SOPHOS

The State of Ransomware in State and Local Government 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 225 from the state and local government 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 state and local government 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 225 in state and local government 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.

3,000
respondents

225
State/local government respondents

14
countries

100-5,000
employees

<$10M - $5B+
annual revenue

Jan-Mar 23
research conducted

Rate of Ransomware Attacks in Government

The 2023 study revealed that the rate of ransomware attacks in state and local government organizations continues to rise: 69% of state and local government organizations reported that they were hit by ransomware, up from 58% in the 2022 report and more than double the rate reported in the 2021 survey, when 34% of state and local government organizations experienced a ransomware attack.

With over two-thirds of state and local government organizations hit by ransomware in the last year, it's clear that adversaries are able to execute attacks at scale consistently, making ransomware arguably the biggest cyber risk facing state and local government organizations 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.

2021	2022	2023
34%	58%	69%

In the last year, has your organization been hit by ransomware? Yes. n=225 (2023), 199 (2022), 131 (2021)

The rising rate of ransomware attacks in state and local government organizations contrasts with the global cross-sector trend that remained 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.

The rate of ransomware attacks in state and local government organizations in the 2023 study was above the cross-sector average. 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 State and Local Government

Exploited vulnerabilities (38%) and compromised credentials (30%) were the two most common root causes of the most significant ransomware attacks in the state and local government sector. Email-based attacks (malicious emails or phishing) were less common root causes but were still the starting points for a quarter of the attacks (25%) in state and local government organizations, whereas the cross-sector average was 30%.

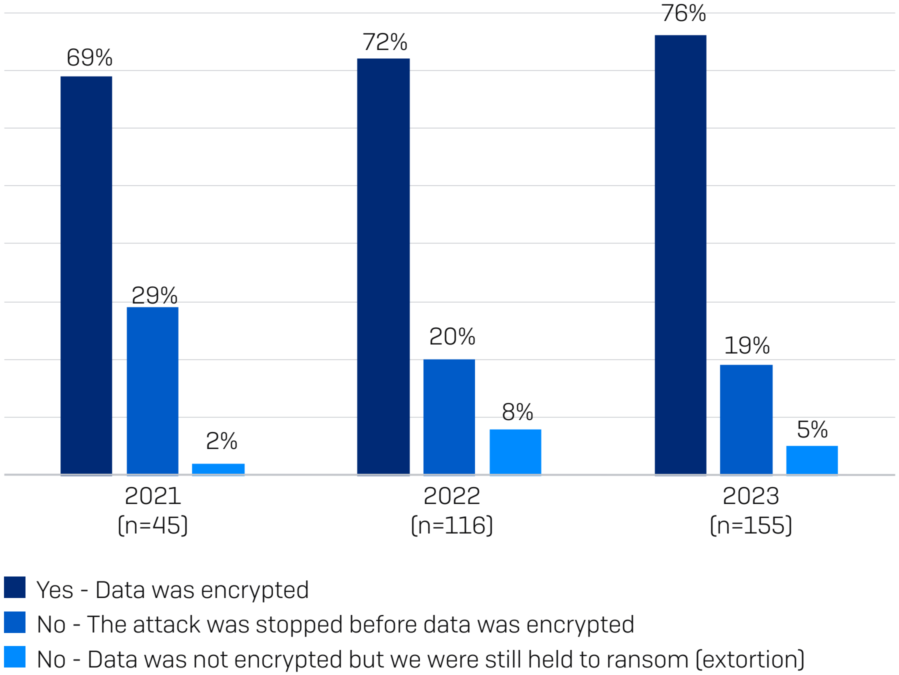
The findings suggest that the state and local government organizations were in line with the cross-sector average that reported exploited vulnerabilities as the most common root cause in 36% of attacks, followed by compromised credentials that were behind 29% of attacks.

	STATE AND LOCAL GOVERNMENT (n=155)	CROSS-SECTOR AVERAGE (n=1,974)
Exploited vulnerability	38%	36%
Compromised credentials	30%	29%
Malicious email	11%	18%
Phishing	14%	13%
Brute force attack	5%	3%
Download	1%	1%

Rate of Data Encryption in State and Local Government

Data encryption in the state and local government sector continues to rise. The rate of data encryption in the 2023 report was the highest in the last three years, with the sector reporting that 76% of attacks resulted in data getting encrypted, up from 72% in the 2022 report and 69% in the 2021 report. This likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

19% of attacks in state and local government organizations were stopped before the data was encrypted, down from 20% in the 2022 report and 29% in the 2021 report. The rate of extortion-only attacks dropped to 5% in the 2023 report from 8% in the 2022 survey, but it was higher than the 2% reported in our 2021 survey.



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

The findings for state and local government are in line with the cross-sector average, where 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.

Concerningly, state and local government organizations reported the highest rate of attacks (48%), where data that was encrypted was also stolen. This was much higher than the global average rate of 30%, suggesting that the state and local government sector is particularly exposed to such "double dip" attacks. This 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.

