SOPHOS

The State of Ransomware in Financial Services 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 336 from the financial services sector, conducted in January-March 2023.

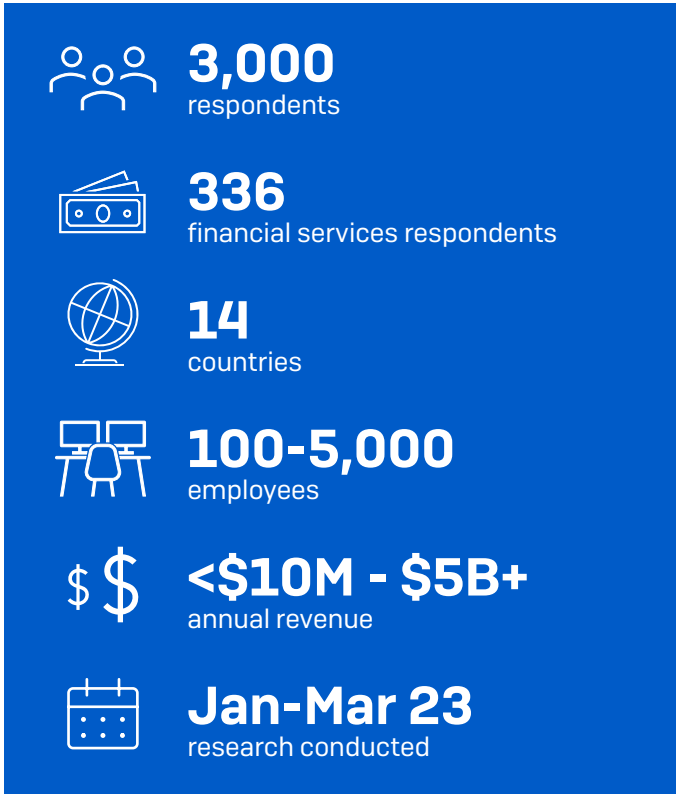
A Sophos Whitepaper. July 2023

Introduction

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

About the Survey

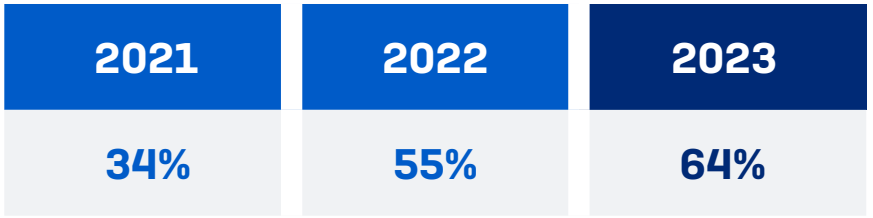
Sophos commissioned an independent, vendor-agnostic survey of 3,000 IT/cybersecurity leaders in organizations with between 100 and 5,000 employees, including 336 in financial services, across 14 countries in the Americas, EMEA, and Asia Pacific. The survey was conducted between January and March 2023, and respondents were asked to respond based on their experiences over the previous year.



Rate of Ransomware Attacks in Financial Services

The 2023 study revealed that the rate of ransomware attacks in financial services grew from 55% in 2022 to 64% in 2023. This increase in the rate of ransomware attacks makes clear that adversaries are able to execute attacks at scale consistently, making ransomware arguably the biggest cyber risk facing financial services 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=336 (2023), 444 (2022), 550 (2021)

The rising rate of ransomware attacks in financial services is in contrast to the global cross-sector trend, which has remained flat: 66% of all 2023 respondents reported that their organization was hit by ransomware, the same as in our 2022 survey.

Although financial services reported an increase in attack rate, the sector remains below the cross-sector 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 Financial Services

Exploited vulnerabilities (40%) were the most common root cause of the most significant ransomware attacks in the financial services sector, followed by compromised credentials (23%). Overall, one-third of financial services organizations (33%) said email (malicious emails or phishing) was the root cause of the attack, in line with the cross-sector average of 30%.

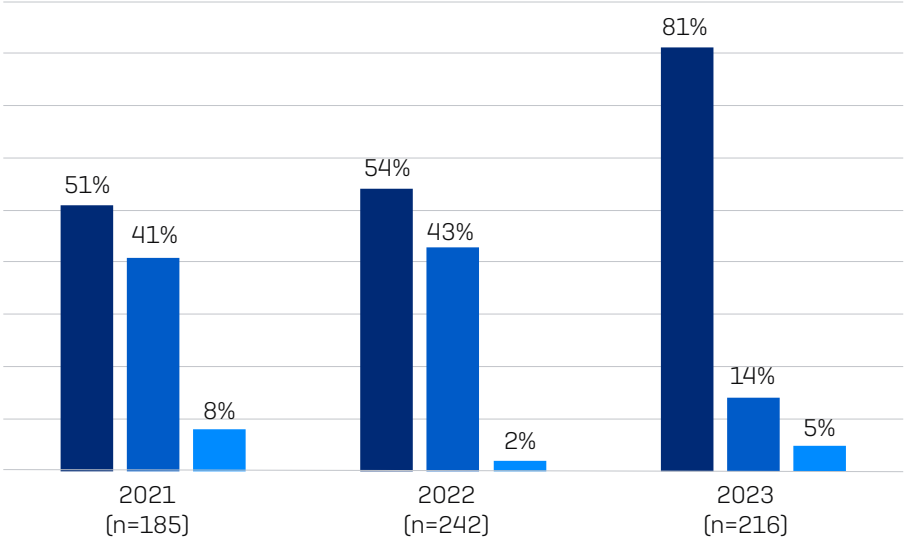
Across all the sectors surveyed, financial services was among the most likely to report exploited vulnerabilities as the root cause of attack. At the same time, the rate of compromised credentials abuse was lower than in many other sectors.

	FINANCIAL SERVICES (N=216)	CROSS-SECTOR AVERAGE (n=1,974)
EXPLOITED VULNERABILITY	40%	36%
COMPROMISED CREDENTIALS	23%	29%
MALICIOUS EMAIL	19%	18%
PHISHING	13%	13%
BRUTE FORCE ATTACK	3%	3%
DOWNLOAD	0%	1%

Rate of Data Encryption in Financial Services

Data encryption in the financial services sector has continued to rise, with the 2023 report revealing the highest encryption level in three years: four out of five financial services organizations (81%) stated that their data was encrypted, a 50% rise over the 2022 report when 54% of financial services organizations reported data encryption. This likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

Concerningly, just over one in ten attacks (14%) were stopped before the data was encrypted, the second lowest rate across all sectors and a decrease of 67% over last year's report. The rate of extortion-only attacks in financial services (5%) more than doubled in the last year, although it remains below the 2021 report's rate of 8%.



