SOPHOS

The State of Ransomware in Retail 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 355 from the retail 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 retail organizations in 2023. It reveals the most common root causes of attacks and shines new light on how ransomware impacts the retail sector. The report also reveals the business and operational impact of paying the ransom to recover data rather than using backups.

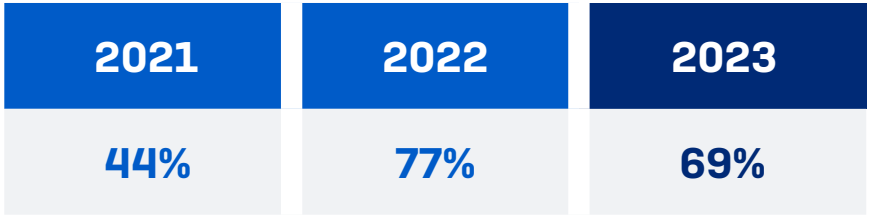
About the Survey

Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in organizations with between 100 and 5,000 employees, including 355 in retail, 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 Retail

The 2023 study revealed that the rate of ransomware attacks in retail has dropped from 77% in 2022 to 69% in 2023. While this is a welcome drop, with over two-thirds of retail 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 retail 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.



In the last year, has your organization been hit by ransomware? Yes. n=355 (2023), 422 (2022), 435 (2021)

Retail's declining rate of ransomware attacks bucks the global cross-sector trend, which has remained flat: 66% of all 2023 respondents reported that their organizations were hit by ransomware, the same as in our 2022 survey.

Despite retail's reported drop in attacks, the rate remains above average. Education was the sector 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 Retail

Exploited vulnerabilities (41%) were the most common root cause of the most significant ransomware attacks in the retail sector, followed by compromised credentials (22%). Phishing was the third most common root cause, behind 17% of incidents. Overall, nearly one-third of retail respondents (32%) said email (malicious emails or phishing) was the root cause of the attack, comparable with the cross-sector average of 30%.

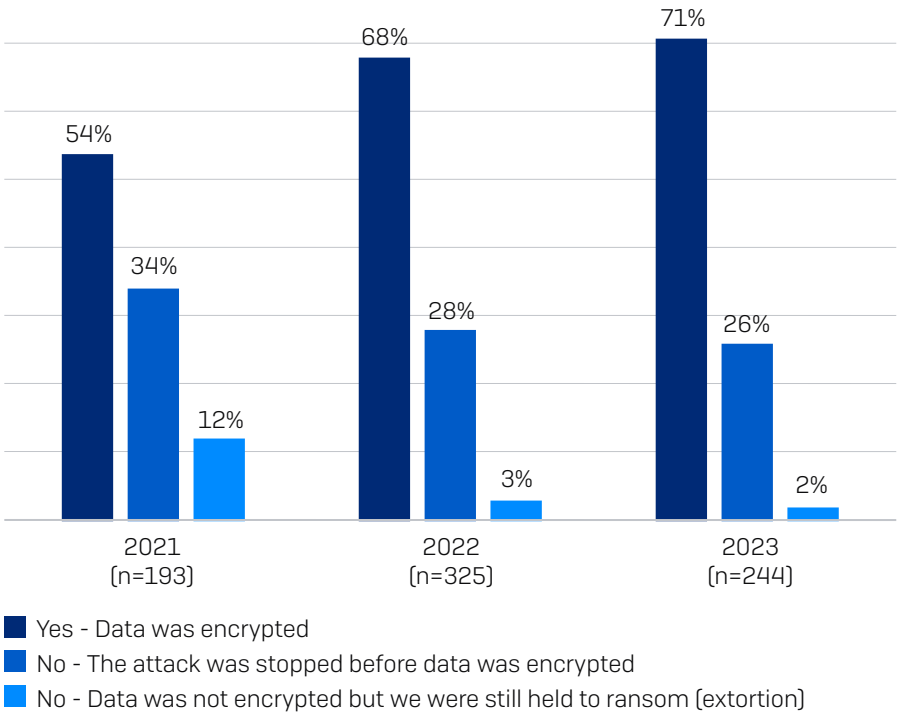
Globally, retail was one of the sectors most likely to report exploited vulnerabilities and phishing as the root causes of attacks. Conversely, the use of compromised credentials as the starting points for ransomware attacks in retail was the lowest of all sectors (joint with IT, telecoms and technology).

	RETAIL (n=244)	CROSS-SECTOR AVERAGE (n=1,974)
Exploited vulnerability	41%	36%
Compromised credentials	22%	29%
Malicious email	15%	18%
Phishing	17%	13%
Brute force attack	2%	3%
Download	2%	1%

Rate of Data Encryption in Retail

Data encryption in the retail sector has continued to rise, with the 2023 report revealing the highest encryption level in three years. This likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

Almost three-quarters of ransomware attacks (71%) in retail resulted in data being encrypted, up from 68% and 54% in the two years prior. While the data encryption rate trends upwards, the percentage of attacks stopped before data was encrypted continues to go down, with just one in four attacks (26%) being stopped before data was encrypted.



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

Even though the sector's ability to stop data encryption has declined over the years, globally, retail performed better than many other sectors. Across all sectors, 76% of attacks resulted in data encryption, and only 21% were stopped before data was encrypted. The highest frequency of data encryption (92%) was reported by business and professional services.

In 21% of attacks in retail where data was encrypted, 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.