48%

of ransomware attacks on state and local governments 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=118/57

Data Recovery Rate in State and Local Government

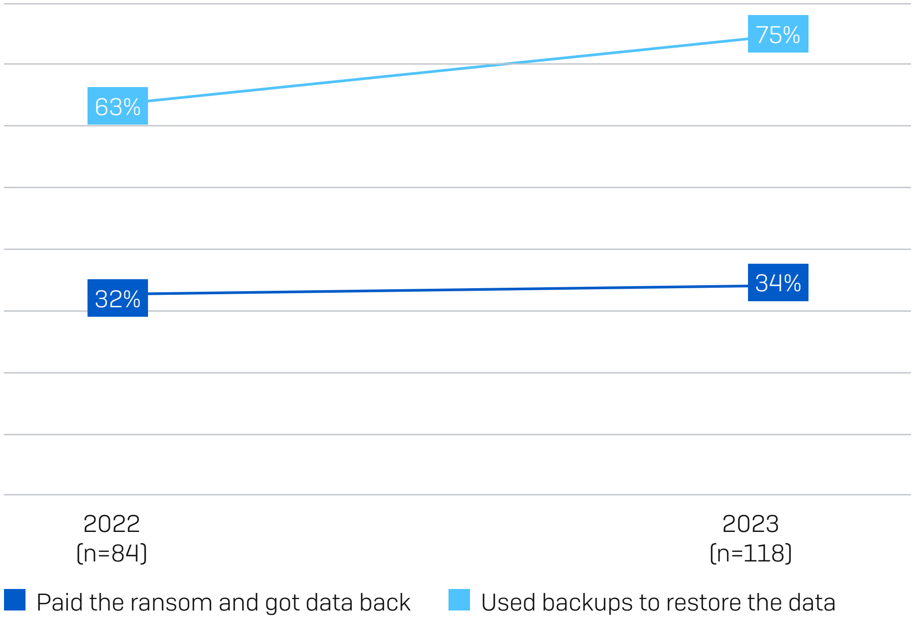
In state and local government organizations where the data was encrypted, 99% got their data back, which is above the cross-sector average of 97%.

It's encouraging to note that the use of backups for data recovery by the state and local government sector went up from 63% in the 2022 report to 75% in this year's survey. At the same time, 34% of organizations paid the ransom to get encrypted data back, slightly up from the 32% who reported paying the ransom in the previous survey. 11% of respondents reported using multiple means to recover encrypted data.

	STATE AND LOCAL GOVERNMENT	CROSS-SECTOR AVERAGE
Got data back	99%	97%
Used backups to restore data	75%	70%
Paid the ransom to get data back	34%	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=118 (state and local government).

Although the rate of ransom payments in state and local government organizations shows an upward trend, it was lower than the cross-sector average of 46% in the 2023 report. 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 state and local government organizations was 99%, the method used to recover data differed 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.

Half of the state and local government organizations (50%) that had data encrypted and had a standalone cyber insurance policy paid the ransom. This dropped to 22% for organizations with broader insurance policies that included cyber.

Impact of insurance on propensity to pay ransom

Standalone cyber policy	Wider insurance policy that includes cyber
50% paid the ransom	**22%** paid the ransom

Did your organization get any data back? Yes, we paid the ransom and got the data back. n=118 state and local government organizations that were hit by ransomware in the last year and had data encrypted (50 with standalone cyber policy, 64 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.

The increase in ransom payment in state and local government was even greater, with the average (mean) ransom payment in state and local government coming in at $1,078,913 in our 2023 survey, which was 5X higher than in our 2022 report ($213,801). The median ransom payment went up from $13,000 to $75,000 year over year.

While this is a considerable increase, it's worth noting that the mean ransom paid by state and local governments in the last year was almost $500,000 less than the cross-sector average ($1,542,330).