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

Globally, financial services was one of the sectors that reported the highest data encryption rates, and only 14% of organizations were able to stop the attack before data was encrypted.

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.

In a quarter of attacks in financial services where data was encrypted (25%), 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.

25%
Of ransomware attacks on financial services 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=174/43

Data Recovery Rate in Financial Services

Where data was encrypted, the good news is that 98% of financial services organizations got their data back, slightly above the 97% cross-sector average.

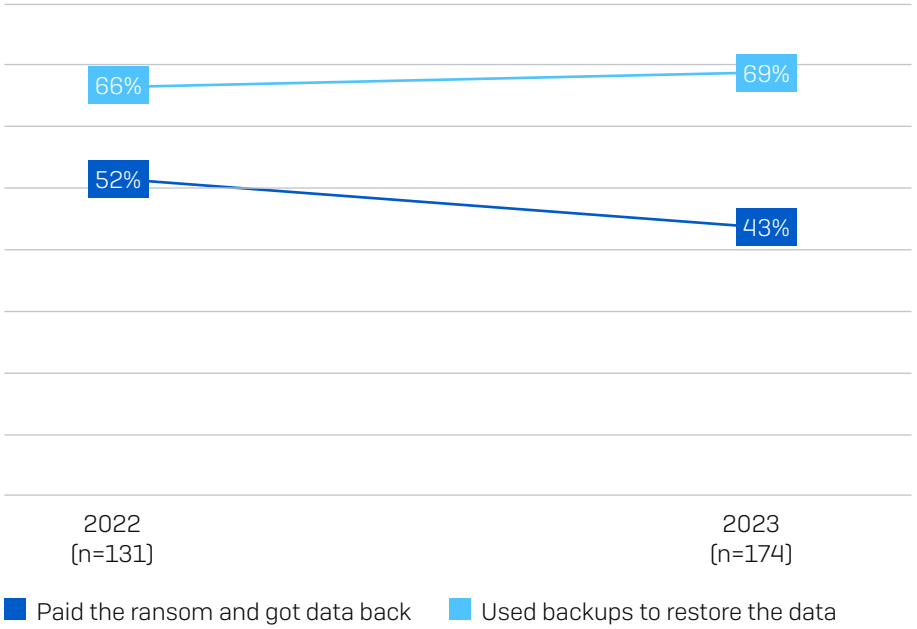
43% of financial services organizations paid the ransom to recover their encrypted data, while over two-thirds (69%) used backups for data recovery, slightly lower than the global averages of 46% and 70%, respectively. 16% of respondents working in financial services reported using multiple means to recover encrypted data.

	FINANCIAL SERVICES	CROSS-SECTOR AVERAGE
Got data back	98%	97%
Used backups to restore data	69%	70%
Paid the ransom to get data back	43%	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=174 (financial services)

In more good news, the rate of ransom payments in financial services is down from 52% in our 2022 study, while the use of backups to restore data has increased (from 66% in the 2022 report to 69% in this year's report).

Globally, the rate of ransom payments remained flat, while the use of backups dropped to 70% in the 2023 report, down from 73% in the 2022 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 Data Recovery

While the overall rate of data recovery in financial services was 98%, the recovery rate differed based on insurance coverage. 99% of financial services organizations with a standalone policy got data back, along with 97% of those with cyber coverage as part of a wider insurance policy. However, the data recovery rate dropped to 89% for those with no policy. It's important to note that only nine financial services respondents said their organization did not have cyber coverage, so this data point should be considered indicative only.

Percentage of ransomware victims in financial services that recovered encrypted data

Did your organization get any data back? n=174 financial services organizations that were hit by ransomware in the last year and had data encrypted [99 with standalone cyber policy, 66 with cyber as part of a wider policy, 9 with no cyber policy]

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

While insurance coverage has a small impact on financial services organizations' abilities to recover encrypted data, it has a much greater impact on the propensity to pay the ransom. 59% of financial services organizations with a standalone cyber policy paid the ransom compared to 24% with a wider insurance policy that also covers cyber, and only 11% for those organizations without cyber coverage.

Impact of Insurance on Ransom Payment in Financial Services

Did your organization get any data back? Yes, we paid the ransom and got the data back. n=174 financial services organizations that were hit by ransomware in the last year and had data encrypted [99 with standalone cyber policy, 66 with cyber as part of a wider policy, 9 with no cyber policy]

*Financial services 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.

18 financial services organizations shared the ransom amounts paid. Amplifying the global trend, the average (mean) ransom payment by financial services in the 2023 report ($1,683,472) was 6X higher than in the previous year's report ($272,655). Overall, the mean ransom payment by financial services in the 2023 report exceeded the cross-sector average by more than $100,000. This suggests that the financial services sector not only paid considerably higher ransom amounts compared to the prior year, but it also paid higher ransoms than many other sectors in this year's survey. However, given the low number of respondents in the financial services sector, the sector findings should be considered indicative.