21%
of ransomware attacks on retail 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=174/36

Data Recovery Rate in Retail

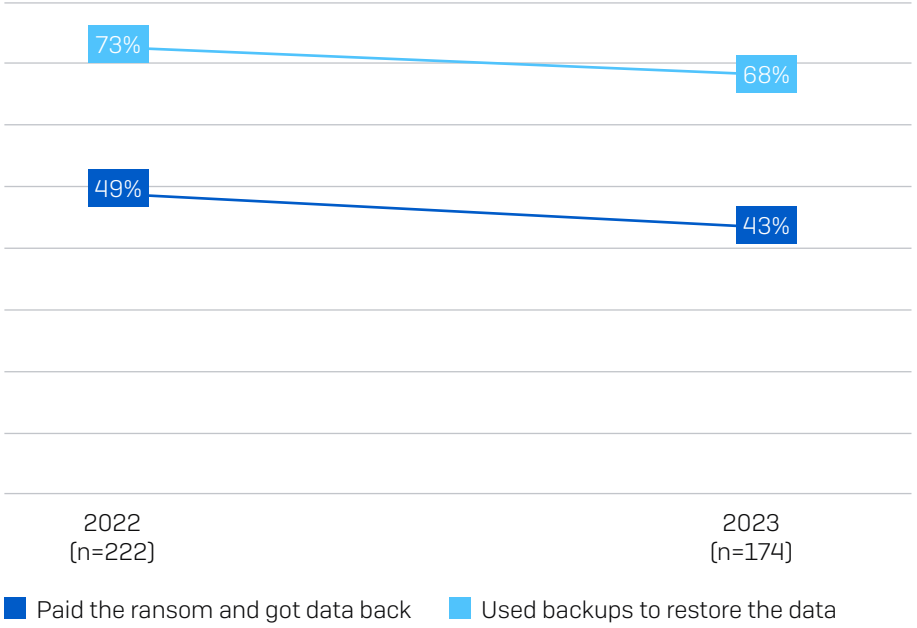
Where data was encrypted, the good news is that 97% of retail organizations got their data back, which is the same as the global average.

43% of retail organizations reported paying the ransom to recover encrypted data, while over two-thirds (68%) relied on backups for data recovery, slightly lower than the global averages of 46% and 70%, respectively. 16% of respondents reported using multiple means to recover encrypted data.

	RETAIL	CROSS-SECTOR AVERAGE
Got data back	**97%**	**97%**
Used backups to restore data	**68%**	**70%**
Paid the ransom to get data back	**43%**	**46%**
Used other means to get data back	**3%**	**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=174 (retail)

Concerningly, the use of backups in retail decreased to 68% in the 2023 survey from 73% in the 2022 survey. This decline in backup use aligns with the global trend that saw a dip to 70% in the 2023 report from 73% in the 2022 report. In terms of the rate of ransom payment, retail saw a drop in the 2023 report to 43% from 49% in the 2022 report, whereas, globally, across all sectors, the ransom payment rate remained level.



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 in retail was 97%, the recovery rate differed based on insurance coverage, with 99% of retail organizations with a standalone policy getting all their data back compared to 94% with cyber as part of a wider insurance policy. This dropped to 90% for those with no policy. However, the number of retail respondents without a cyber policy was only 10, so it should merely be considered indicative.

Percentage of ransomware victims in retail that recovered encrypted data

Did your organization get any data back? n=174 retail organizations that were hit by ransomware in the last year and had data encrypted [114 with standalone cyber policy, 50 with cyber as part of wider policy, 10 with no cyber policy].

*Retail with no cyber policy has low base numbers, so the findings should be considered indicative.

While insurance coverage has a limited impact on retail organizations' abilities to recover encrypted data, it has a much greater impact on the propensity to pay the ransom. 49% of retail organizations with a standalone cyber policy paid the ransom compared to 36% with a wider insurance policy that also covers cyber, and only 10% for those organizations without cyber coverage.

Impact of insurance on propensity to pay ransom in retail

Did your organization get any data back? Yes, we paid the ransom and got data back. n=174 retail organizations that were hit by ransomware in the last year and had data encrypted [114 with standalone cyber policy, 50 with cyber as part of wider policy, 10 with no cyber policy].

*Retail with no cyber policy has low base numbers, so the findings should be considered indicative.

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.

Aligning with the global trend, the average (mean) ransom payment by retail ($2,458,481) increased considerably year over year, coming in more than 10X higher than in our 2022 report ($226,044).

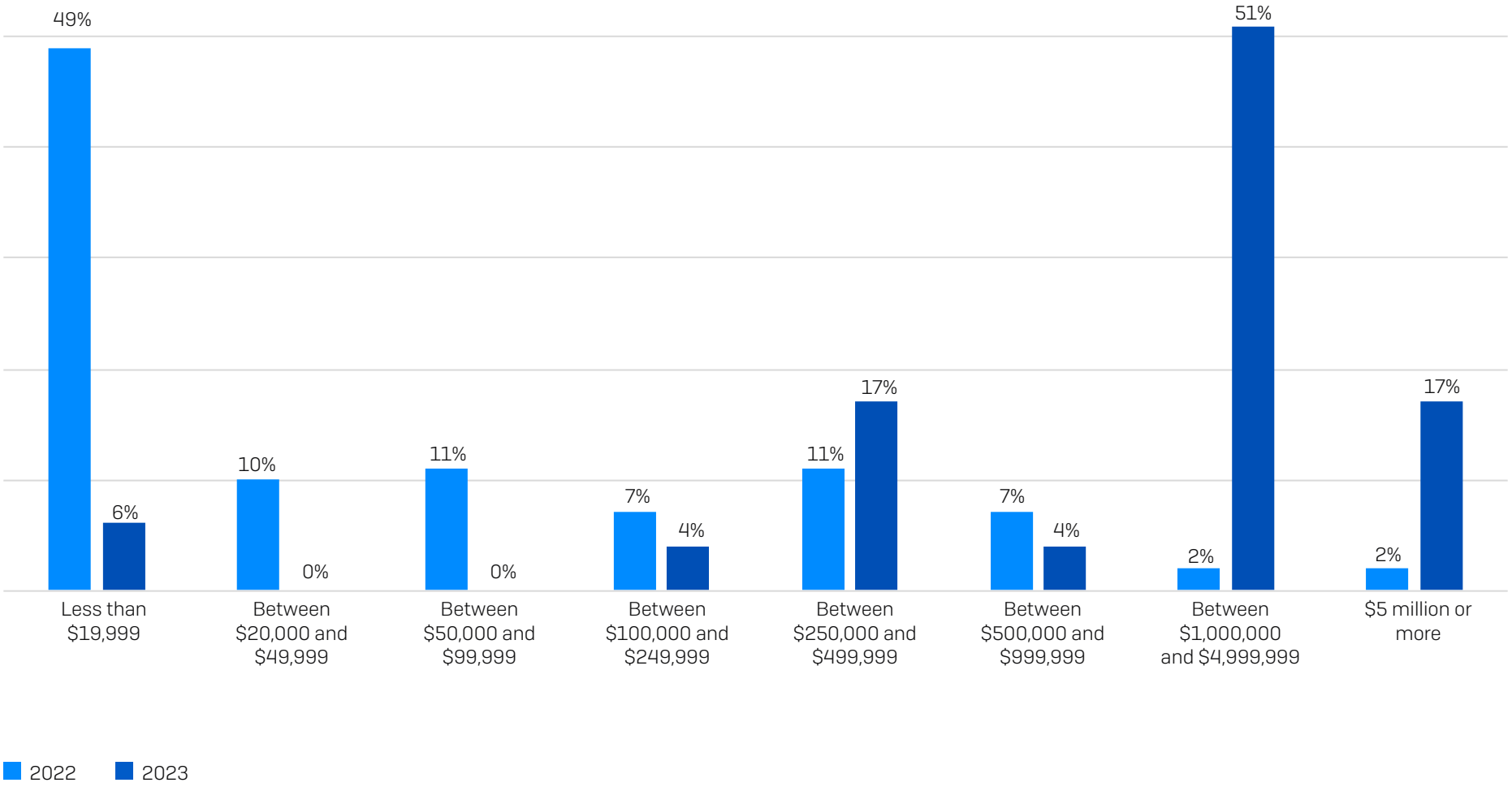
Not only is retail paying more ransom than last year, but it's also paying more than many other sectors: the mean ransom payments by retail were nearly 60% higher than the global cross-sector average ($1,542,330) in this year's study.