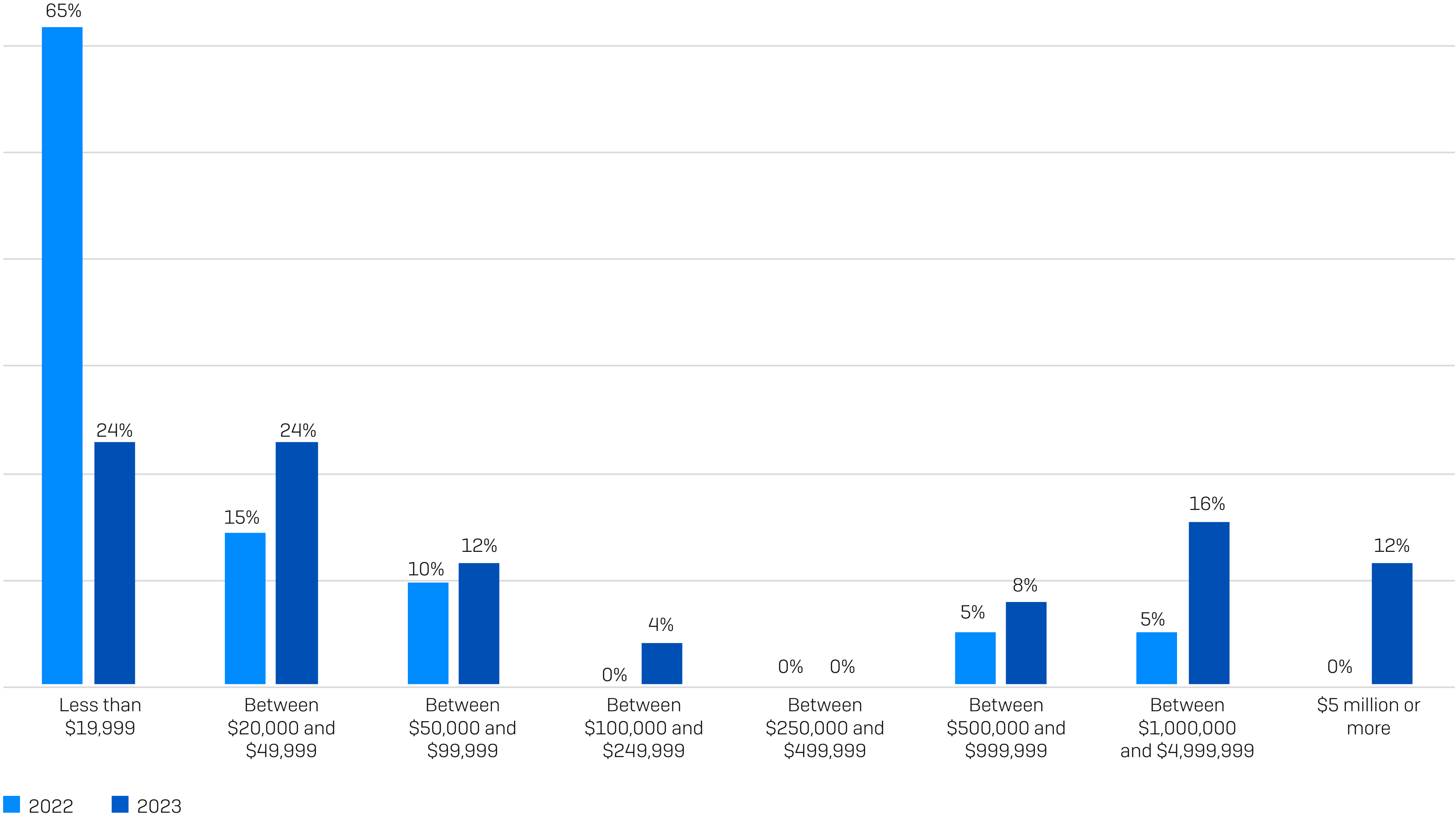
	2022	2023
Cross-sector Average	$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)
State and Local Government	$213,801 (mean) $13,000 (median)	$1,078,913 (mean) $75,000 (median)

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); State and local government: n=25 (2023)/ 20 (2022).

* State and local government has low base numbers, so the findings should be considered indicative.

The proportion of state and local government organizations paying higher ransoms has increased from our 2022 study, with over a quarter of organizations (28%) reporting payments of $1 million or more compared to 5% (with rounding) the year prior. Conversely, 60% paid less than $100,000, down from 90% in last year's report.

Ransom Payments by Retail: 2023 vs. 2022



How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses. n=25 (2023)/ 20 (2022).

*Response base is low, 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 state and local government organizations have doubled from $0.66M to $1.21M year over year but are lower than the $1.64M reported in the 2021 survey. The increase in recovery costs in the state and local government sector this year is likely impacted by its challenges when trying to stop data encryption following attacks.

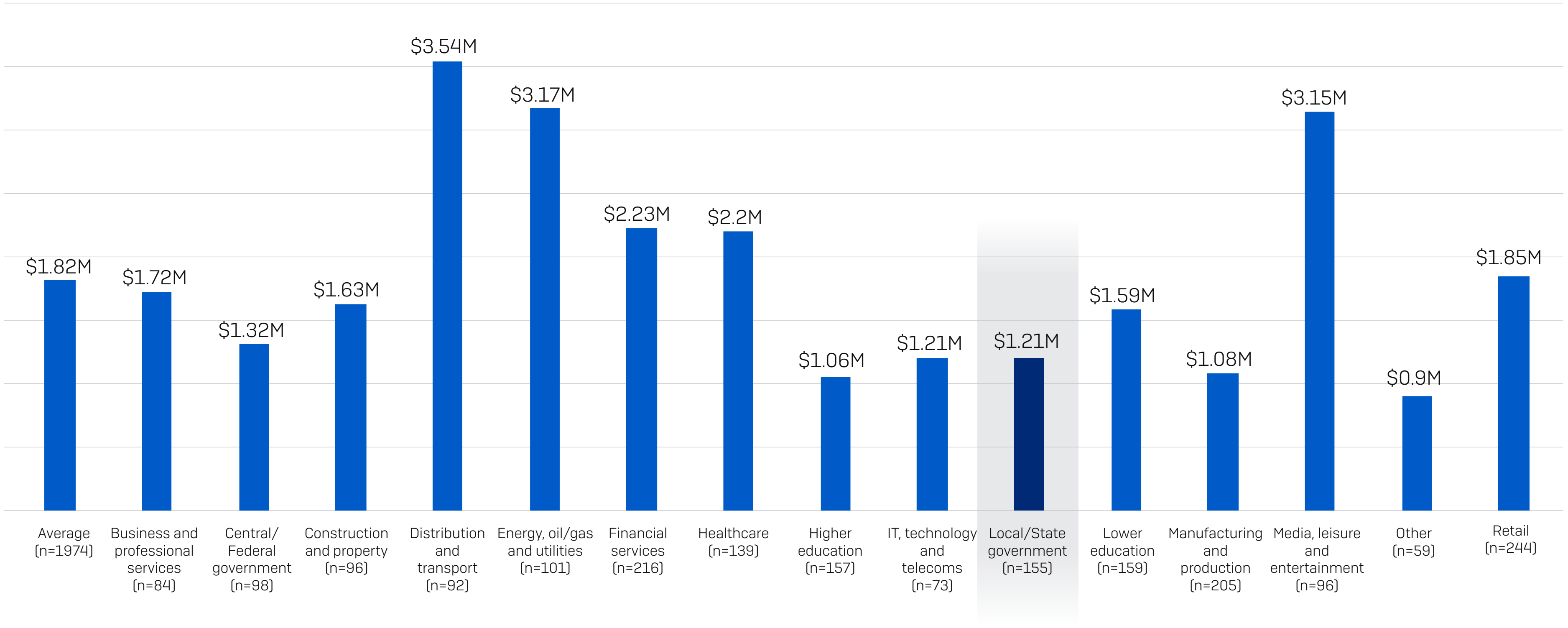
	2021	2022	2023
Cross-sector Average	$1.85M	$1.4M	$1.82M
State and Local Government	$1.64M	$0.66M	$1.21M

