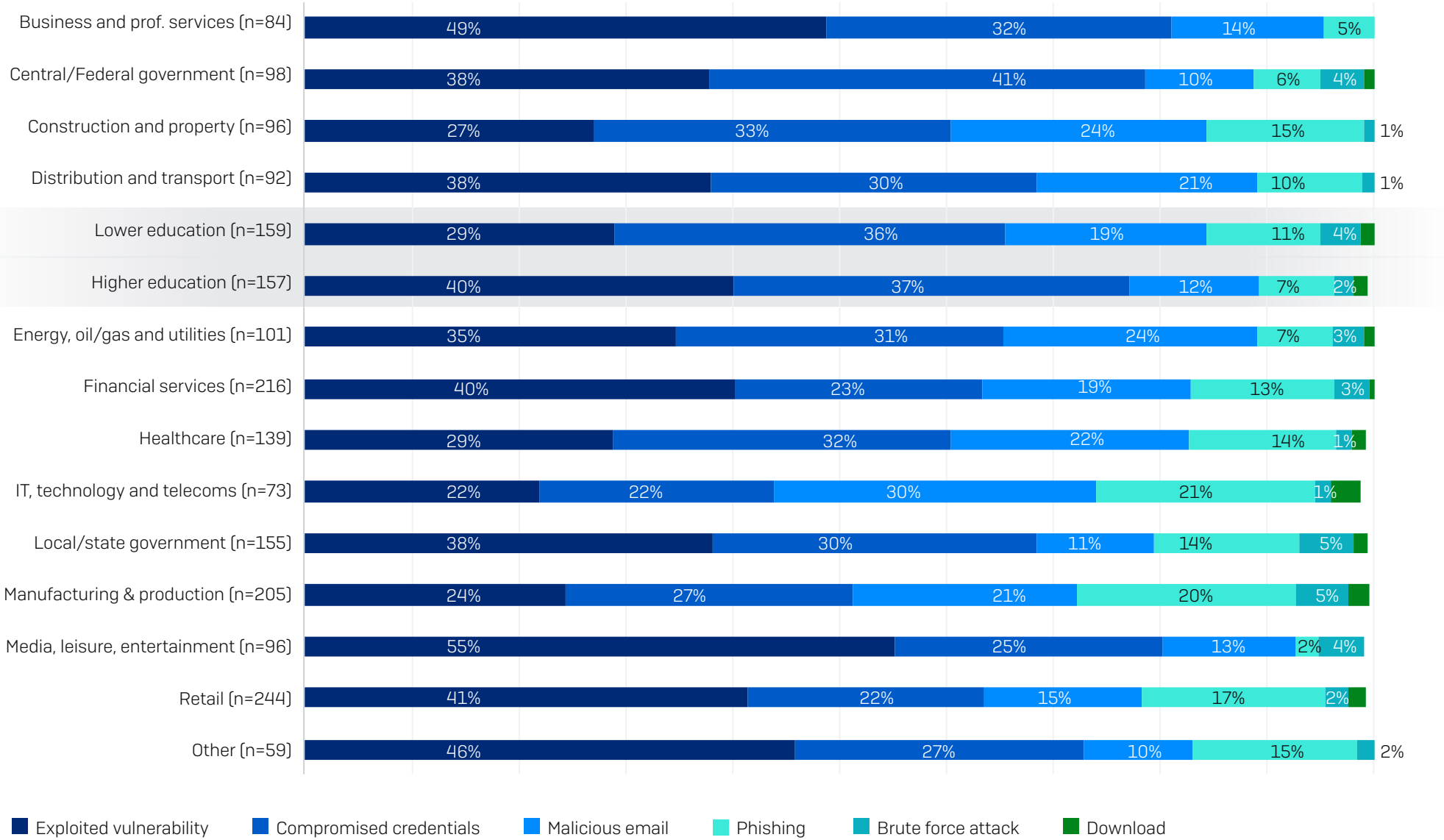
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