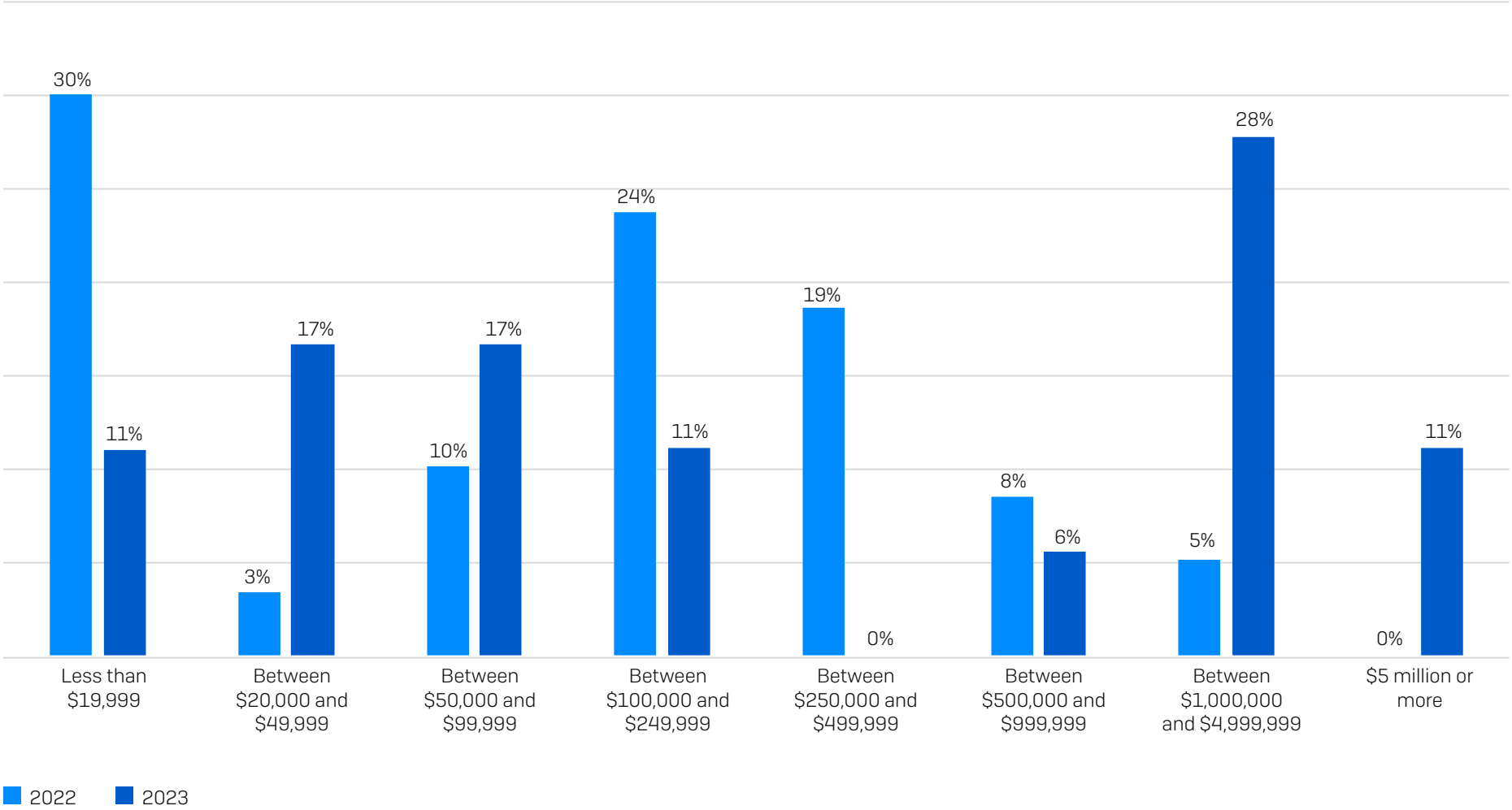
	2022	2023
Cross-sector Average	$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)
Financial Services	$272,655 (mean) $120,000 (median)	$1,683,472 (mean) $109,000 (median)

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); Financial services: n=18 (2023)/ 59 (2022).

* Financial services in the 2023 study have low base numbers, so the findings should be considered indicative.

The proportion of financial services organizations paying higher ransoms has increased, with almost 39% paying a ransom of $1M or more in our 2023 study compared to just 5% in the year before. At the same time, the percentage of financial services organizations that paid less than $100,000 remained in line with last year's report, coming in at around 40%.

Ransom Payments by Financial Services: 2023 vs 2022



How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses. n=18 (2023)/ 59 (2022).

*Response base for 2023 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. 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 this global trend, the recovery cost for financial services has increased to $2.23M from $1.59M year over year. A likely reason for this may be a significant increase in the data encryption rates for this sector and the reduced ability to stop attacks before the data was encrypted.

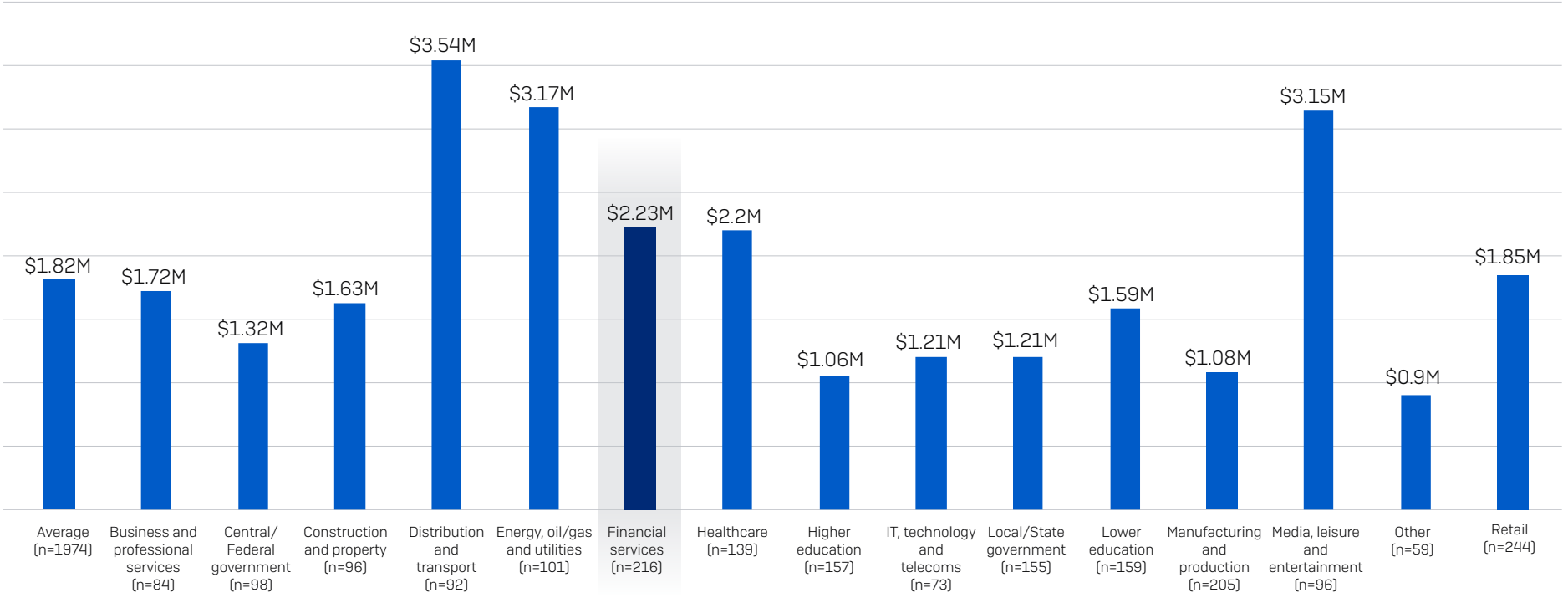
	2021	2022	2023
Cross-sector Average	$1.85M	$1.4M	$1.82M
Financial Services	$2.10M	$1.59M	$2.23M

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); Financial services: n=216 (2023)/ 242 (2022)/ 185 (2021)

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

Financial services organizations were among those who spent the most to recover from an attack, with an average recovery cost of $2.23M. In comparison, the cross-sector average was $1.82M.