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); State and local government: n=155 (2023)/ 116 (2022)/ 45 (2021)

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

Recovery costs in state and local government organizations were far below 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 state and local government sector, where the mean recovery cost for those that used backups ($930,000) was less than half the bill incurred by those that paid the ransom ($2M).

	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
State and Local Government	**$375,000** median **$2M** mean	**$375,000** median **$930,000** mean

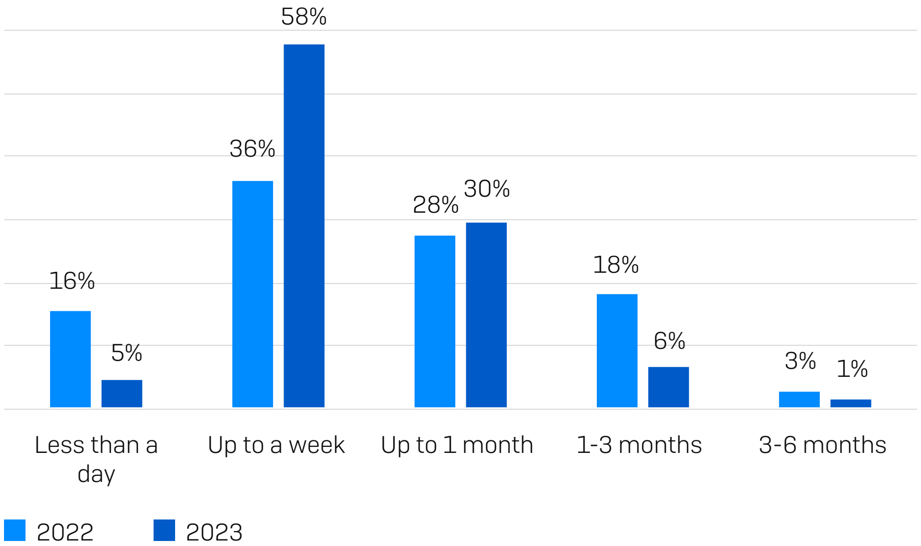
What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? Cross-sector: n=694 that paid the ransom and got data back and 1,053 that used backups to restore the data;

State and local government: n=40 that paid the ransom and got data back and 88 that used backups to restore the data.

Recovery Time

State and local government organizations have gotten quicker at getting back up and running after a ransomware attack, with 63% recovering within a week in this year's study compared to 52% in the last survey.

The percentage of organizations that took more than a month to recover decreased to 7% (with rounding) from 21% (with rounding) year over year, suggesting that recovery is faster for this sector.



How long did it take your organization to fully recover from the ransomware attack?
155 (in 2023) /116 (in 2022) state and local government organizations that were hit by ransomware.

Conclusion

Ransomware remains a major threat to state and local government organizations, with over two-thirds (69%) of respondents reporting being hit by ransomware in this year's report. 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: over three-quarters of state and local government organizations (76%) hit by ransomware had their data encrypted. In addition, almost half of these respondents (48%) reported that their encrypted data was also stolen – the highest rate across all industries.

On an encouraging note, state and local government organizations increased their use of backups to recover encrypted data, which saw a rise from 63% reported in our 2022 study to 75% this year. However, the rate of ransom payments went slightly up from 32% to 34% year over year. All said, 99% of state and local government respondents that had data encrypted could recover data after the attack, which is higher than the cross-sector average of 97%.

Organizations' insurance positions impacted the data recovery method. While 50% of state and local government organizations that had data encrypted and had a standalone cyber insurance policy paid the ransom, the number dropped to 22% for organizations with broader insurance policies that included cyber.

The recovery cost for state and local government organizations has doubled from $0.66M to $1.21M year over year, likely because of the sector's challenges with stopping data encryption following attacks. At the same time, the cost was significantly below 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.