The proportion of retail organizations paying higher ransoms has increased from our 2022 study, with over two-thirds of retail organizations (68%) reporting payments of $1 million or more compared to 5% (with rounding) the year prior. Conversely, 6% paid less than $100,000, down from 70% in last year's report.

	2022	2023
Cross-sector Average	$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)
Retail	$226,044 (mean) $20,000 (median)	$2,458,481 (mean) $3,000,000 (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); Retail: n=47 (2023)/ 88 (2022).

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=47 (2023)/ 88 (2022).

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, globally, organizations reported an estimated mean cost to recover from ransomware attacks of $1.82 million, 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 report.

Aligning with the global trend, the recovery costs for retail have increased to $1.85M from $1.27M year over year but is still lower than the $1.97M reported in the 2021 report. The increase in recovery costs in retail this year is likely impacted by the sector's challenges when trying to stop data encryption following attacks. Furthermore, this sector's decreased use of backups to recover encrypted data has likely resulted in increased recovery costs.

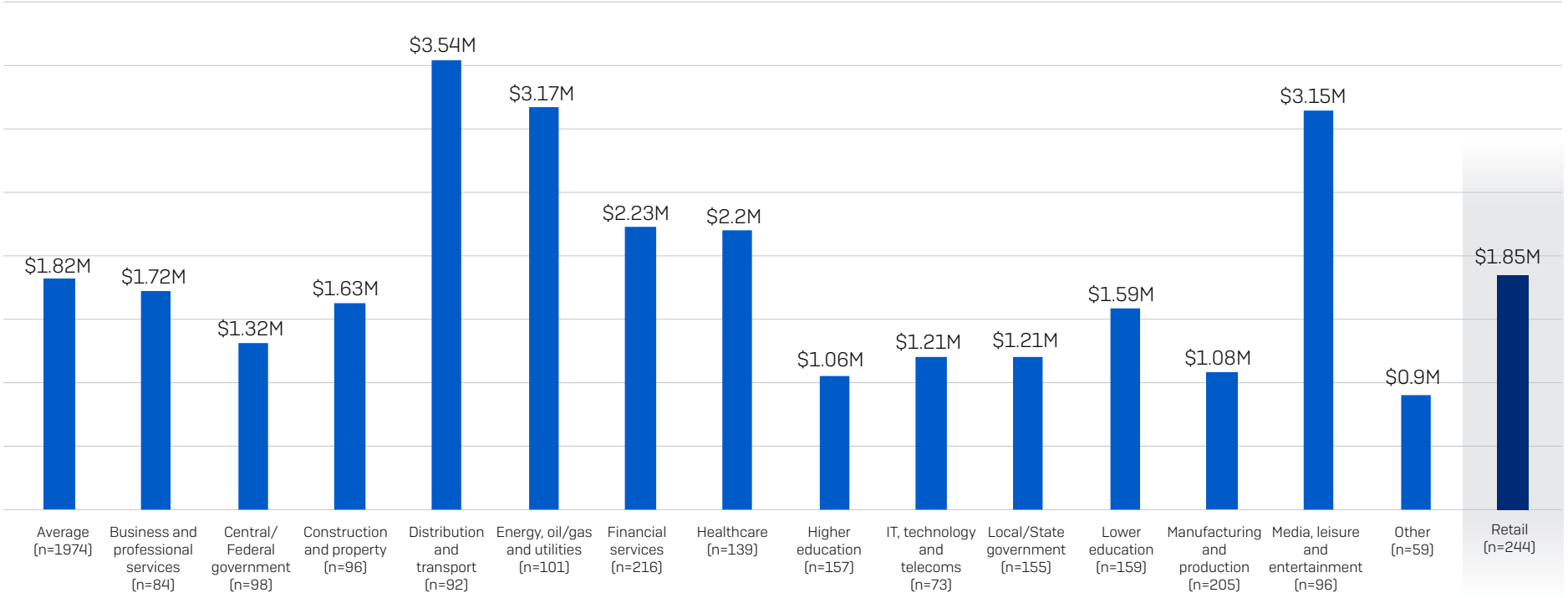
	2021	2022	2023
Cross-sector Average	$1.85M	$1.4M	$1.82M
Retail	$1.97M	$1.27M	$1.85M

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); Retail: n=244 (2023)/ 325 (2022)/ 193 (2021)

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

Recovery costs in retail organizations were slightly higher than the global average of $1.82M. Across sectors, distribution and transport paid the highest recovery costs ($3.54), which is almost double what organizations in most other industries 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 survey confirms that backups are less expensive than paying a ransom to recover encrypted data.

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.

