SOPHOS

The State of Ransomware in Healthcare 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 233 from the healthcare sector, conducted in January-March 2023.

A Sophos Whitepaper. August 2023

Introduction

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

About the Survey

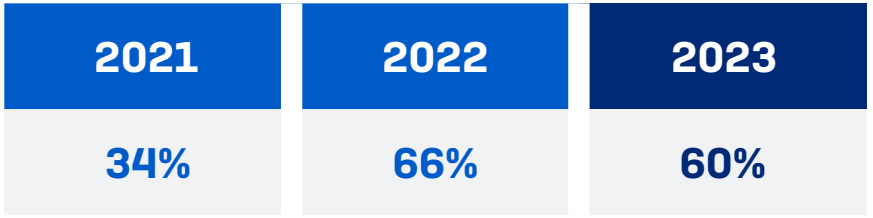
Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in organizations with between 100 and 5,000 employees, including 233 in healthcare organizations, across 14 countries in the Americas, EMEA, and Asia Pacific. The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences over the previous year.

Rate of Ransomware Attacks in Healthcare

Our 2023 study reveals that the rate of ransomware attacks in healthcare has decreased from 66% to 60% year over year. Despite the downward trend, the 2023 report's rate of attacks is almost double the rate reported in the 2021 survey, when 34% of healthcare organizations reported being hit by ransomware.

Although the sector observed a reduced frequency of attacks, with almost two-thirds of healthcare organizations hit by ransomware in the last year, it is clear that adversaries are able to execute attacks at scale consistently, and ransomware is arguably the biggest cyber risk facing the healthcare sector 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=233 (2023), 381 (2022), 328 (2021)

In contrast with the decrease in the rate of ransomware attacks in the healthcare sector, the global cross-sector trend remains flat: in both our 2023 and 2022 surveys, 66% of all respondents reported that their organizations had been hit by ransomware in the previous year.

Across all sectors, education was most likely to be hit, with 80% in lower education and 79% in higher education reporting an attack. IT, technology, and telecoms reported the lowest attack level (50%), indicating increased cyber readiness and defenses.

Root Causes of Ransomware Attacks in Healthcare

Compromised credentials (32%) were the most common root cause of the most significant ransomware attacks in the healthcare sector, followed by exploited vulnerabilities (29%). Email-based attacks (malicious emails or phishing) were the starting points for over a third of attacks (36%) in healthcare organizations, higher than the cross-sector average of 30%.

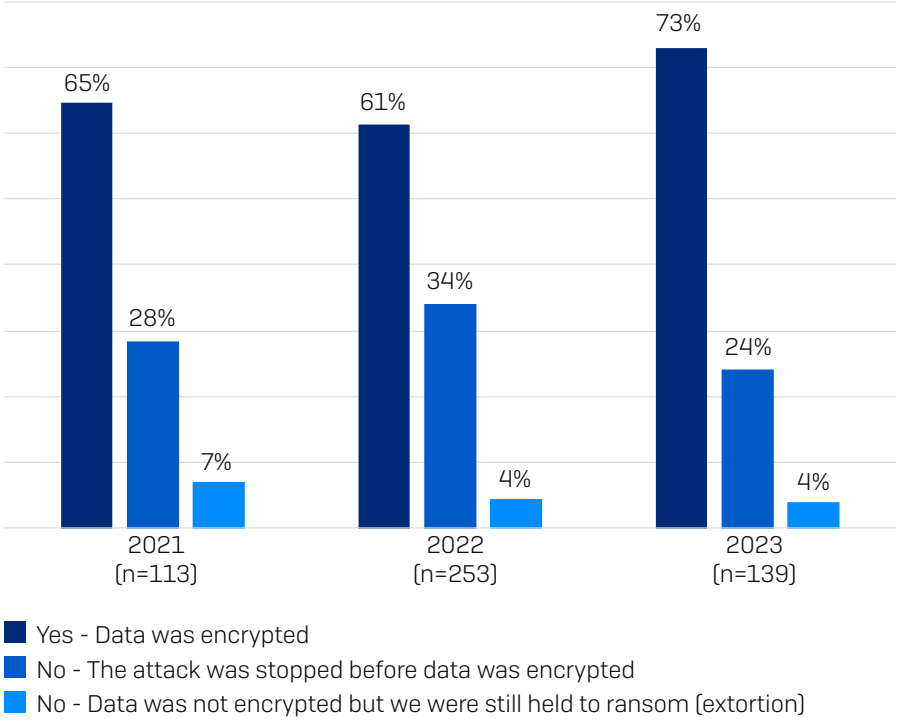
At a global, cross-sector level, the order of the top two root causes is switched, with exploited vulnerabilities the most common root cause (used in 36% of attacks), followed by compromised credentials (behind 29% of attacks).

	HEALTHCARE (n=139)	CROSS-SECTOR AVERAGE (n=1,974)
Exploited vulnerability	29%	36%
Compromised credentials	32%	29%
Malicious email	22%	18%
Phishing	14%	13%
Brute force attack	1%	3%
Download	1%	1%

Rate of Data Encryption in Healthcare

The rate of data encryption in the healthcare sector was the highest in the last three years of reports, with almost three-quarters of healthcare organizations (73%) reporting that their data was encrypted, up from 61% in the 2022 report and 65% in the 2021 report. This likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

The rate of extortion-only attacks in healthcare remained flat at 4%, below the 7% reported in our 2021 study.



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

While high, the rate of data encryption reported by healthcare is below the cross-sector average, where 76% of attacks resulted in data encryption. The highest frequency of data encryption (92%) was reported by business and professional services.

In more than one-third of the attacks in healthcare (37%) where data was encrypted, the data was also stolen. 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.

37%
of ransomware attacks on healthcare where data was encrypted also resulted in data being stolen.

Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack?
Yes/Yes, and the data was also stolen; n=101/37

Data Recovery Rate in Healthcare

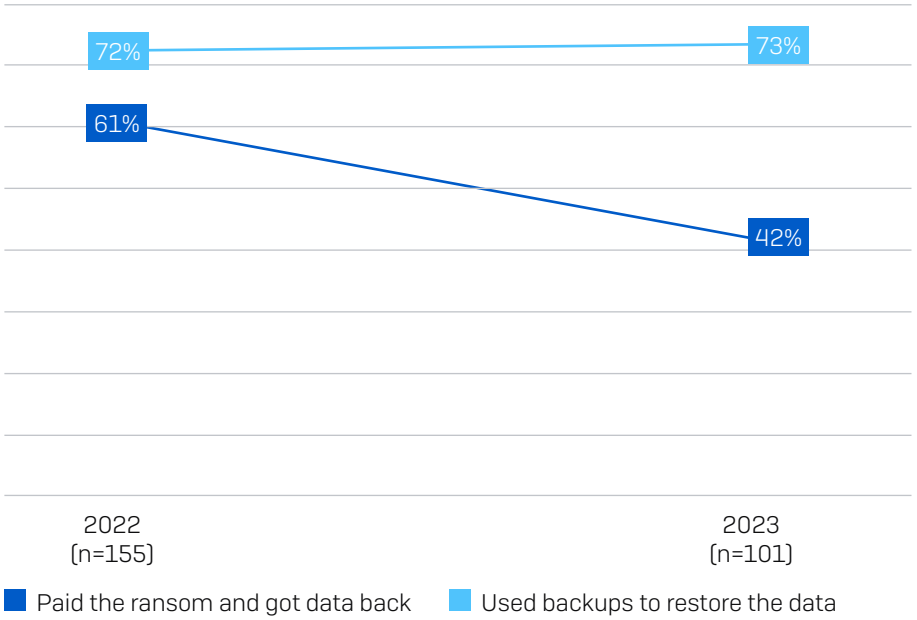
The good news is that all healthcare organizations that had data encrypted got data back, above the cross-sector average of 97%.

73% of healthcare organizations that had data encrypted used backups to recover data, very slightly up from the 72% reported in our 2022 survey. What is encouraging to note is the drop in propensity to pay the ransom to recover encrypted data: 42% of healthcare respondents reported that they paid the ransom to recover data, down from 61% in last year's report. 17% of respondents reported using multiple means to recover encrypted data.

	HEALTHCARE	CROSS-SECTOR AVERAGE
Got data back	**100%**	**97%**
Used backups to restore data	**73%**	**70%**
Paid the ransom to get data back	**42%**	**46%**
Used other means to get data back	**2%**	**2%**

Did your organization get any data back? Yes, we used backups to restore the data; Yes, we paid the ransom and got data back; Yes, we used other means to get our data back. n=1,497 (cross-sector); n=101 (healthcare).

The rate of ransom payments in healthcare was not only significantly lower than the year before, it was also below the cross-sector average of 46%. Globally, the rate of ransom payments remained flat year over year, while the use of backups dropped from 73% in our 2022 study to 70% in the 2023 report.



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 Propensity to Pay Ransom

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

More than half of healthcare organizations (53%) that had data encrypted and had a standalone cyber insurance policy paid the ransom. This dropped to 34% for organizations with broader insurance policies that included cyber.

Impact of insurance on ransom payment in healthcare

Standalone cyber policy	Wider insurance policy that includes cyber
53% paid the ransom	**34%** paid the ransom

Did your organization get any data back? Yes, we paid the ransom and got the data back. n=101 healthcare organizations that were hit by ransomware in the last year and had data encrypted (45 with standalone cyber policy, 53 with cyber as part of a wider policy)

Ransom Payments

At a global, cross-sector level, while the overall propensity to pay the ransom remains level with last year's study, the payments themselves have increased considerably, with the average (mean) ransom payment almost doubling from $812,360 to $1,542,330 year over year. The median ransom payment increased from $76,500 to $400,000 year over year.

In the case of healthcare, 12 healthcare organizations shared the exact ransom amounts paid, with the median coming in at $2.5M, up from $30,000 in 2022.

Nine healthcare organizations reported paying ransoms of $1M or more, and only one paid less than $100,000. While the low base number means the 2023 report's data is not statistically significant, and so should be used with caution, the findings do indicate that ransom payments in healthcare are increasing.

	2022	2023
Cross-sector Average	$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)
Healthcare	$196,749 (mean) $30,000 (median)	$2,884,167 (mean) $2,500,000 (median)

How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses and outliers. Cross-sector: n=216 (2023)/ 965 (2022); Healthcare: n=12 (2023)/ 83 (2022).

* Healthcare in the 2023 study has low base numbers, so the findings should be considered indicative.

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 of $1.82 million to recover from ransomware attacks, an increase from the 2022 report's figure (which included ransom payments) of $1.4 million and in line with the $1.85 million including ransom reported in the 2021 survey.

In line with the global trend, the recovery costs for healthcare organizations have increased from $1.85M to $2.20M year over year and are almost double the $1.27M reported by the sector in our 2021 survey. The increase in recovery costs in the healthcare sector this year is likely impacted by the increased frequency of data encryption in ransomware attacks.