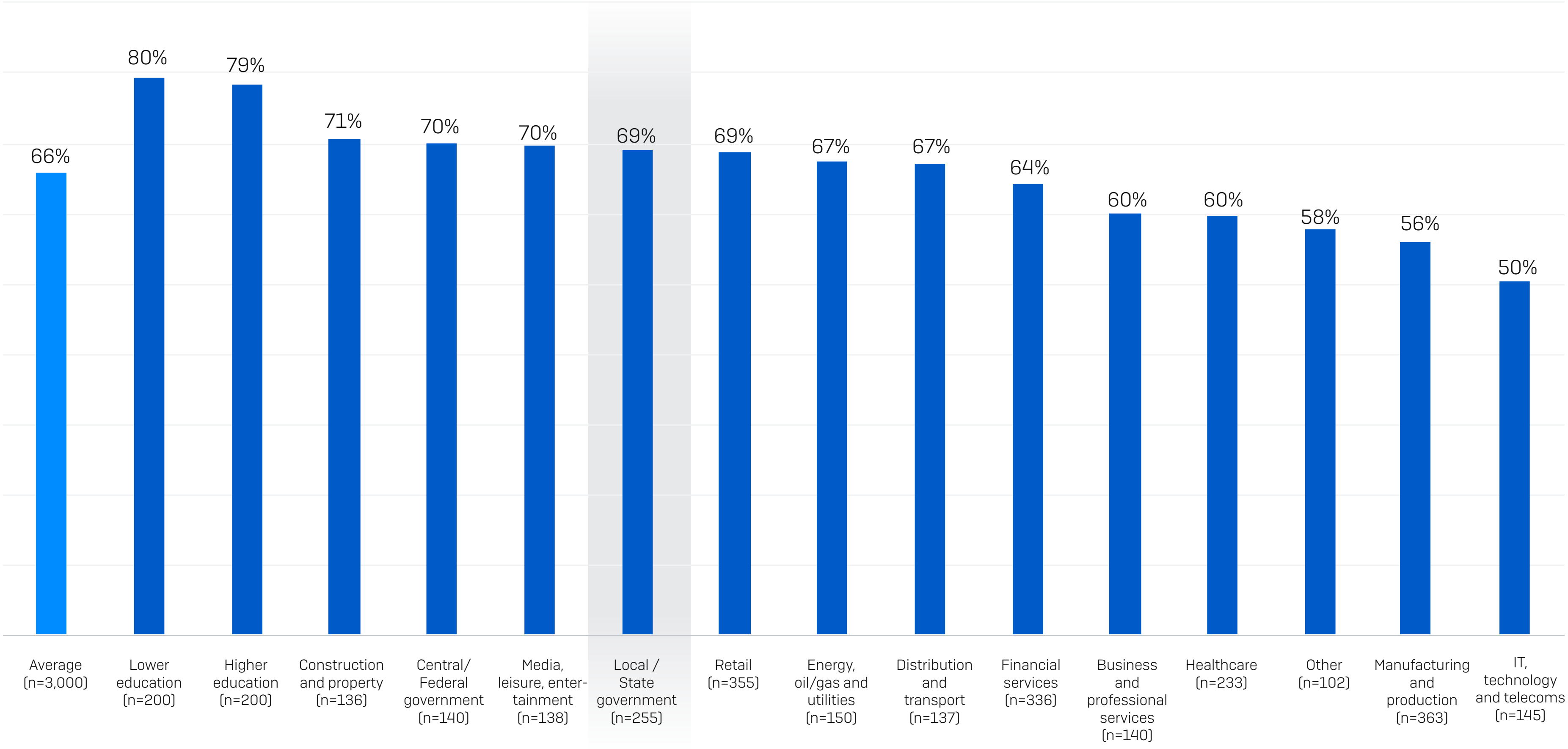
Organizations should focus on:

- 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

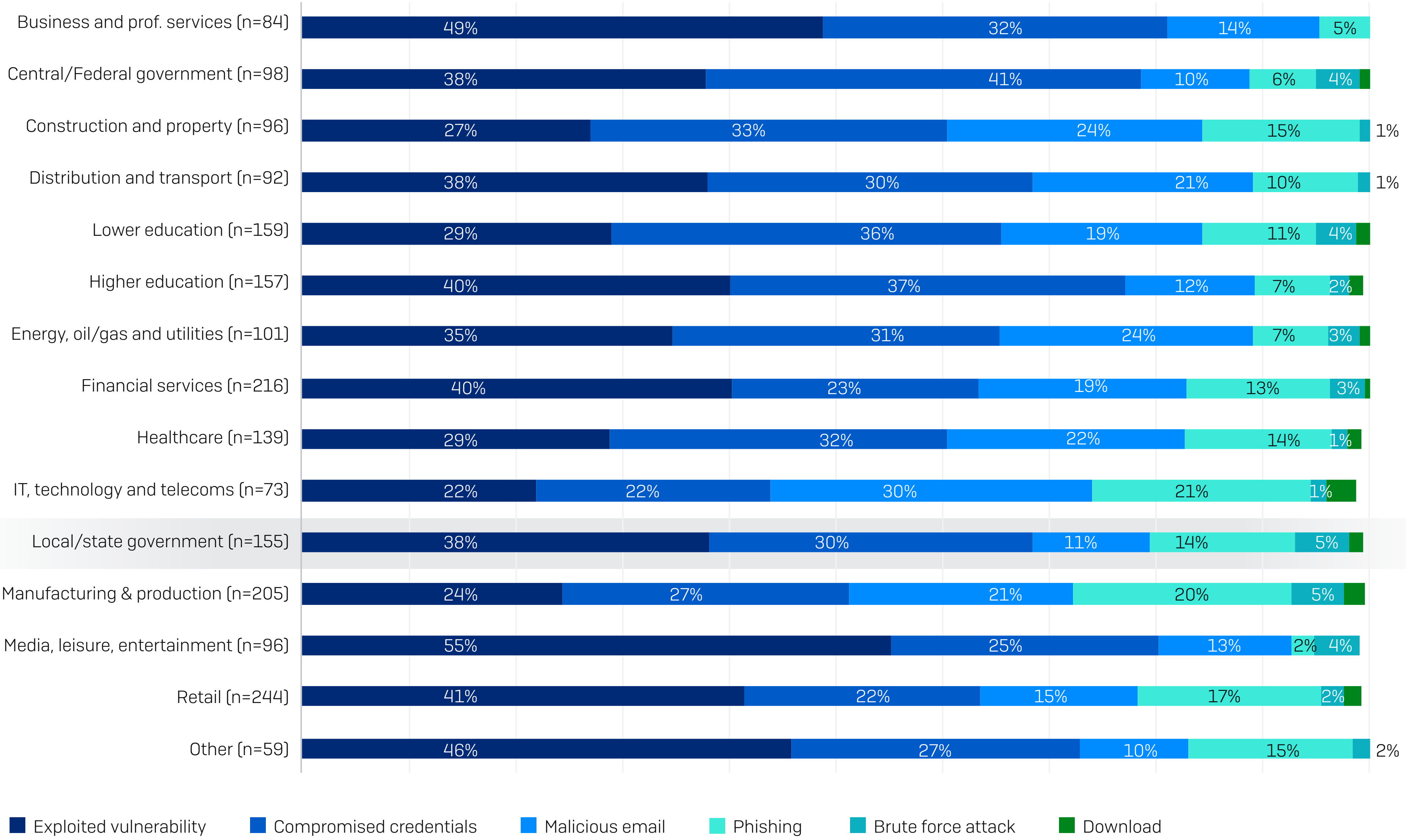
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



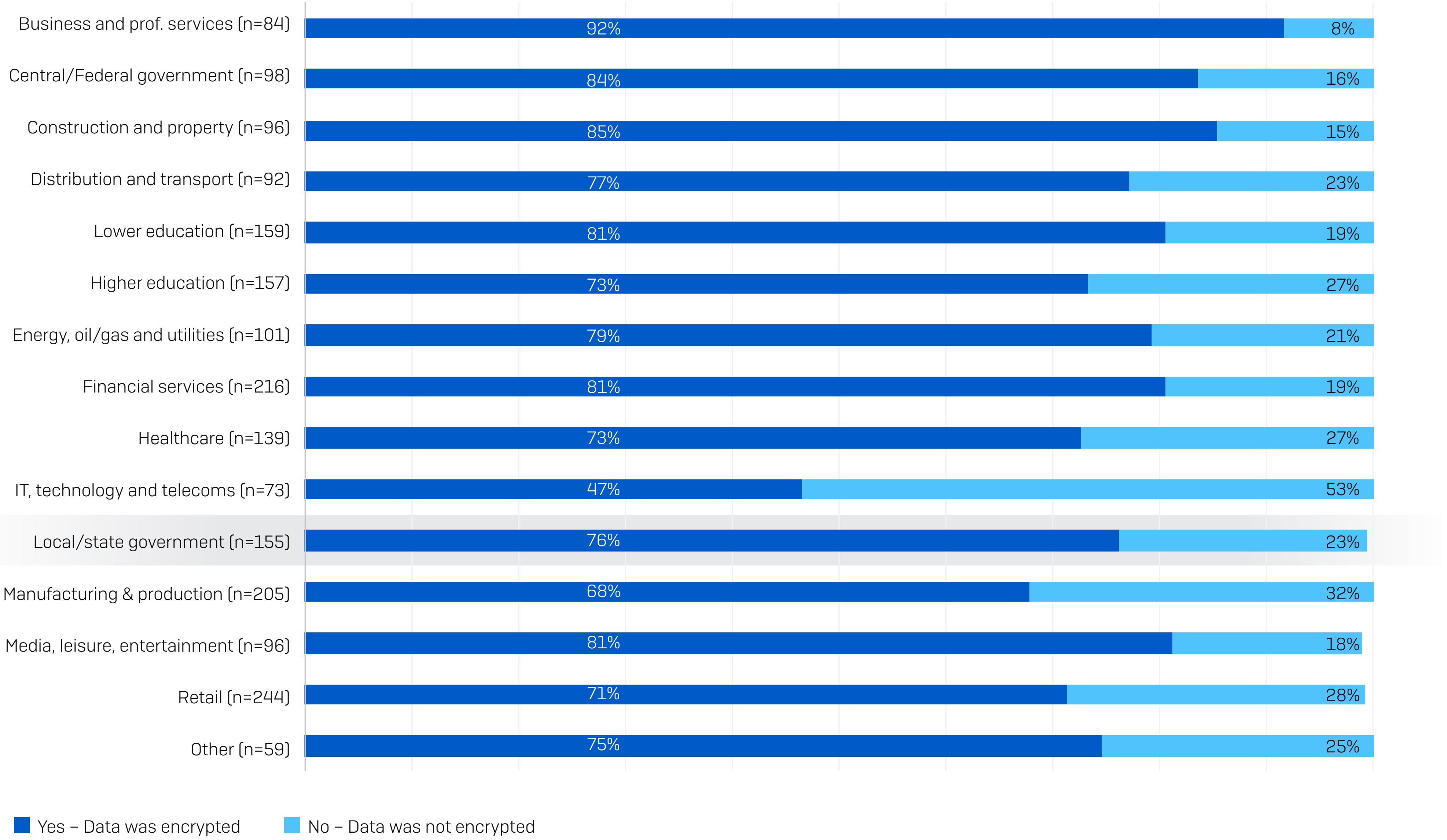
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