Retail intensifies this point: the median recovery cost for those that used backups ($750,000) was just one-quarter of the bill incurred by those that paid the ransom ($3,000,000). The mean recovery cost with backups ($1.97M) was much less than the mean recovery cost when paying the ransom ($2.83M).

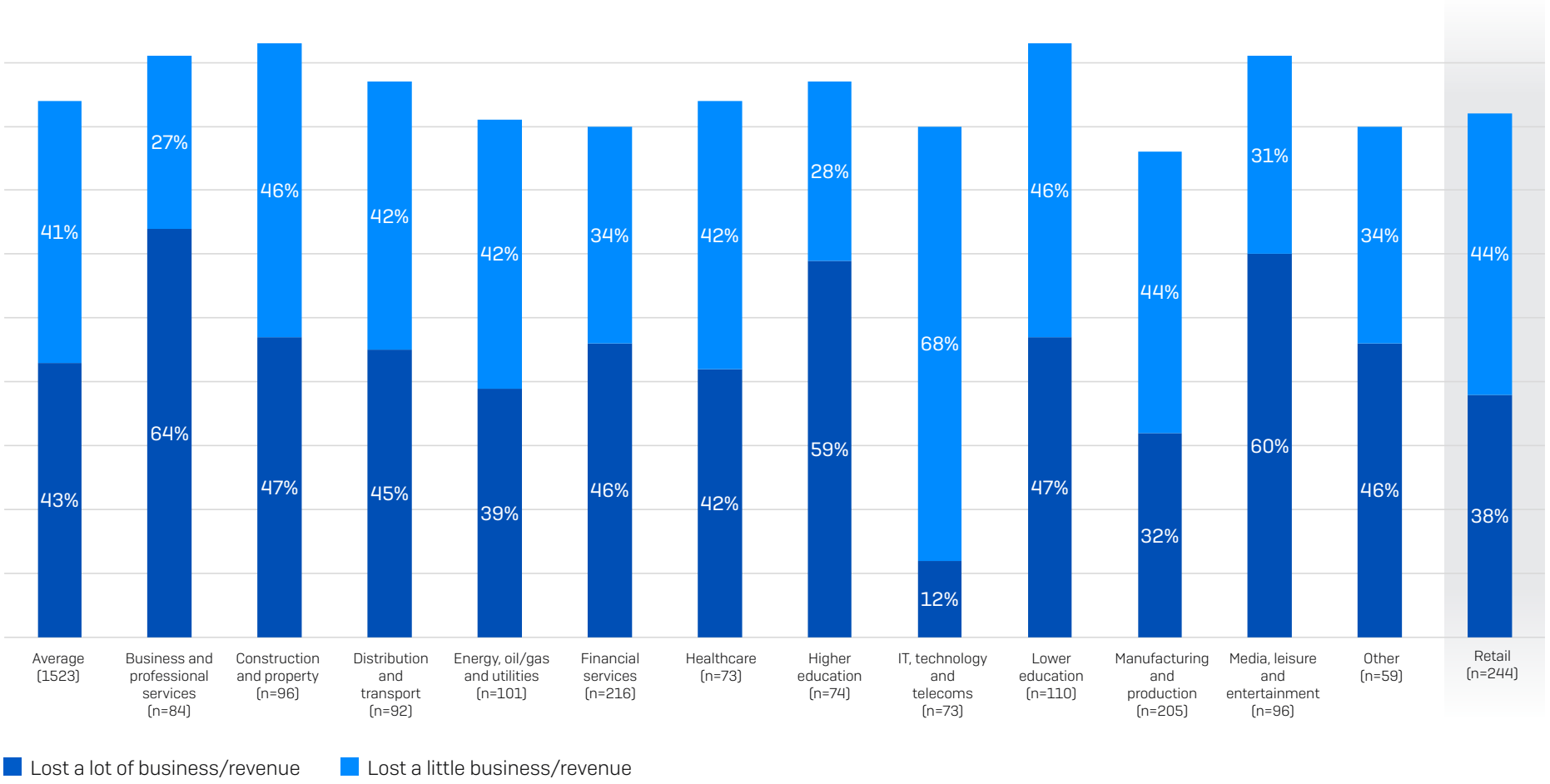
	Paid the ransom and got data back	Used backups to restore data
Cross-sector Average	**$750,000** median **$2.6M** mean	**$375,000** median **$1.62M** mean
Retail	**$3,000,000** median **$2.83M** mean	**$750,000** median **$1.97M** mean

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;

Retail: n=75 that paid the ransom and got data back and 118 that used backups to restore the data.

Business Impact

82% of retail organizations hit by ransomware said the attacks caused them to lose business/ revenue, which is in line with 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 had the highest percentage (64%) reporting that they lost a lot of business/revenue. Conversely, the manufacturing and production sector was least likely to report a business/revenue impact.

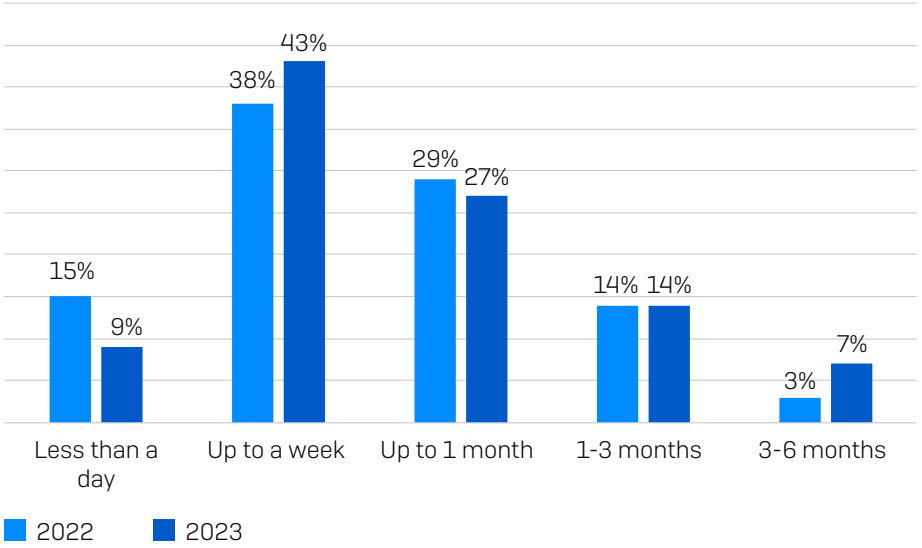


Did the ransomware attack cause your organization to lose business/revenue? Yes, we lost a lot of business/ revenue, Yes, we lost a little business/ revenue.
Private sector organizations that were hit by ransomware, base numbers in chart

Recovery Time

While the time to recover from ransomware attacks in retail is broadly in line with the 2022 report's findings, the percentage that recovers in less than a day has dropped from 15% to 9% year over year.