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 a cheaper way to recover encrypted data than paying a ransom.

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

Financial services amplifies the global trend: the median recovery cost for those that paid the ransom was $3,000,000 vs. $375,000 for those that used backups. The mean recovery cost with backups ($1.58M) was less than half that incurred by those that paid the ransom ($4.05M).

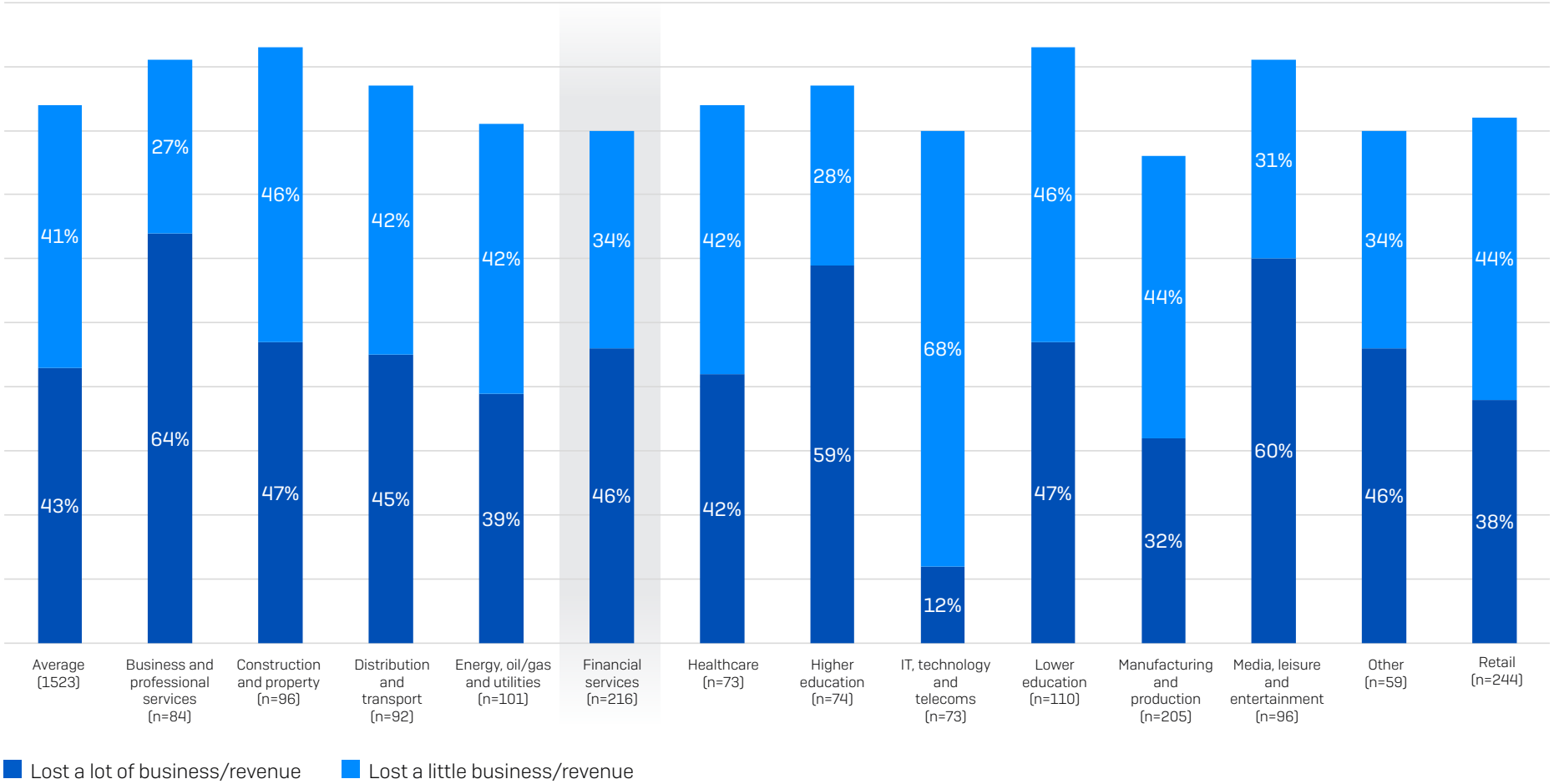
	Paid the ransom and got data back	Used backups to restore data
Cross-sector Average	**$750,000** median **$2.6M** mean	**$375,000** median **$1.62M** mean
Financial Services	**$3,000,000** median **$4.05M** mean	**$375,000** median **$1.58M** mean

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;

Financial services: n=75 that paid the ransom and got data back and 120 that used backups to restore the data.

Business Impact

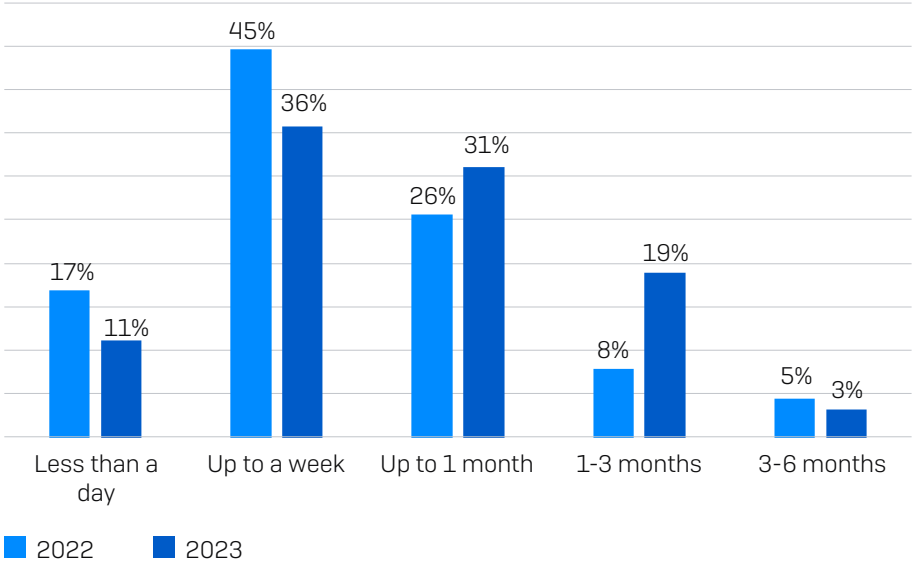
80% of financial services organizations hit by ransomware said the attack caused them to lose business/revenue, below the global cross-sector average of 84%. Lower education (94%) and construction and property (93%) were most likely to have lost some business/revenue, while business and professional 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