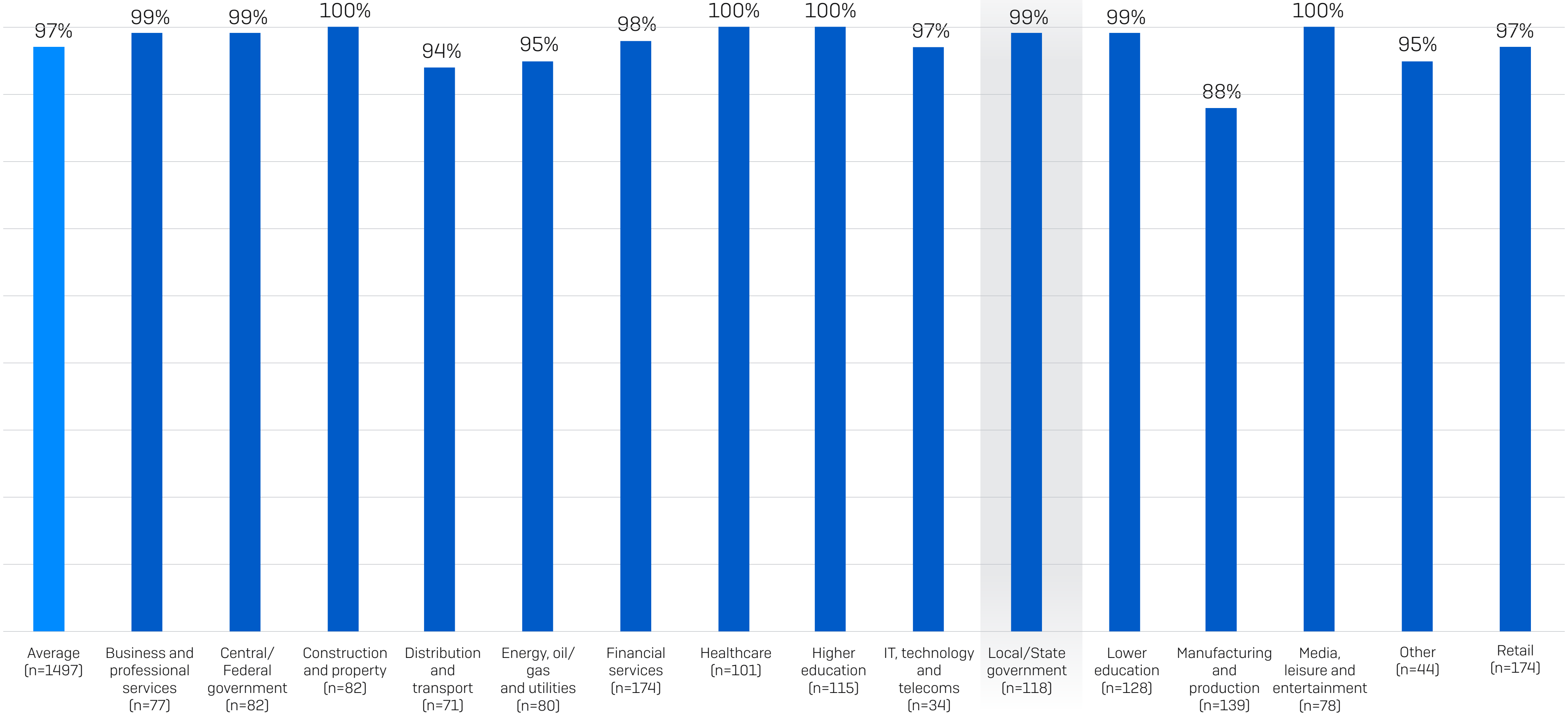
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