The percentage of organizations that took more than a month to recover increased to 21% (with rounding) from 17% (with rounding) year over year, suggesting that recovery is now taking longer for this sector.



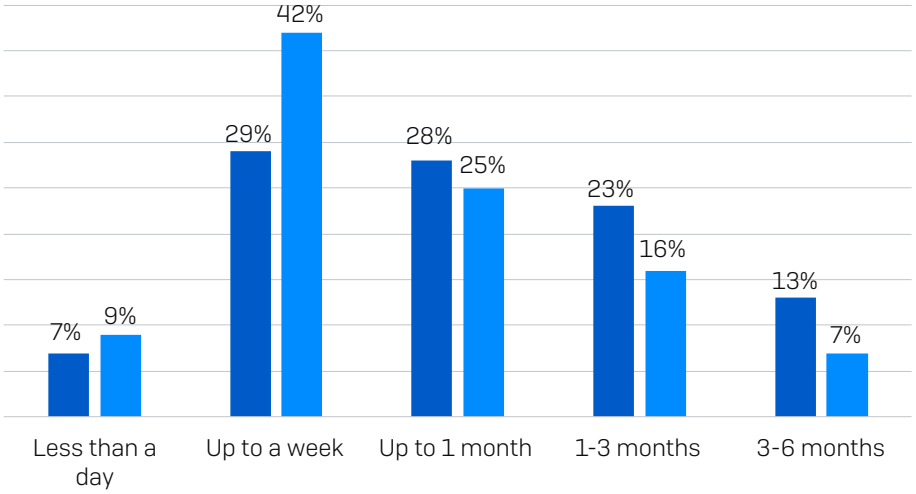
How long did it take your organization to fully recover from the ransomware attack? 244 (in 2023) /325 (in 2022) retail organizations that were hit by ransomware.

Recovery time by data recovery method

The research reveals that retail organizations that use backups to recover their data recover from attacks more quickly than those that pay the ransom. 52% of those that used backups recovered within a week, compared with 36% of those that paid the ransom.

23% of retail organizations that used backups took more than a month to recover compared with over a third (36%) 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.



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 continues to be a major threat to retail organizations. 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: nearly three-quarters of retail organizations (71%) hit by ransomware had their data encrypted. In addition, 21% reported that their encrypted data was also stolen.

Concerningly, the use of backups to recover encrypted data in retail decreased from 73% to 68% year over year. More encouragingly, the rate of ransom payments in retail has dropped to 43% from 49% year over year. All said, the good news is that 97% of retail organizations that had data encrypted were able to recover data after an attack, in line with the global average.

Unlike other sectors, insurance coverage had only a small impact on the data recovery rate in retail. However, it did have a considerable impact on the propensity to pay the ransom. In short, retail organizations 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 or for those without a policy.

The ransomware recovery cost for retail has increased to $1.85M from $1.27M year over year, likely impacted by the sector's challenges with stopping data encryption following attacks and the decline in the use of backups to recover encrypted data.

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

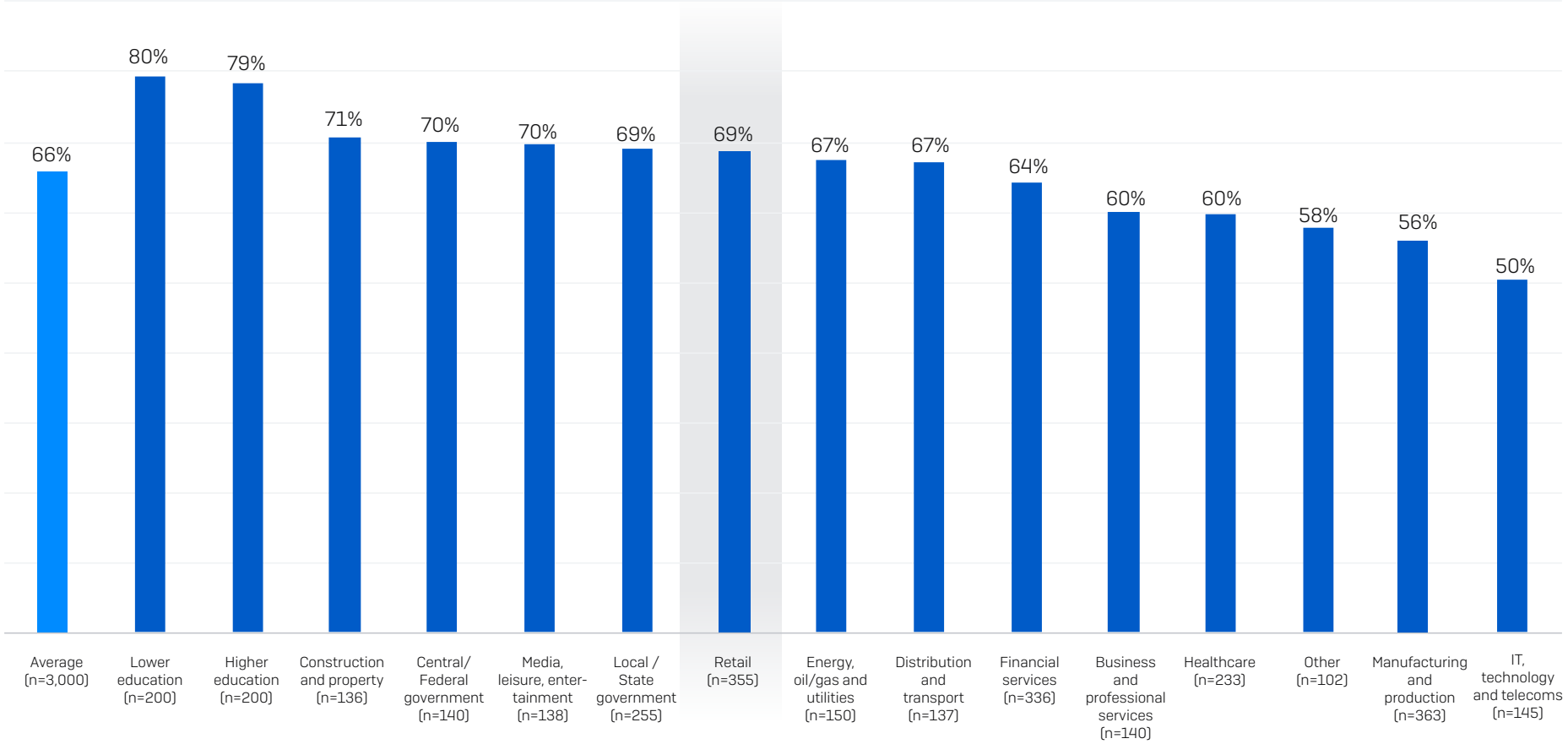
Organizations should focus on:

- 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

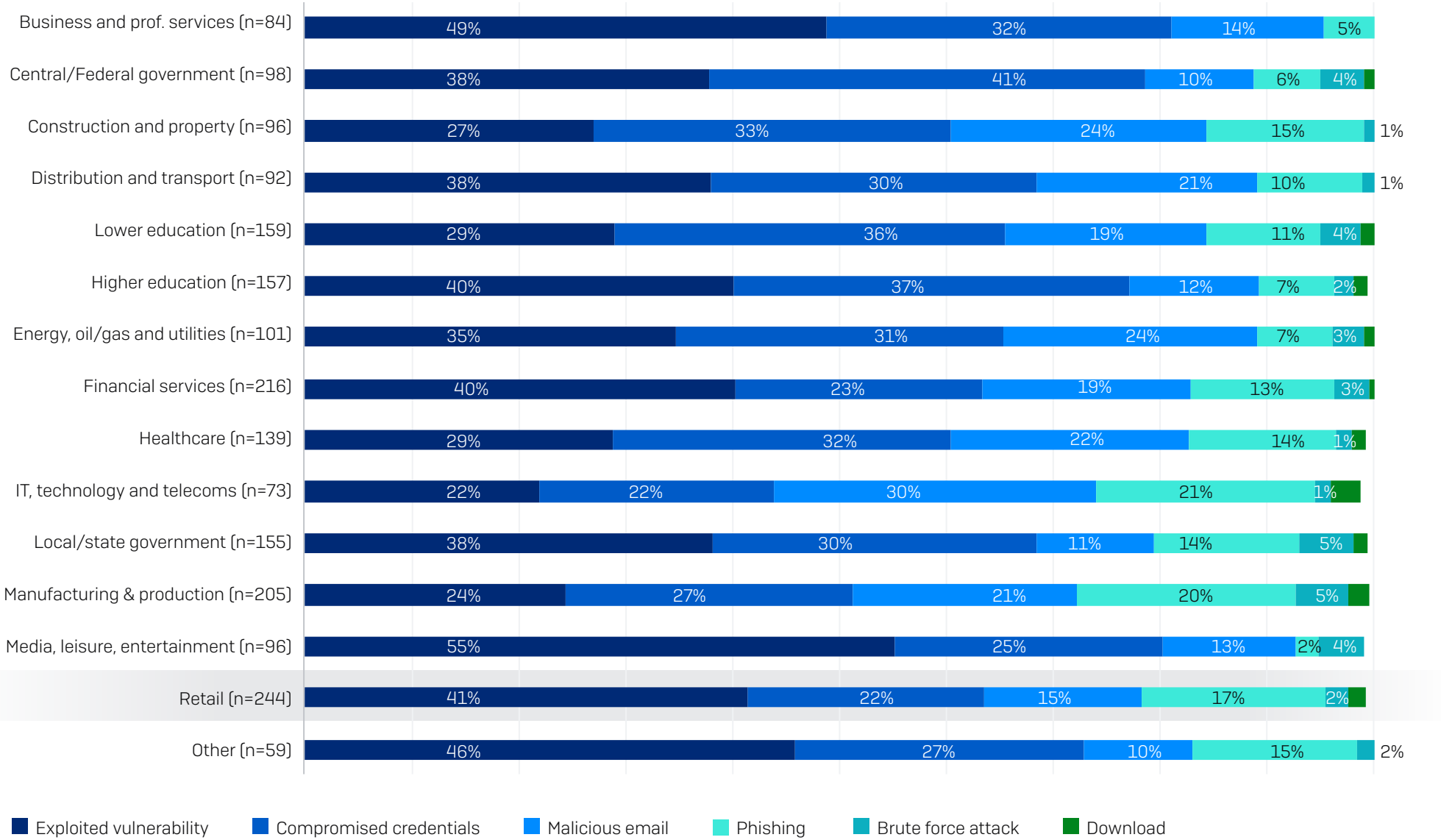
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