The percentage of financial services organizations that recover in less than a day dropped to 11% in our 2023 survey, down from 17% the year before. At the same time, the percentage of financial services organizations that took more than a month to recover has almost doubled to 22% (with rounding) compared to 13% (with rounding) year over year. This increase in recovery time is likely influenced by the increase in attacks that result in data encryption.



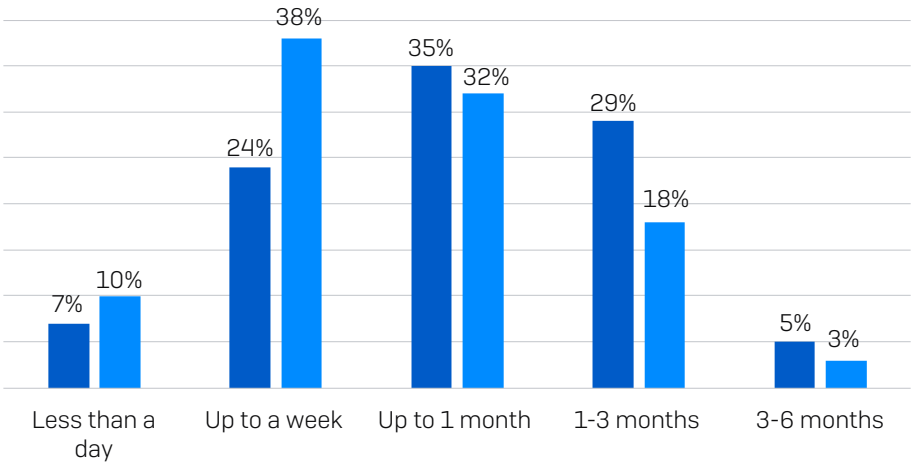
How long did it take your organization to fully recover from the ransomware attack? 216 (in 2023) /242 (in 2022) financial services organizations that were hit by ransomware.

Recovery time by data recovery method

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

10% of those that used backups recovered in less than a day, compared with 7% of those that paid the ransom. At the same time, one-fifth of the respondents (21% with rounding) that used backups took more than a month to recover data, while over one-third (35% 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 continues to be a major threat to financial services organizations, with two-thirds (64%) reporting being hit in the last year. As adversaries continue to hone their attack tactics, techniques, and procedures (TTPs), defenders are struggling to keep pace, resulting in increased encryption rates: over four in five financial service organizations (81%) hit by ransomware reported that adversaries succeeded in encrypting their data. In addition, 25% reported that their encrypted data was also stolen.

Financial services reported a drop in the propensity to pay the ransom (2023 report: 43%, 2022 report: 52%) to get encrypted data back. The use of backups for data recovery increased only slightly, up from 66% to 69%. Fortunately, 98% of those that had data encrypted were able to get at least some data back, in line with the global average of 97%.

Unlike other sectors, in financial services, cyber insurance had little impact on the rate of data recovery. However, it did have a considerable impact on the propensity to pay the ransom: financial service organizations with cyber insurance were much more likely to pay a ransom to recover data than those without a policy.

The recovery cost for financial services grew year over year to $2.23M, likely influenced by the significant increase in data encryption rates and the sector's reduced ability to stop attacks before the data was encrypted. While 80% of financial services organizations hit by ransomware reported loss of business/revenue due to attack, the sector was less impacted in this way than many other industries.

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

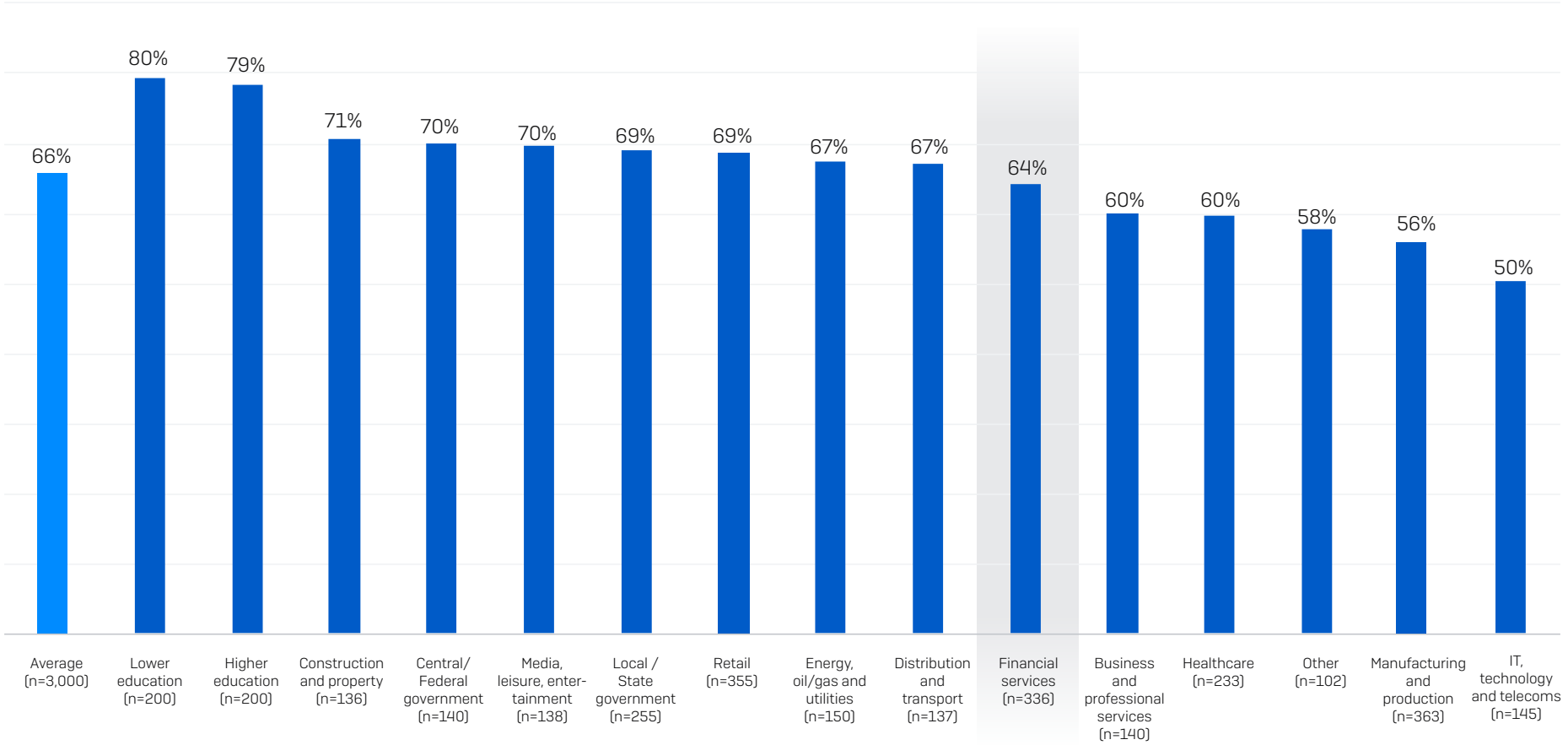
Organizations should focus on:

- 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

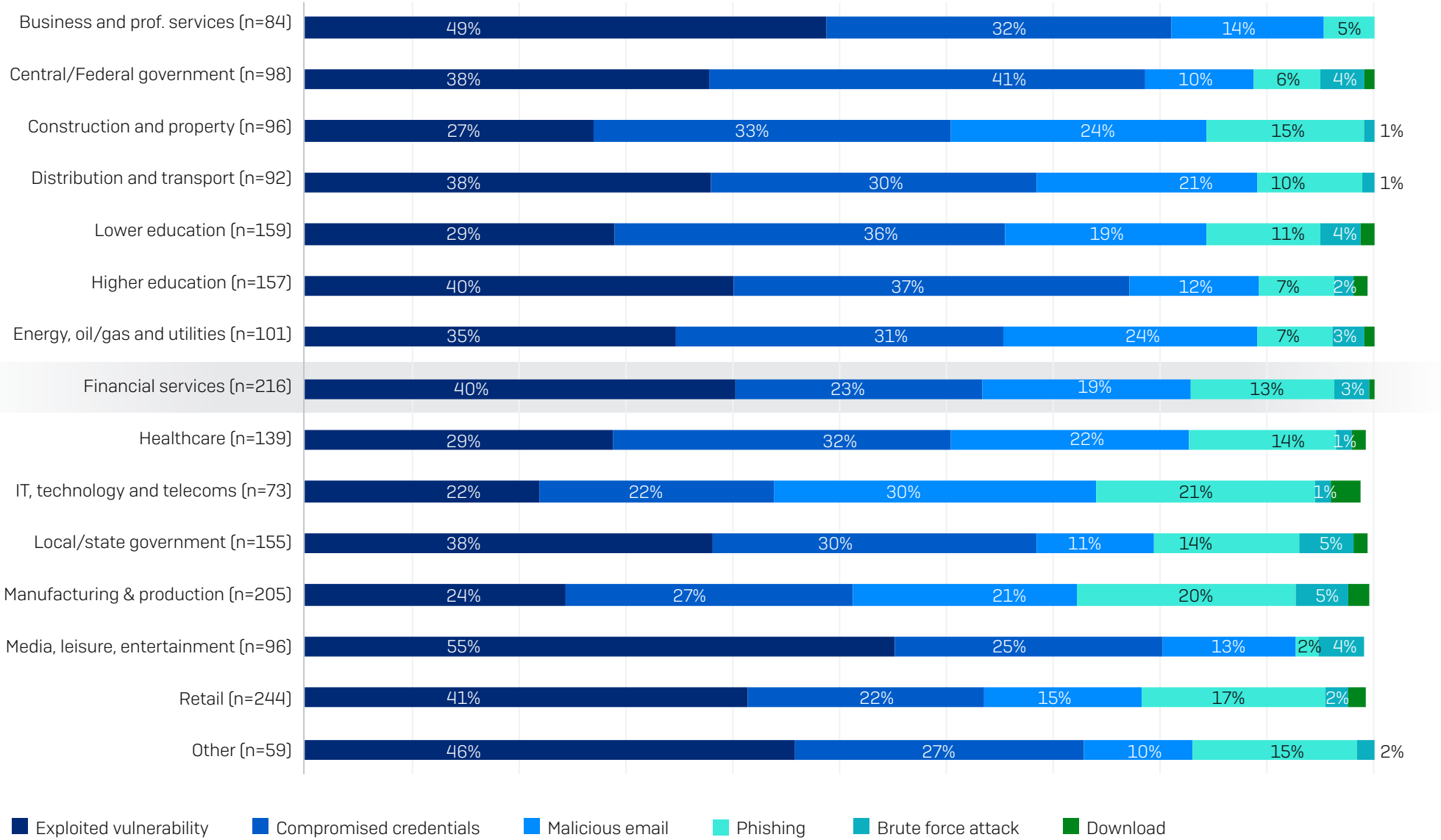
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