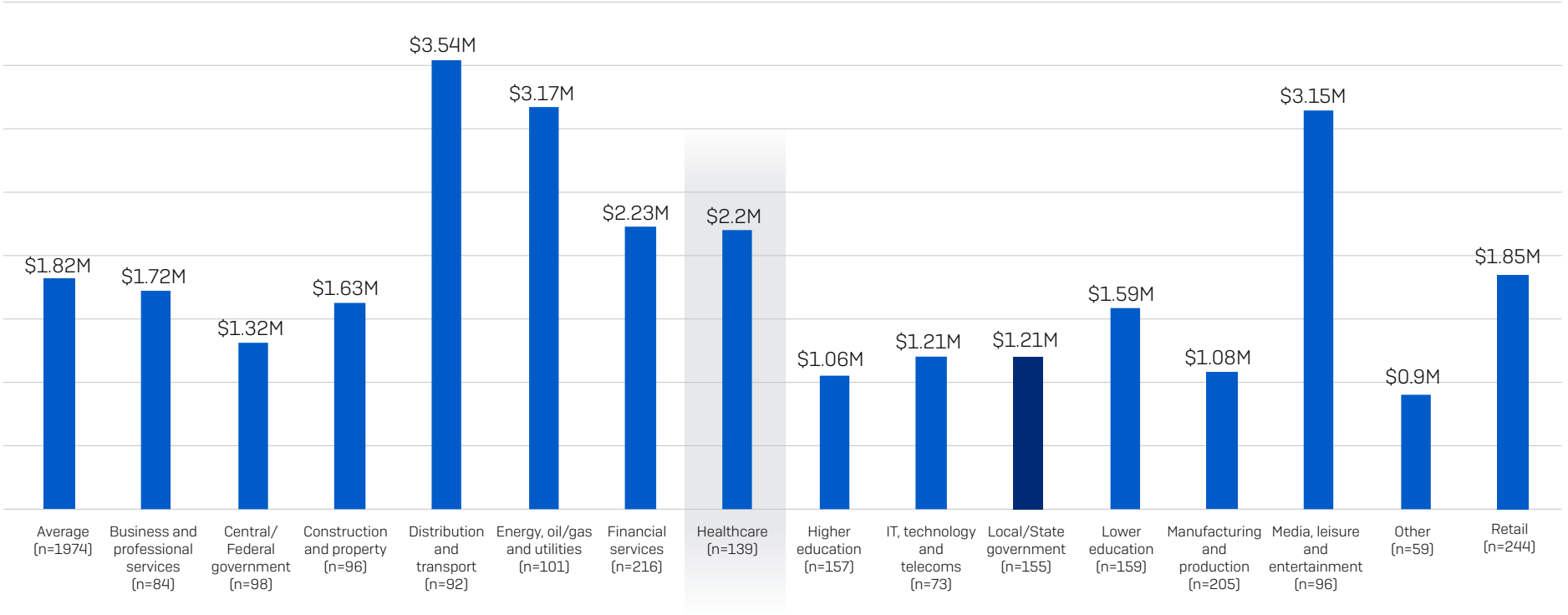
	2021	2022	2023
Cross-sector Average	$1.85M	$1.4M	$1.82M
Healthcare	$1.27M	$1.85M	$2.20M

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)/ 2,006 (2021); Healthcare: n=139 (2023)/ 253 (2022)/ 113 (2021)

N.B. 2022 and 2021 question wording also included 'ransom payment';

Recovery costs in healthcare organizations were above the cross-sector average of $1.82M. Distribution and transport paid the highest recovery cost ($3.54M), almost double the global average.

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 it is cheaper to recover encrypted data using backups than to pay a ransom.

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

The same trend was observed in the healthcare sector, where the mean recovery cost for those that used backups ($2.11M) was less than the bill incurred by those that paid the ransom ($2.58M).

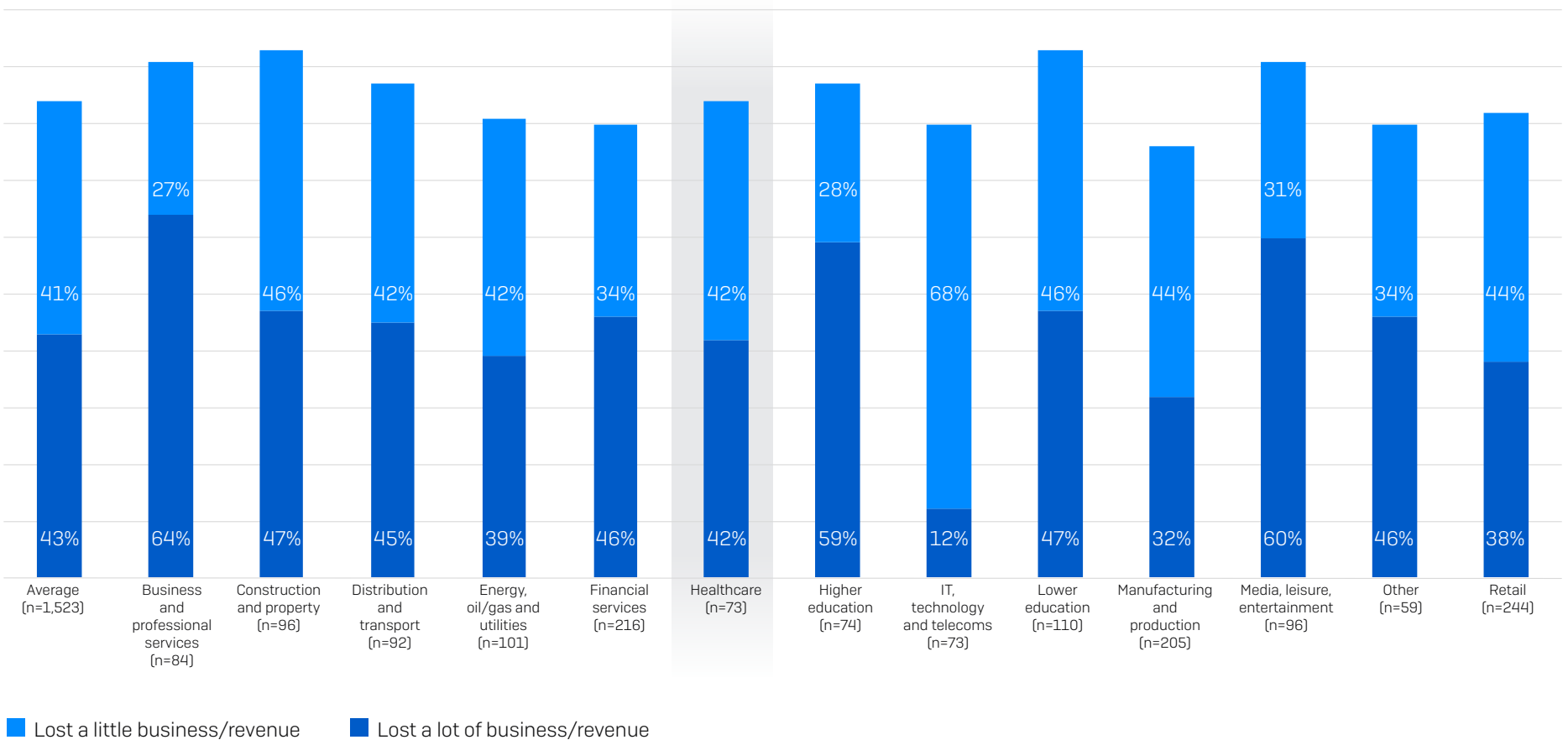
	Paid the ransom and got data back	Used backups to restore data
Cross-sector Average	**$750,000** median **$2.6M** mean	**$375,000** median **$1.62M** mean
Healthcare	**$750,000** median **$2.58M** mean	**$750,000** median **$2.11M** mean