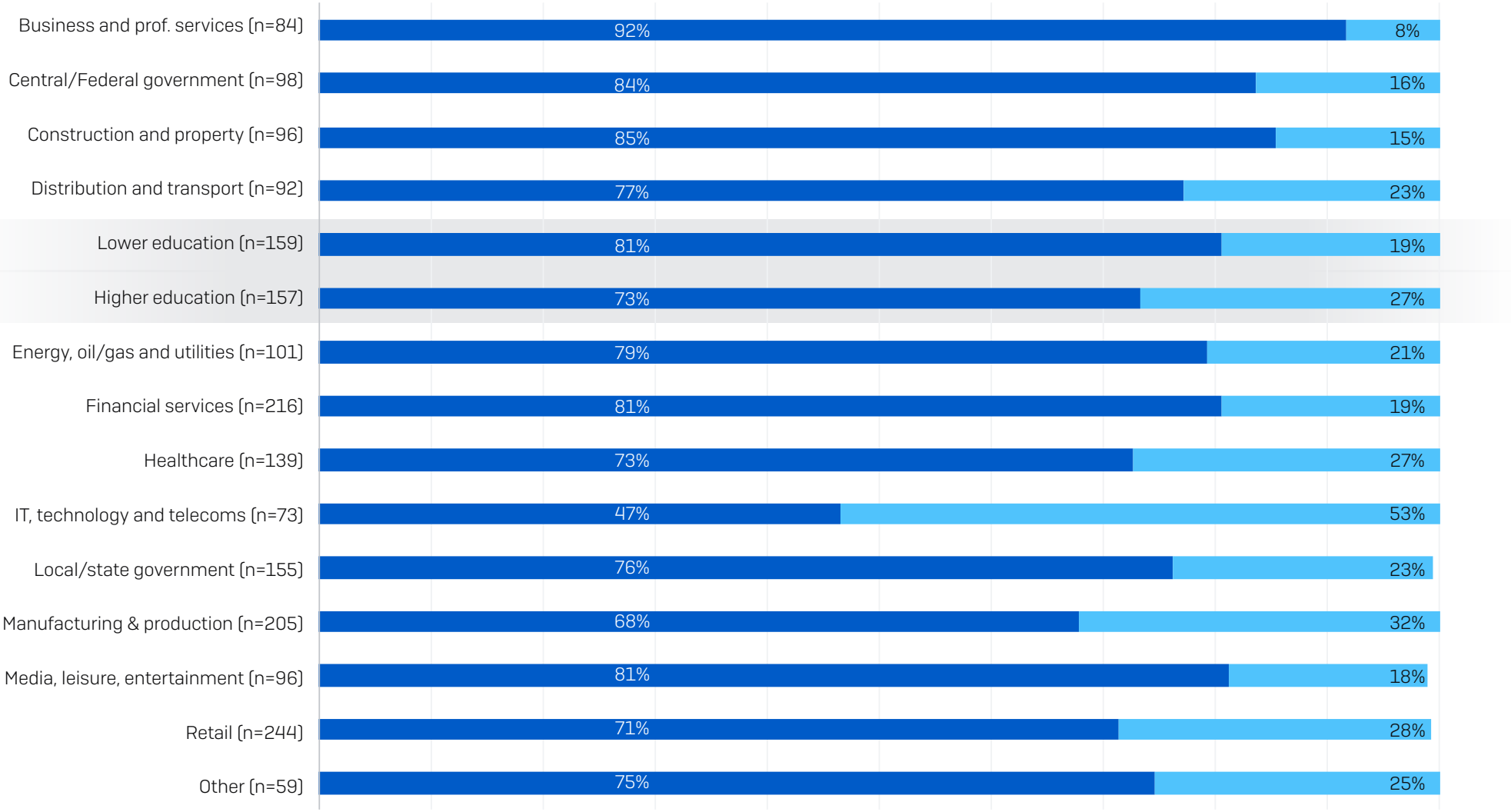
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



