SOPHOS

The State of Ransomware in Manufacturing and Production 2023

Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries, including 363 from the manufacturing and production sector, conducted in January-March 2023.

A Sophos Whitepaper. June 2023

Introduction

Sophos' annual study of the real-world ransomware experiences of IT/cybersecurity leaders makes clear the realities facing organizations in 2023. It reveals the most common root causes of attacks and shines new light on how experiences with ransomware differ based on industry. 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 363 in manufacturing and production, 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

363
manufacturing respondents

14
countries

100-5,000
employees

<$10M - $5B+
annual revenue

Jan-Mar 23
research conducted

Rate of Ransomware Attacks in Manufacturing

The research revealed that the rate of ransomware attacks in manufacturing and production has remained level, with 56% of respondents reporting that their organization was hit by ransomware in the previous year, compared to 55% in our 2022 survey. With adversaries now able to consistently execute attacks at scale, ransomware is arguably the biggest cyber risk facing 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 an attack. For more information on ransomware-as-a-service, read the Sophos 2023 Threat Report.

2021	2022	2023
36%	55%	56%

In the last year, has your organization been hit by ransomware? Yes. n=363 (2023), 419 (2022), 438 (2021)

The findings for the manufacturing sector are consistent with the cross-sector average in that the rate of ransomware attacks has also remained flat over the last year, with 66% of respondents reporting that their organization was hit by ransomware, the same as in our 2022 survey.

Manufacturing and production reported the second lowest rate of ransomware attacks of all sectors surveyed, with only IT, technology, and telecoms reporting a lower rate of attack (50%), suggesting higher cyber readiness and defenses in these sectors. Education was the sector most likely to be hit, with 80% in lower education and 79% in higher education reporting an attack.

Root Causes of Ransomware Attacks in Manufacturing

Compromised credentials (27%) were the most common root cause of the most significant attack reported by respondents in manufacturing and production, followed by exploited vulnerabilities (24%). For both causes, manufacturing and production reported lower rates than the global average which suggests that the sector is performing better than most others in reducing the attack surface. In comparison, exploited vulnerabilities (36%) followed by compromised credentials (29%) were the most common root causes of ransomware attacks globally.

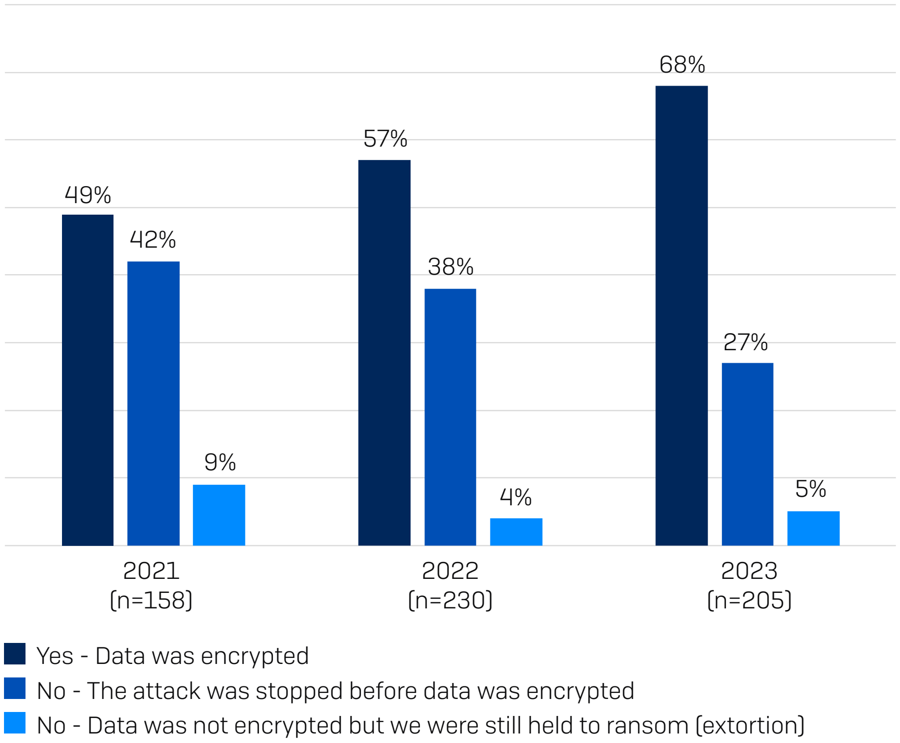
41% reported malicious emails or phishing as the root causes of attack [vs. 30% cross-sector average], indicating that manufacturing and production is particularly exposed to email-based attacks.

	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Exploited vulnerability	24%	36%
Compromised credentials	27%	29%
Malicious email	21%	18%
Phishing	20%	13%
Brute force attack	5%	3%
Download	2%	1%

Rate of Data Encryption in Manufacturing

Data encryption in the manufacturing and production sector has continued to rise, with the sector now reporting 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.

Manufacturing saw over two-thirds of attacks (68%) resulting in data being encrypted. At the same time, the sector was less able to stop the encryption than ever before with only just over one in four attacks (27%) being stopped before the 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, manufacturing performed the second-best after IT, technology, and telecoms which stopped 49% of attacks, indicating its ability to stop attacks was better than most other sectors last year.