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;

Healthcare: n=42 that paid the ransom and got data back and n=74 that used backups to restore the data.

Business Impact

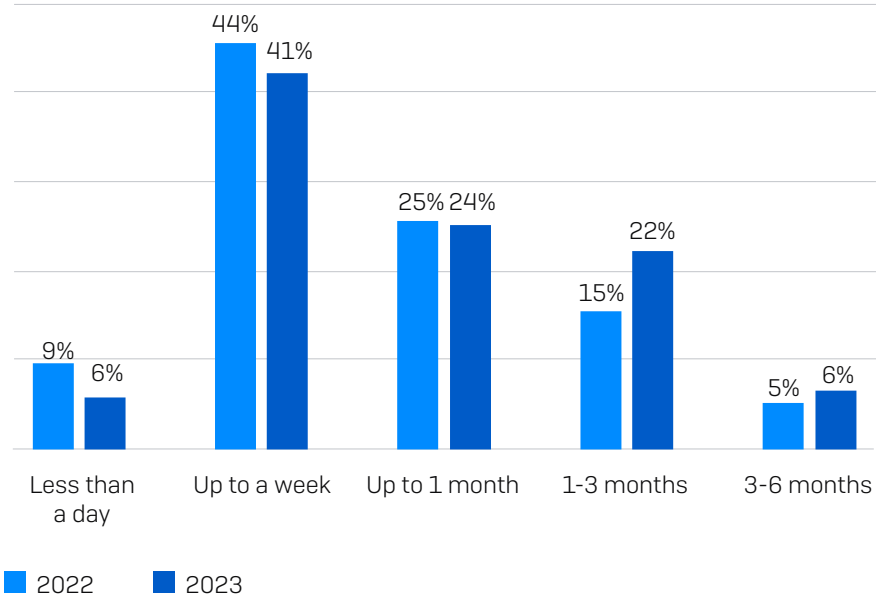
85% of private-sector healthcare organizations hit by ransomware said the attack caused them to lose business/revenue, slightly above the global cross-sector average of 84%. Lower education (94%) and construction and property (93%) were most likely to have lost some business/revenue, while business and professional services was most likely to report that they lost a lot of business/revenue (64%). Conversely, in the well-prepared IT, technology, and telecoms sector, just 12% reported losing a lot of business/revenue.



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

It is taking healthcare organizations longer to recover from a ransomware attack, with 47% now recovering within a week compared to 54% in the 2022 report. Furthermore, the percentage of organizations that took more than a month to recover increased to 28% (with rounding) from 20% (with rounding) year over year.



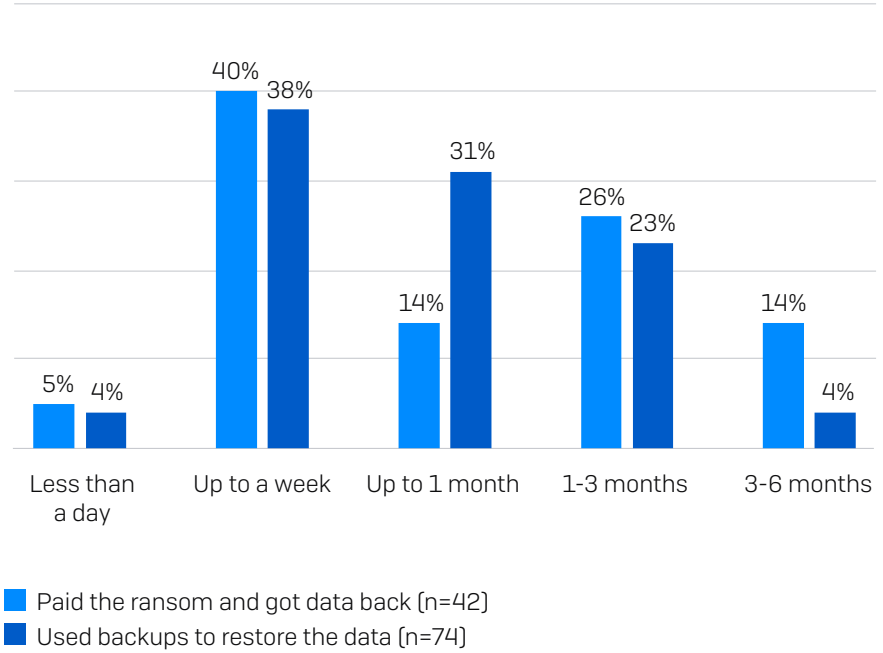
How long did it take your organization to fully recover from the ransomware attack?
139 (in 2023) /253 (in 2022) healthcare organizations that were hit by ransomware.