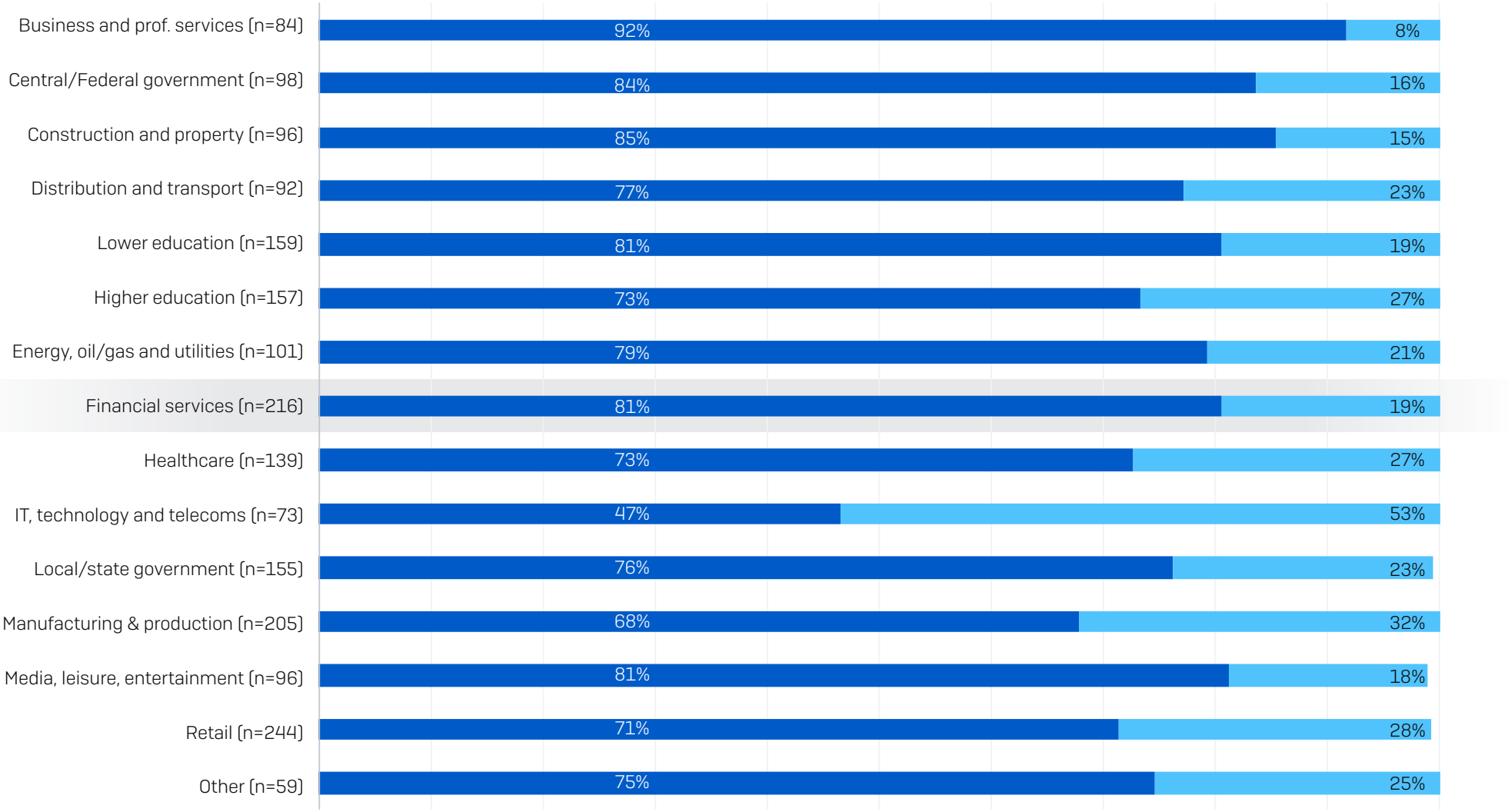
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



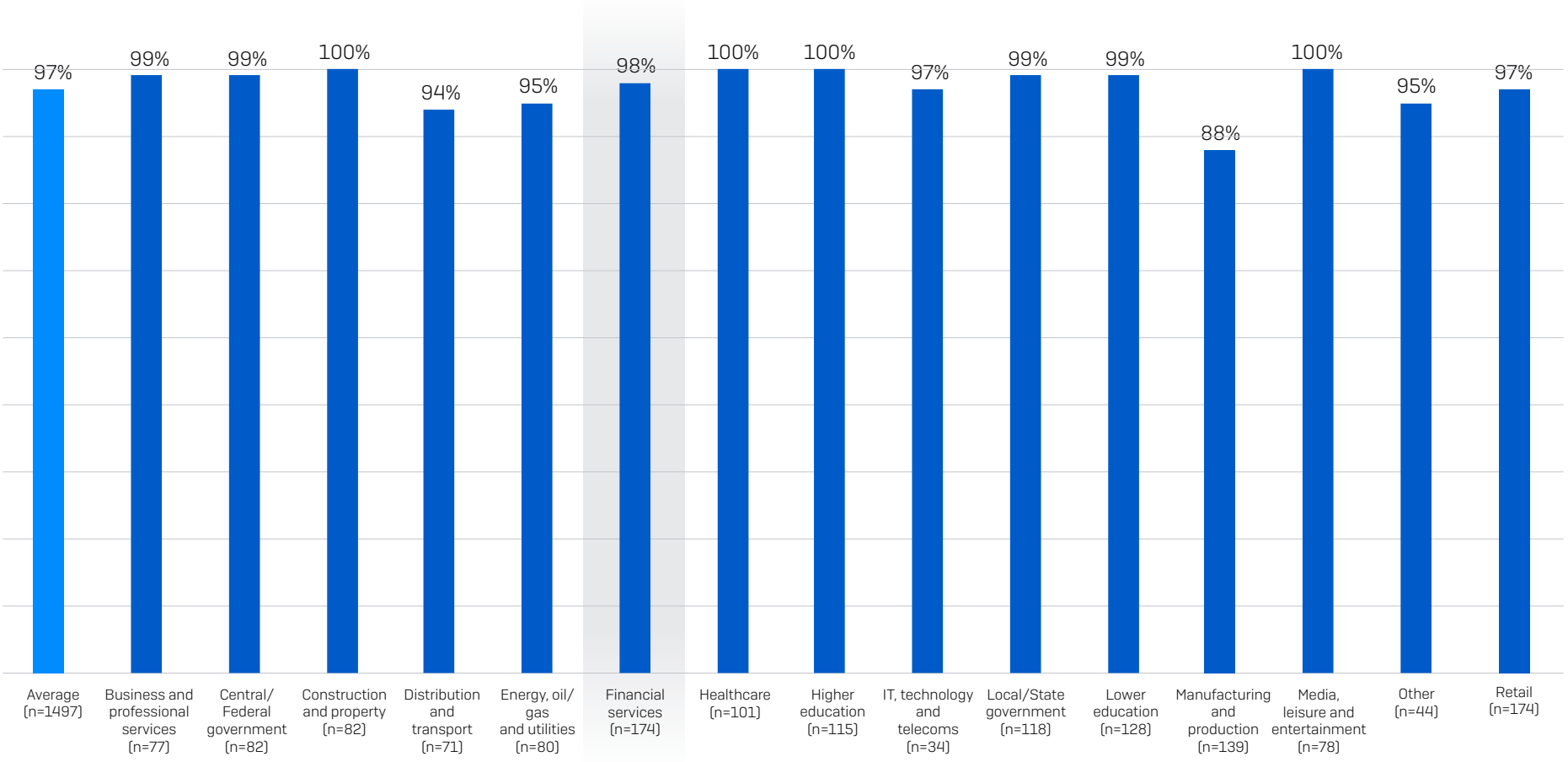
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