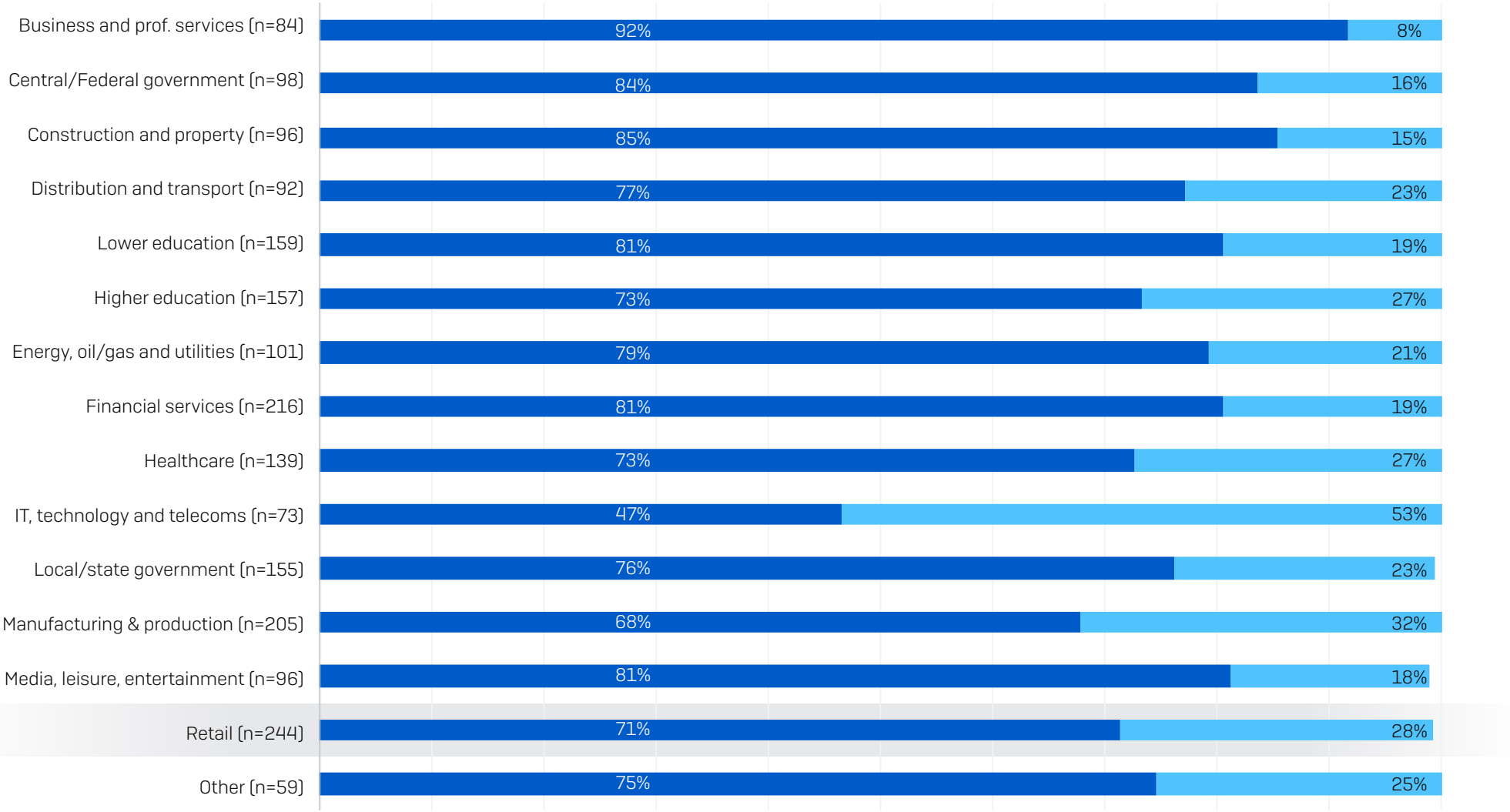
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



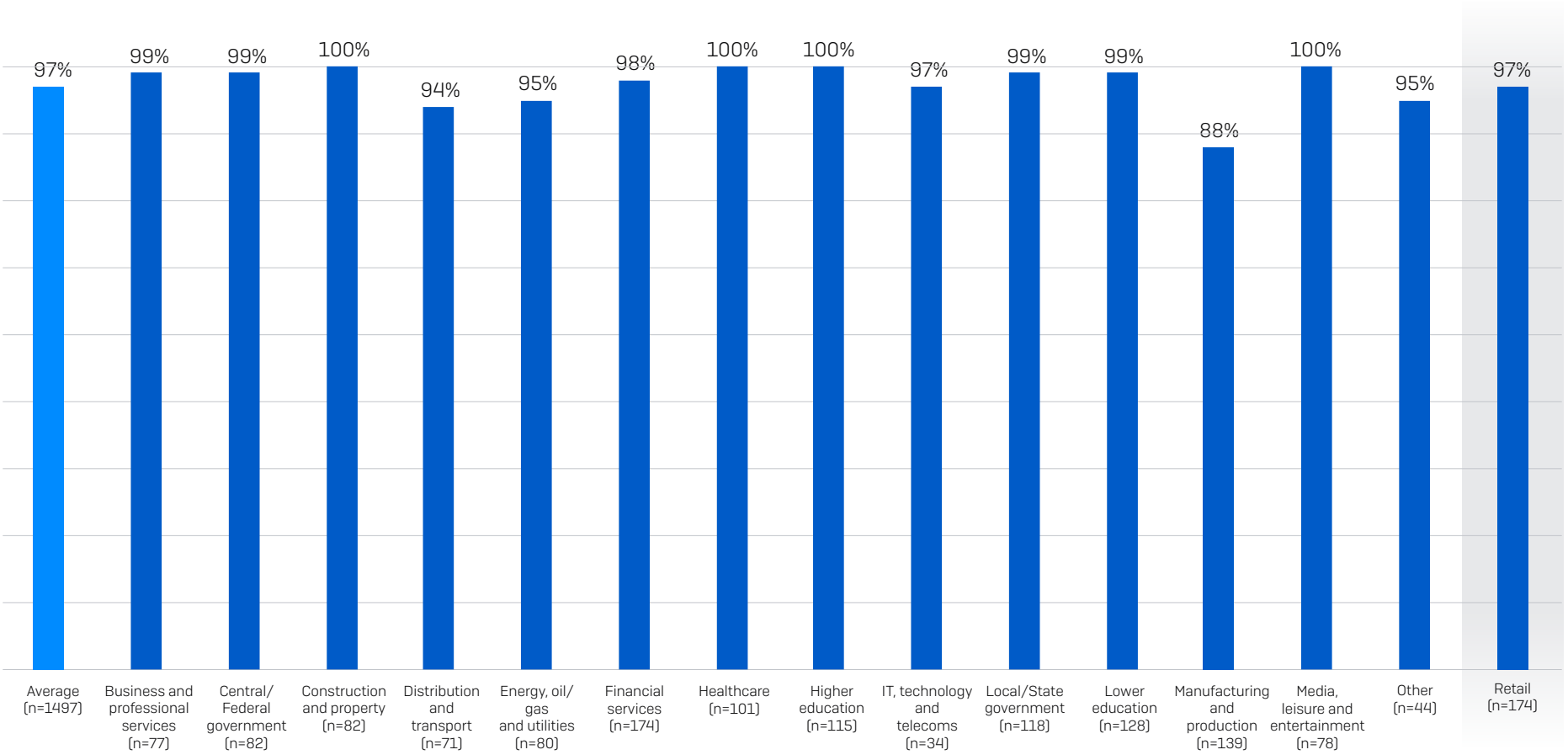
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