Recovery time by data recovery method

The research revealed that healthcare organizations that use backups to restore their data recover from the attack more quickly than those that pay the ransom.

One-fourth of the respondents (27% with rounding) that used backups took more than a month to recover data, while 40% (with rounding) that paid the ransom took more than a month to recover.

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.



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 to healthcare organizations. Although the sector reported a drop in the rate of ransomware attacks in this year's report, almost two-thirds (60%) of respondents were hit by ransomware.

As adversaries continue to hone their attack tactics, techniques, and procedures (TTPs), defenders struggle to keep pace, resulting in consistently high levels of attack and increased encryption rates: almost three-quarters of healthcare organizations (73%) hit by ransomware had their data encrypted, up from 61% the year prior. In addition, 37% of those that had data encrypted reported that data was also stolen.

On an encouraging note, the healthcare sector reported a decrease in the propensity to pay the ransom to recover encrypted data, down from 61% in last year's survey to 42% in the 2023 report.

At the same time, the use of backups by healthcare only increased slightly, from 72% to 73% year over year. The good news is that all healthcare organizations that had data encrypted were able to recover data after the attack, higher than the cross-sector average of 97%.

Organizations' insurance positions impacted their data recovery method. While 53% of healthcare organizations that had data encrypted and had a standalone cyber insurance policy paid the ransom, the number dropped to 34% for organizations with broader insurance policies that included cyber.

The overall recovery cost for healthcare organizations has increased from $1.85M to $2.20M year over year, likely – in part – due to the increased encryption rate following attacks. The healthcare recovery cost was above the cross-sector average of $1.82M.

With the growth of the ransomware-as-a-service business model, Sophos does not anticipate a drop in attacks over the course of 2023.

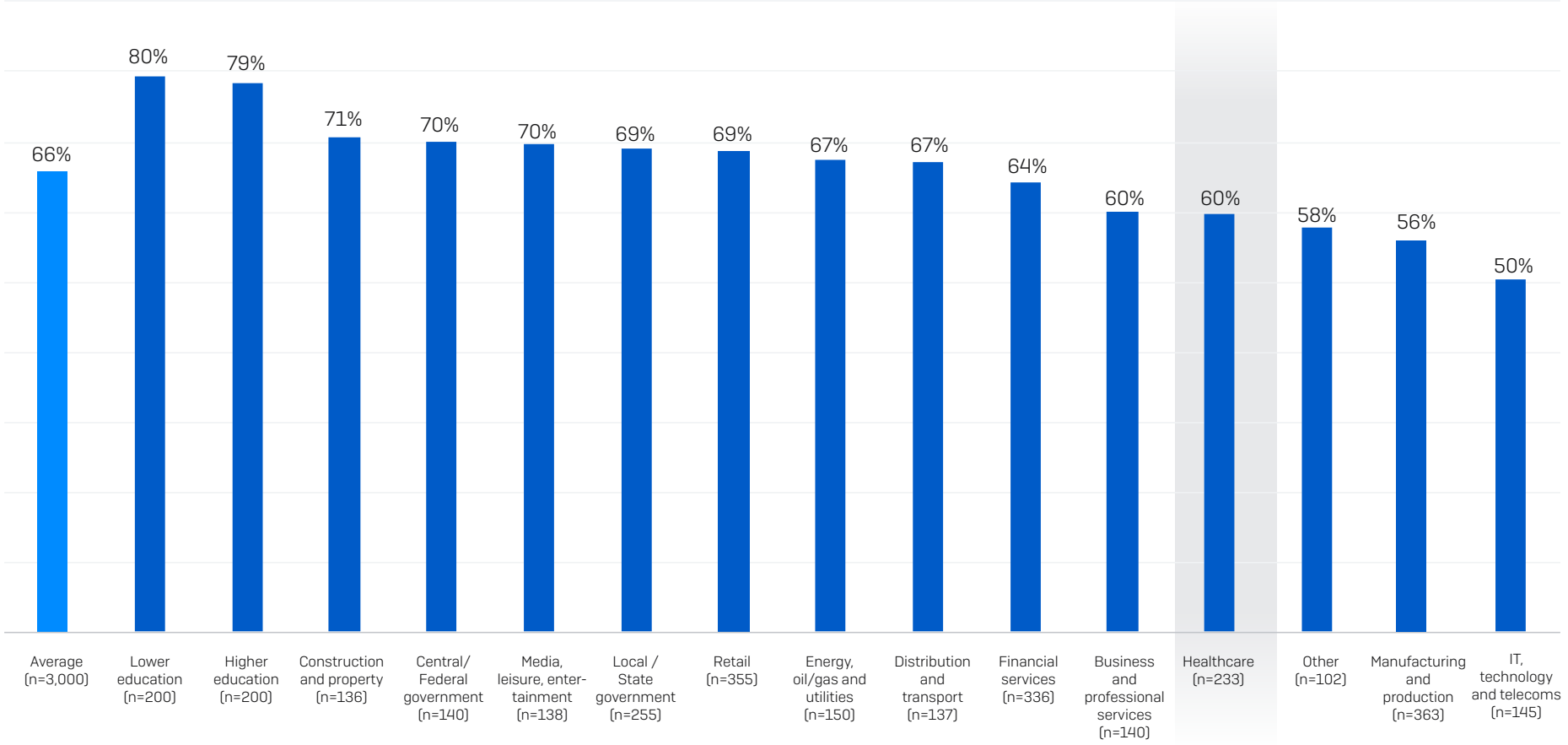
Organizations should focus on:

- 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
- Optimizing attack preparation, including making regular backups, practicing recovering data from backups, and maintaining an up-to-date incident response plan
- Maintaining good security hygiene, including timely patching and regularly reviewing security tool configurations

Additional Charts

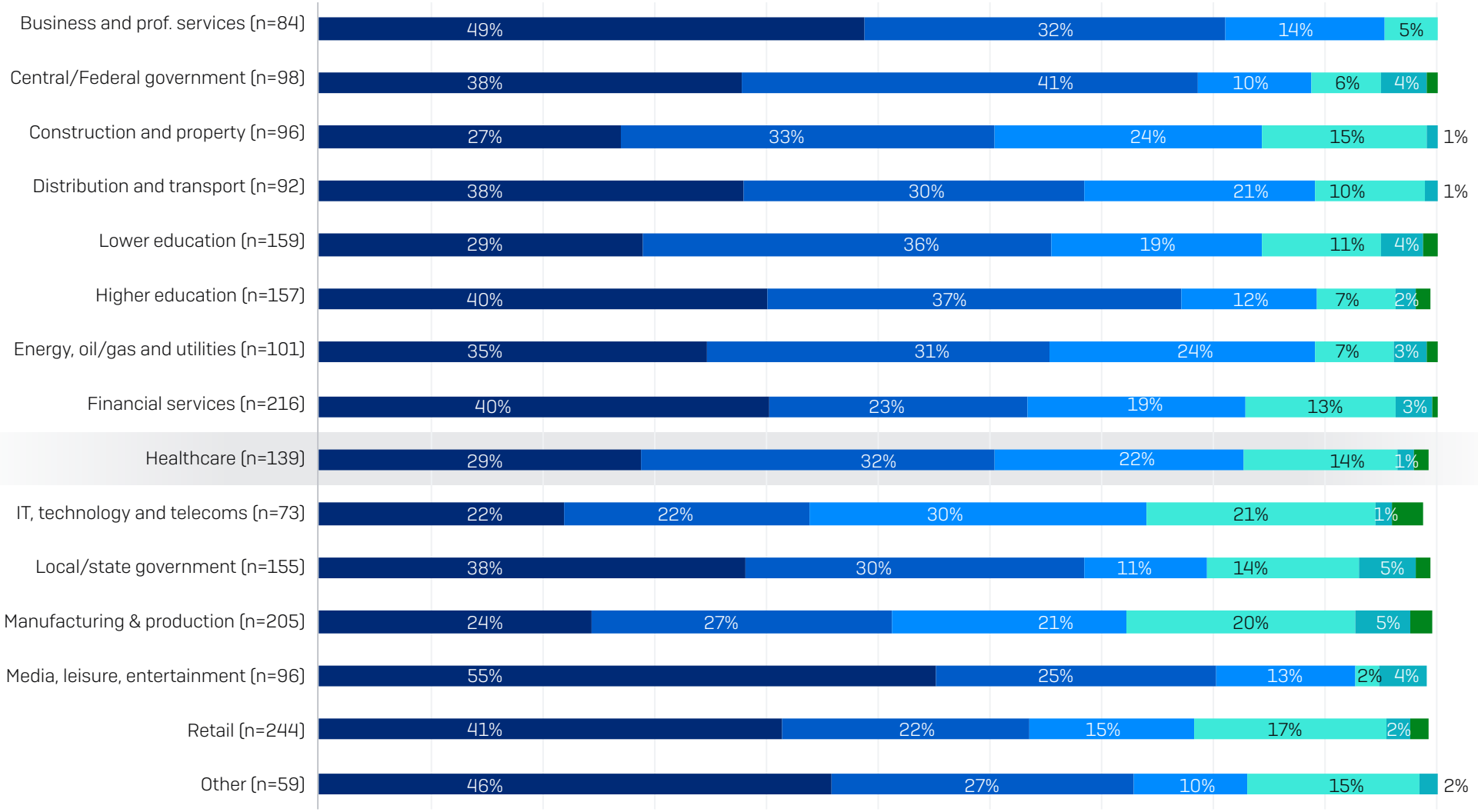
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