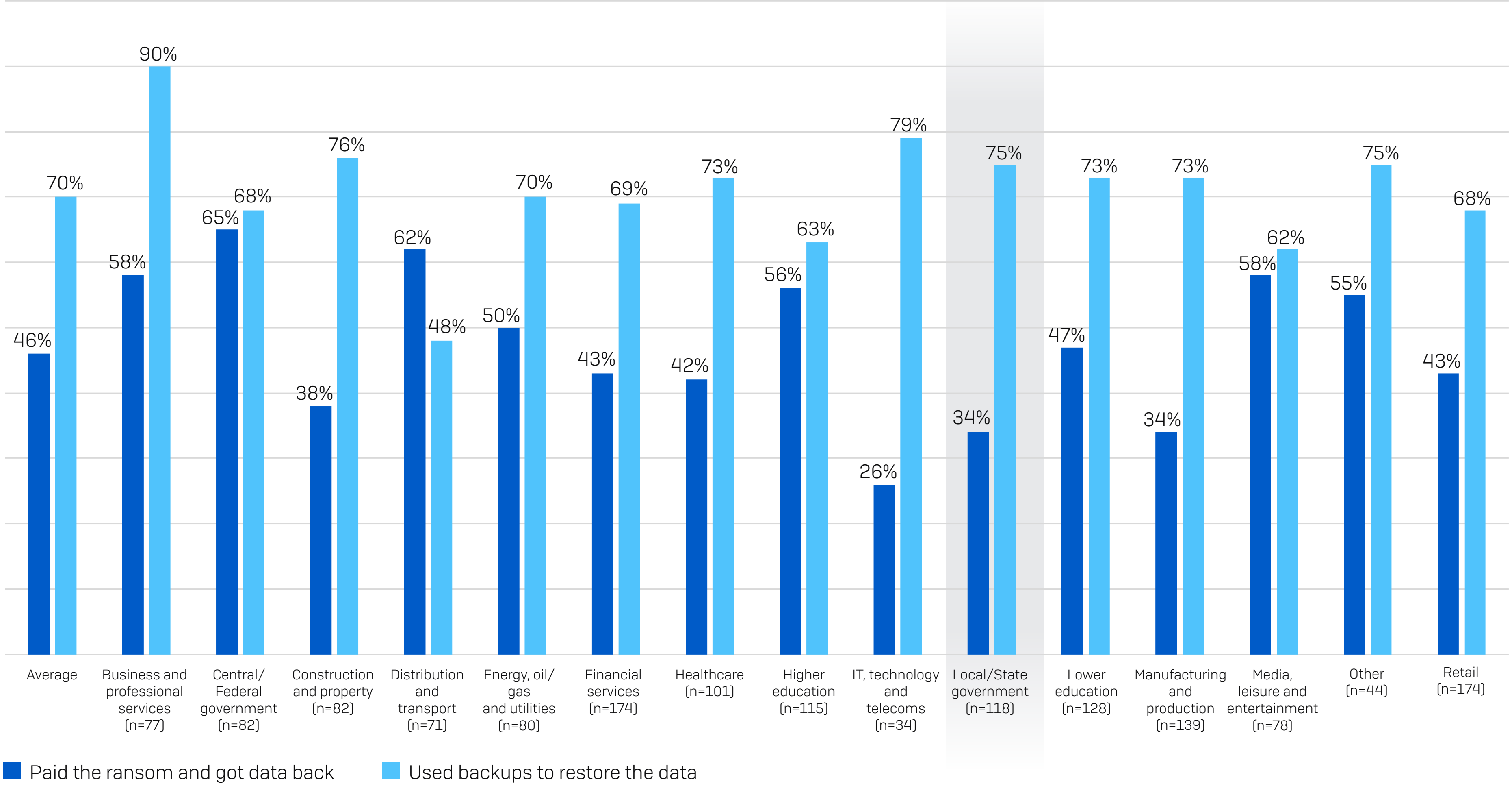
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

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

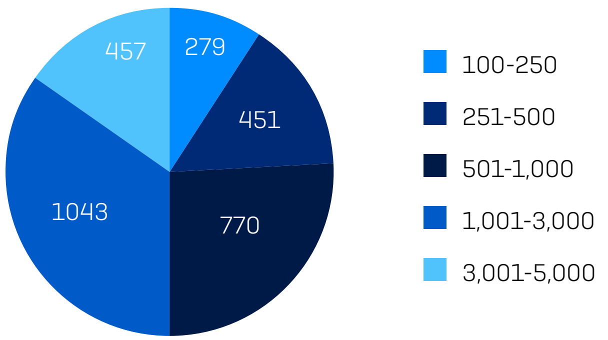
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

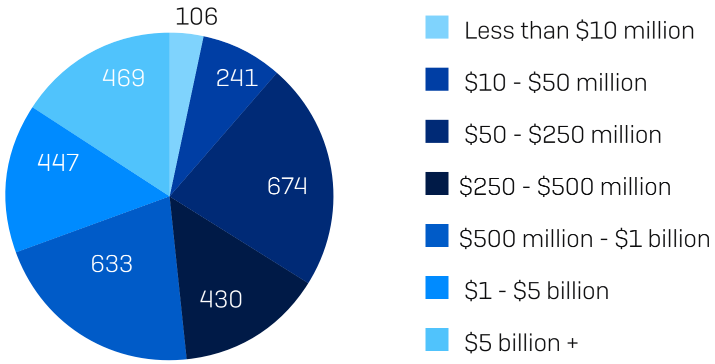
Respondents by Country

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.

2023-07-26 (WP-NP)

SOPHOS