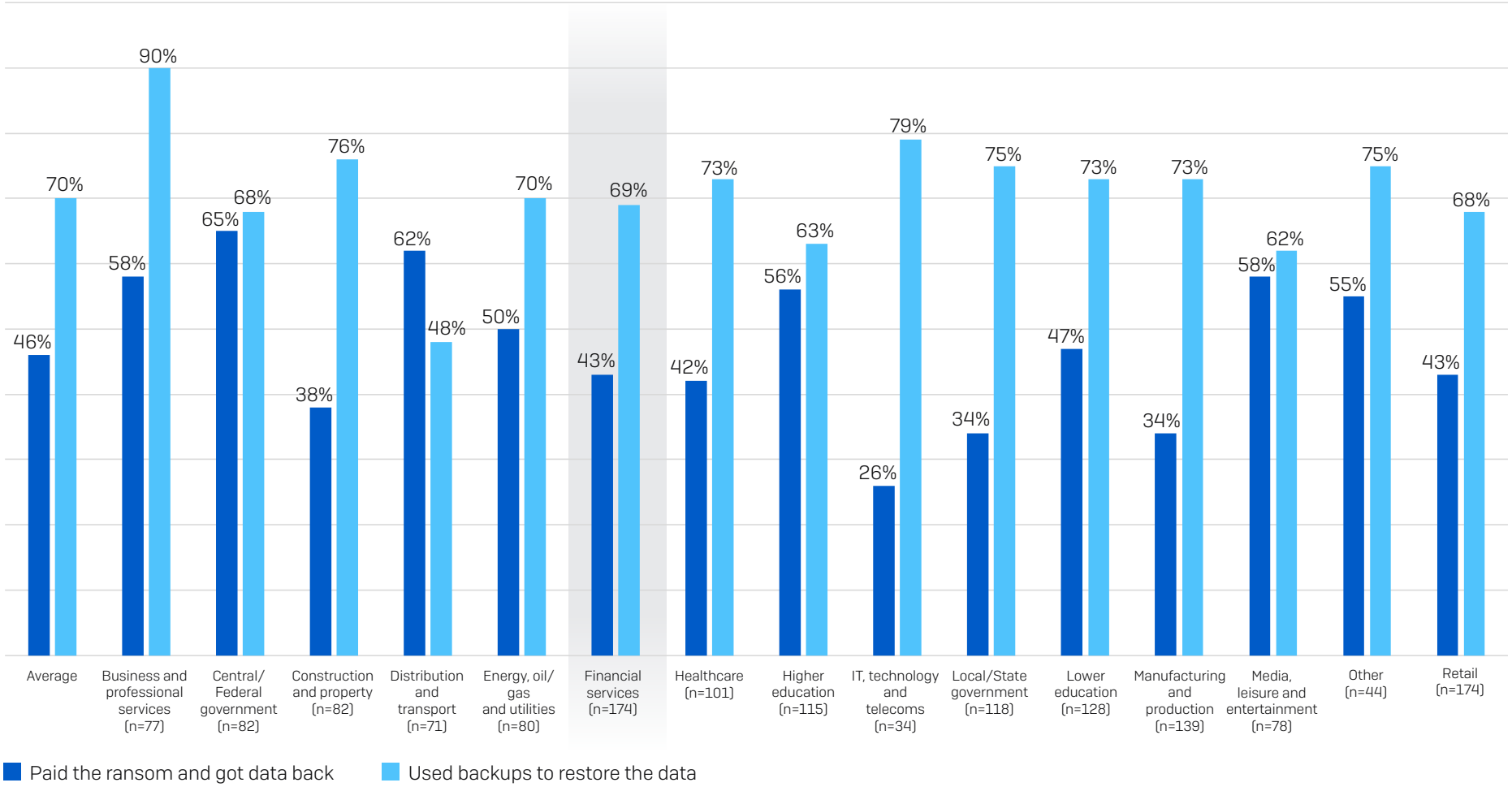
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

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

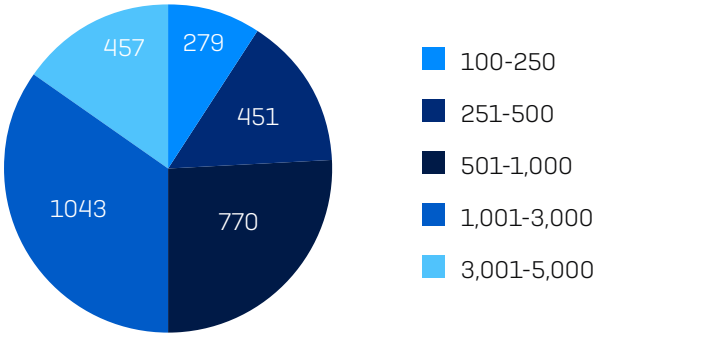
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

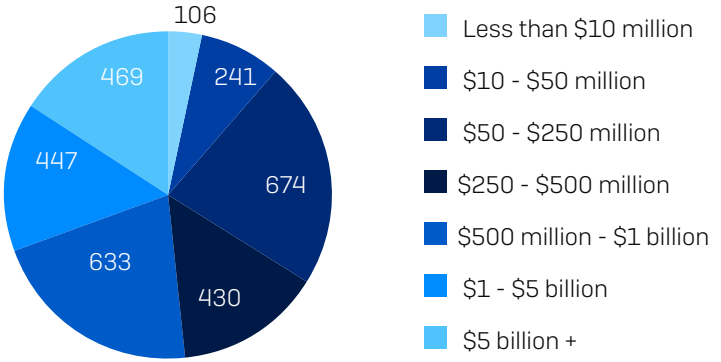
Respondents by Country

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.

2023-07-05 (WP-NP)

SOPHOS