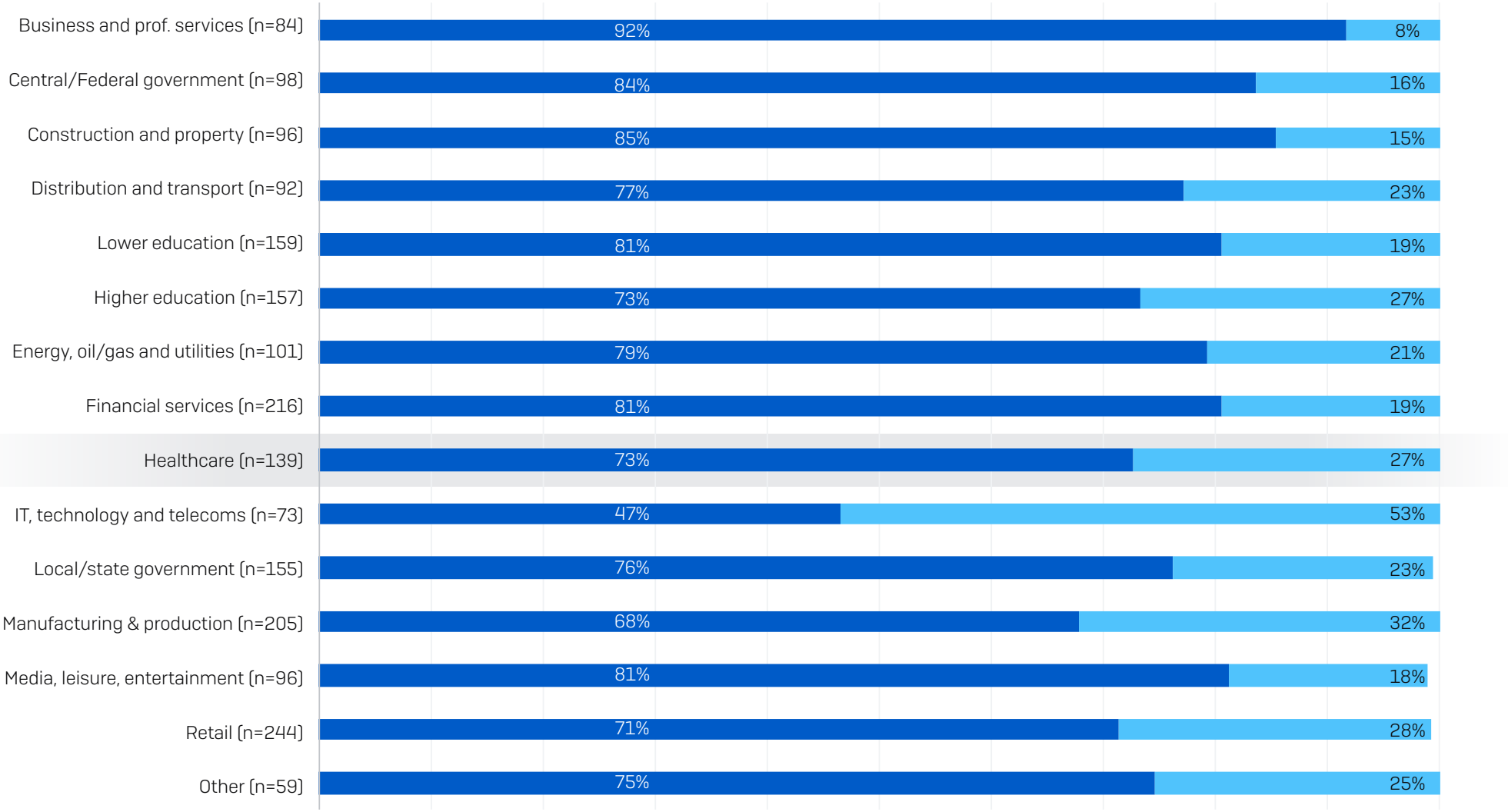
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



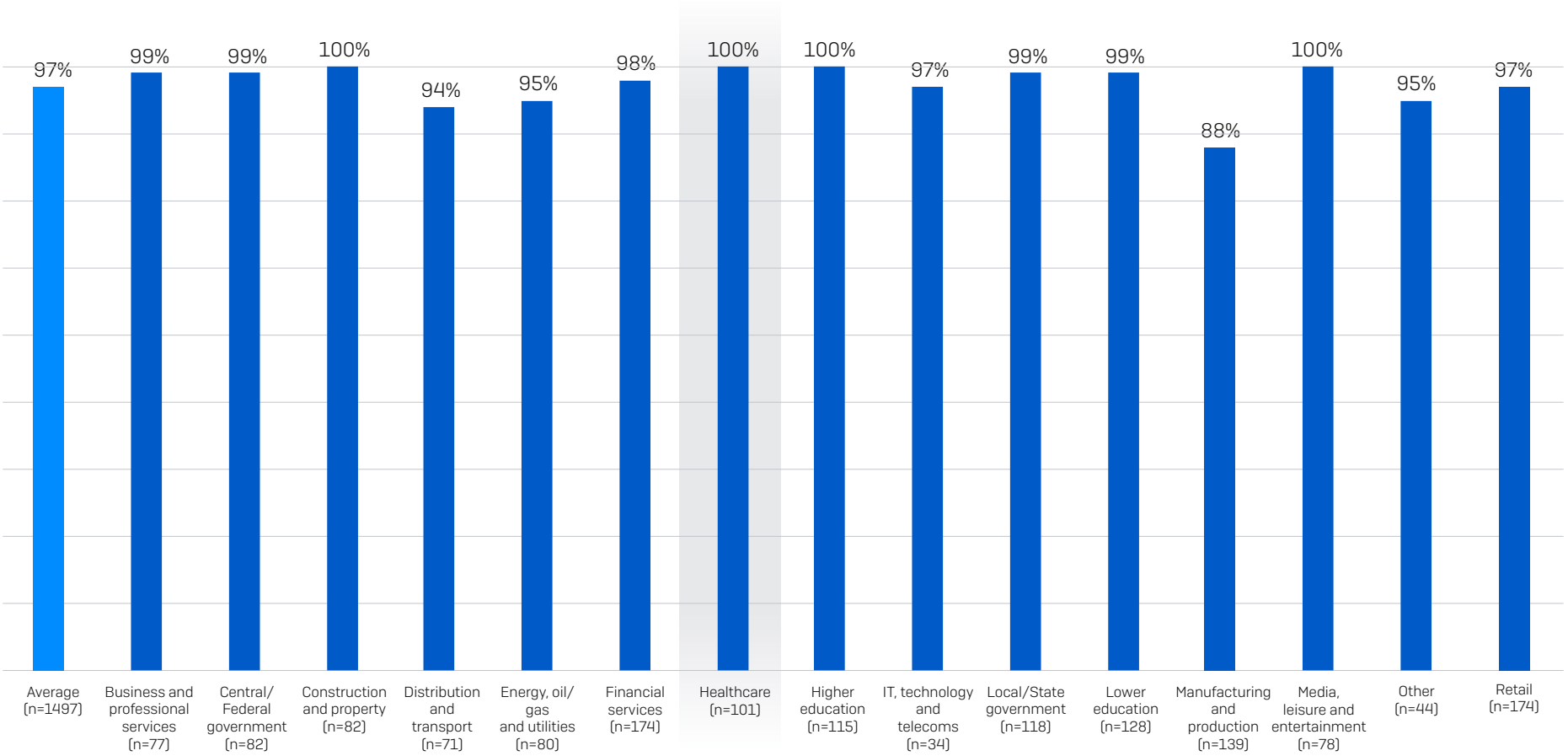
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