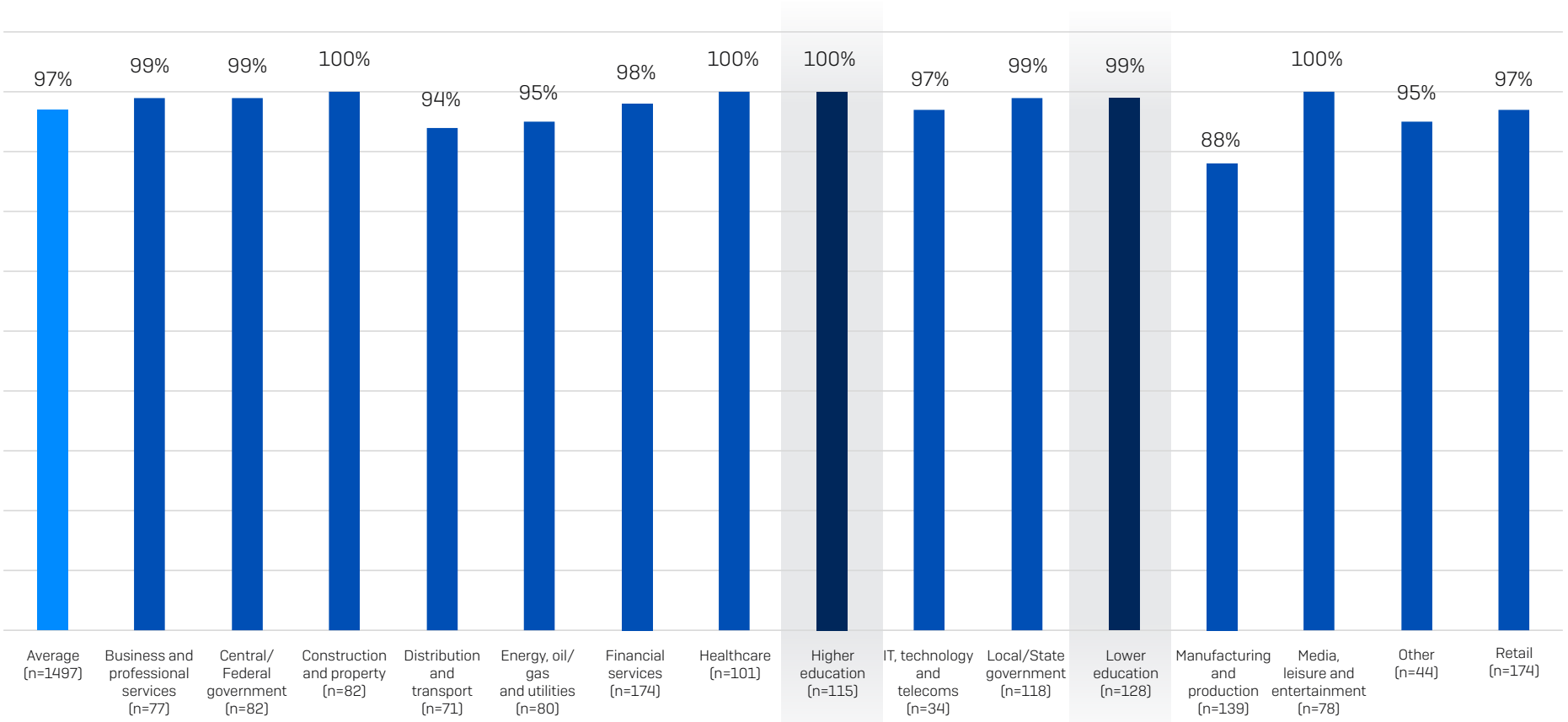
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



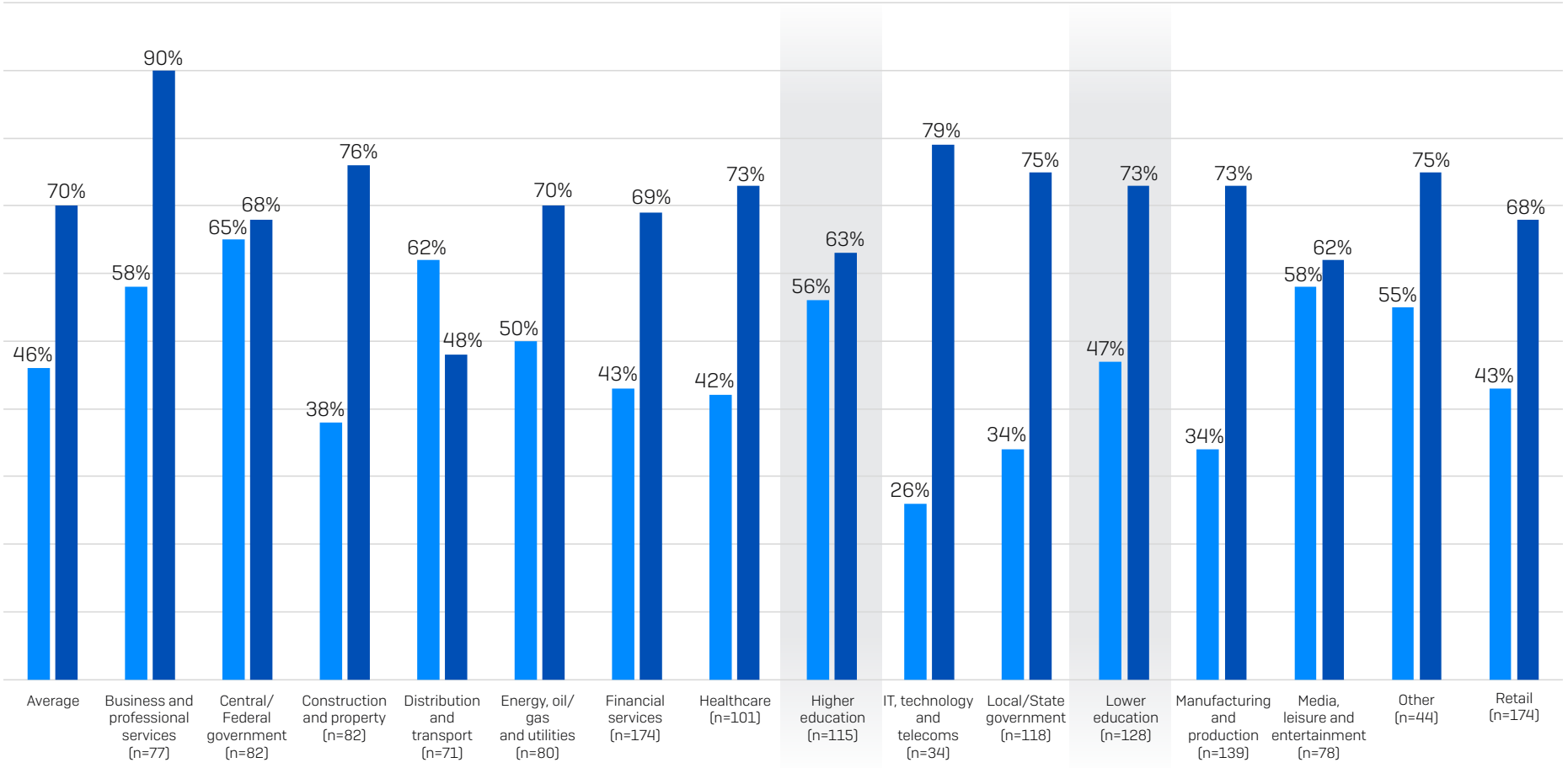
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