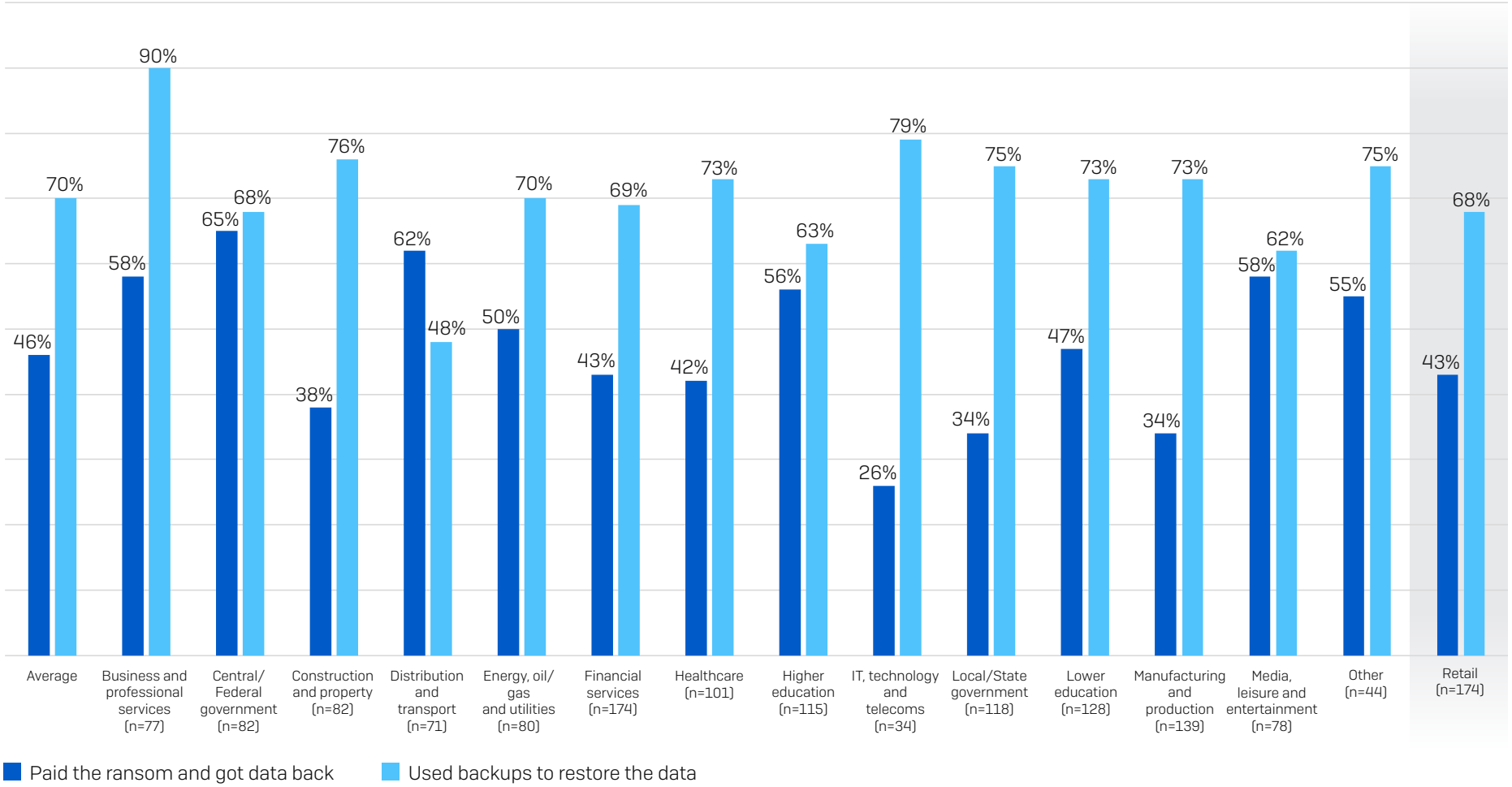
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

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

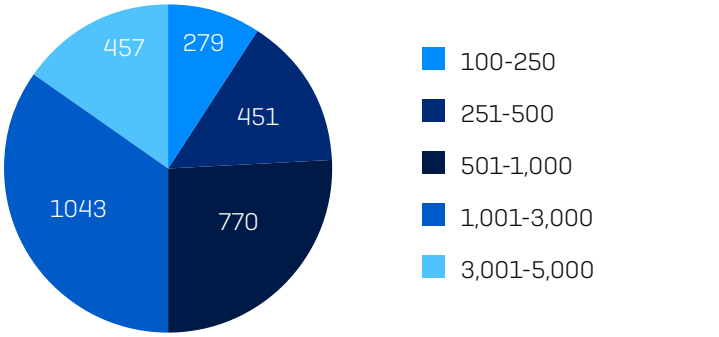
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

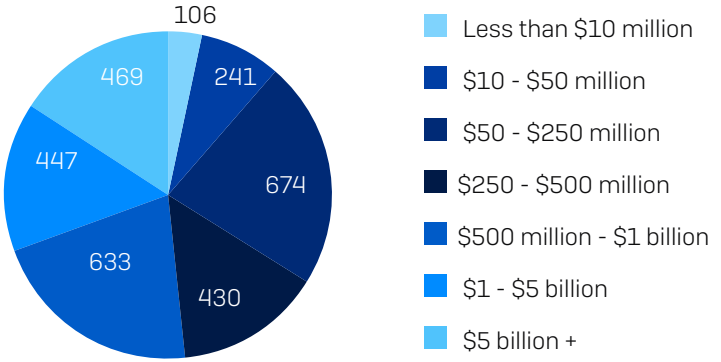
Respondents by Country

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.

2023-06-20 (WP-NP)

SOPHOS