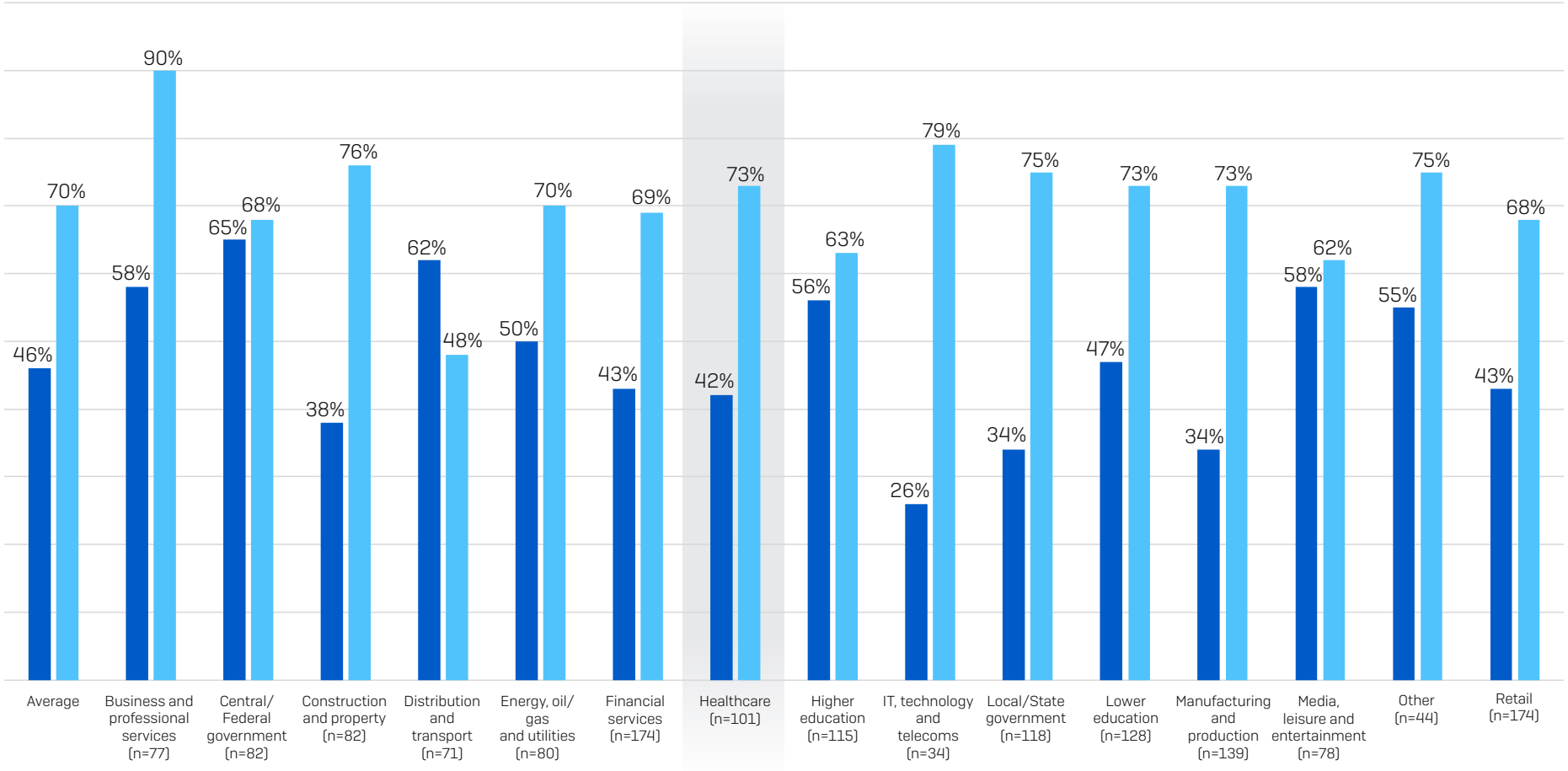
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

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

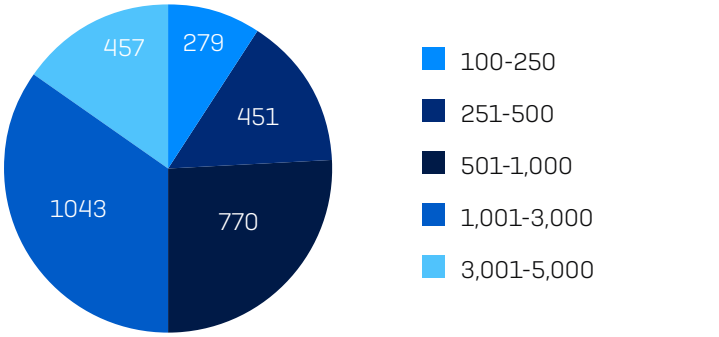
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

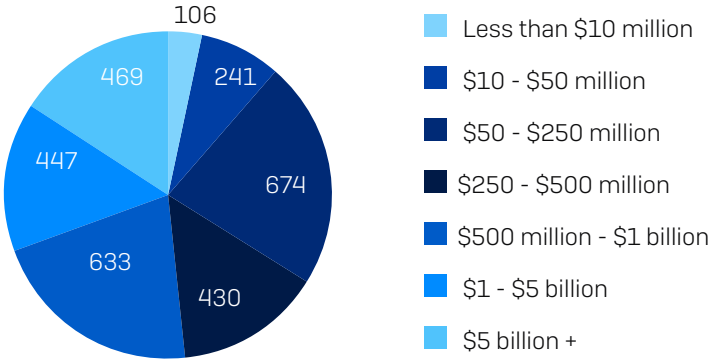
Respondents by Country

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.

2023-08-03 (WP-NP)

SOPHOS