Data Recovery Rate



Did your organization get any data back? n=1,497 organizations that were hit by ransomware and had data encrypted

Ransom Payment and Backup Use for Data Recovery



Did your organization get any data back? n=1,497 organizations that were hit by ransomware and had data encrypted

Research Methodology

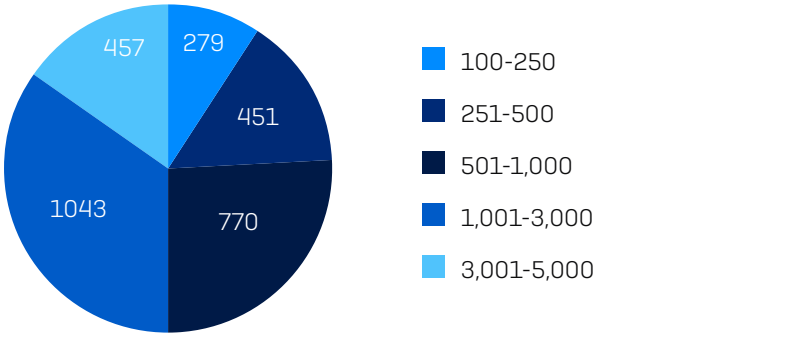
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

All respondents were from organizations with between 100 and 5,000 employees (50% 100-1,000 employees, 50% 1,001-5,000 employees). Within the research cohort, annual revenue ranged from less than $10 million to more than $5 billion.

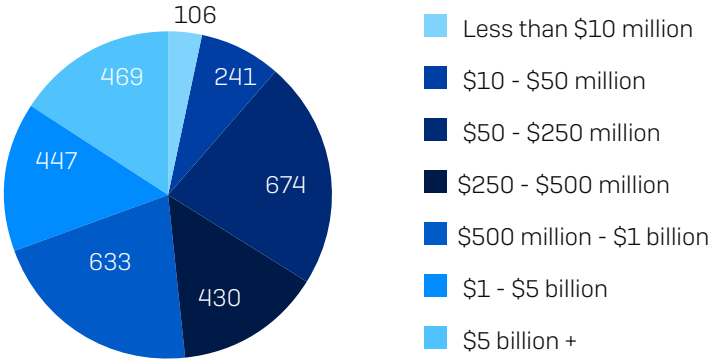
Respondents by Country

COUNTRY	NUMBER OF RESPONDENTS	COUNTRY	NUMBER OF RESPONDENTS
United States	500	United Kingdom	200
Germany	300	South Africa	200
India	300	France	150
Japan	300	Spain	150
Australia	200	Austria	100
Brazil	200	Singapore	100
Italy	200	Switzerland	100

Respondents by Organization Size (number of employees)



Respondents by Organization Size (annual revenue)



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.

2023-07-14 (WP-PS)

SOPHOS