In 32% of attacks where data was encrypted, data was also stolen. This "double dip" approach by adversaries is becoming increasingly 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.

32%

of ransomware attacks on manufacturing 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=139/45

Data Recovery Rate in Manufacturing

Where data was encrypted, manufacturing and production organizations reported the lowest data recovery rate (88%) of all industries, considerably below the global average where 97% of organizations that had data encrypted got their data back.

One-third of manufacturing organizations (34%) paid the ransom and got data back, while almost three-quarters (73%) used backups for data recovery. In fact, the sector reported one of the lowest rates of ransom payment resulting in their data being returned, in the 2023 survey. 19% of respondents reported using multiple means to recover encrypted data.

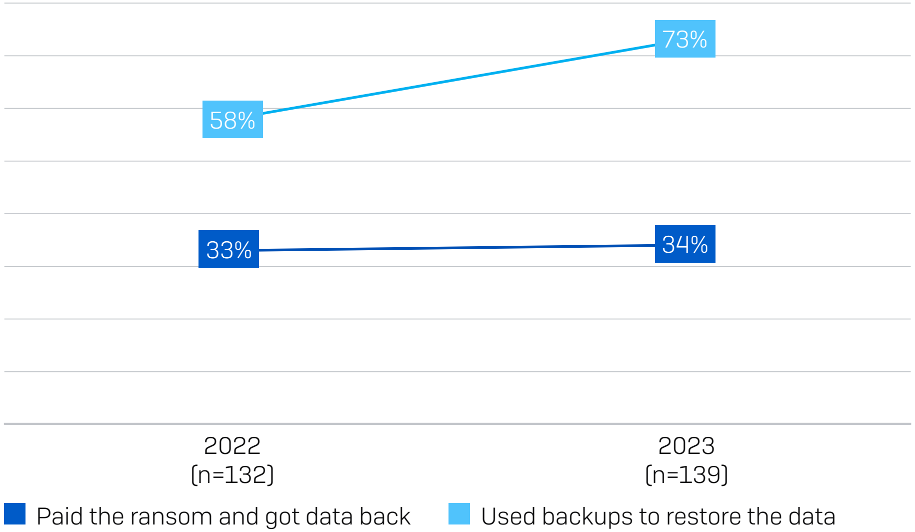
	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Got data back	88%	97%
Used backups to restore data	73%	70%
Paid the ransom to get data back	34%	46%
Used other means to get data back	1%	2%

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=139 (manufacturing and production).

The rate of ransom payments in manufacturing (34%) remained level with the findings from last year's study (33%), which is in line with the cross-industry trend.

Globally, backups continue to be the most common approach to recovering encrypted data (70%). However, concerningly, the use of backups has dropped in the last year to 70% from 73% in the 2022 survey.

Bucking the global trend, the use of backups in manufacturing increased over the last year from 58% in 2022 (the lowest backup use rate reported in the 2022 survey across all sectors) to 73% this year. While this is a welcome improvement, the fact that manufacturing has the lowest rate of data recovery suggests that the sector should continue to focus on strengthening backup use.



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

Manufacturing organizations with cyber insurance were considerably more likely to recover encrypted data than those without such policies.

The type of cyber coverage made very little difference: 94% of manufacturing organizations with a standalone policy and 93% of those with a wider insurance policy that covers cyber got data back. In comparison, only 53% of those without a policy were able to get encrypted data back.

Percentage of ransomware victims in manufacturing that recovered encrypted data

94%	93%	53%
With a standalone cyber policy	With a wider insurance policy that includes cyber	Without a cyber policy

Did your organization get any data back? n=139 manufacturing organizations that were hit by ransomware in the last year and had data encrypted (62 with standalone cyber policy, 58 with cyber as part of wider policy, 19 with no cyber policy)

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

There are likely several factors behind this variance: First, cyber insurance typically requires organizations to have backups and recovery plans as conditions of coverage. In addition, insurers are also able to guide ransomware victims through the recovery process in order to optimize outcomes.

Furthermore, organizations with cyber insurance are more likely to pay a ransom to recover data than those without a policy – and those with a standalone cyber policy reported more than double the ransom payment rate of those with cyber covered as part of a wider policy.

Impact of insurance on propensity to pay ransom in manufacturing

Standalone cyber policy	Wider insurance policy that includes cyber	No cyber policy
52% paid the ransom	22% paid the ransom	11% paid the ransom

Did your organization get any data back? Yes, we paid the ransom and got data back. n=139 manufacturing organizations that were hit by ransomware in the last year and had data encrypted (62 with standalone cyber policy, 58 with cyber as part of wider policy, 19 with no cyber policy)

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

Ransom Payments

While the overall propensity to pay the ransom remains level with last year's study, the payments have increased considerably over the last year, with the average (mean) ransom payment almost doubling from $812,380 in 2022 to $1,542,333 in 2023. The median ransom payment went up from $76,500 in 2022 to $400,000 reported in this year's study.

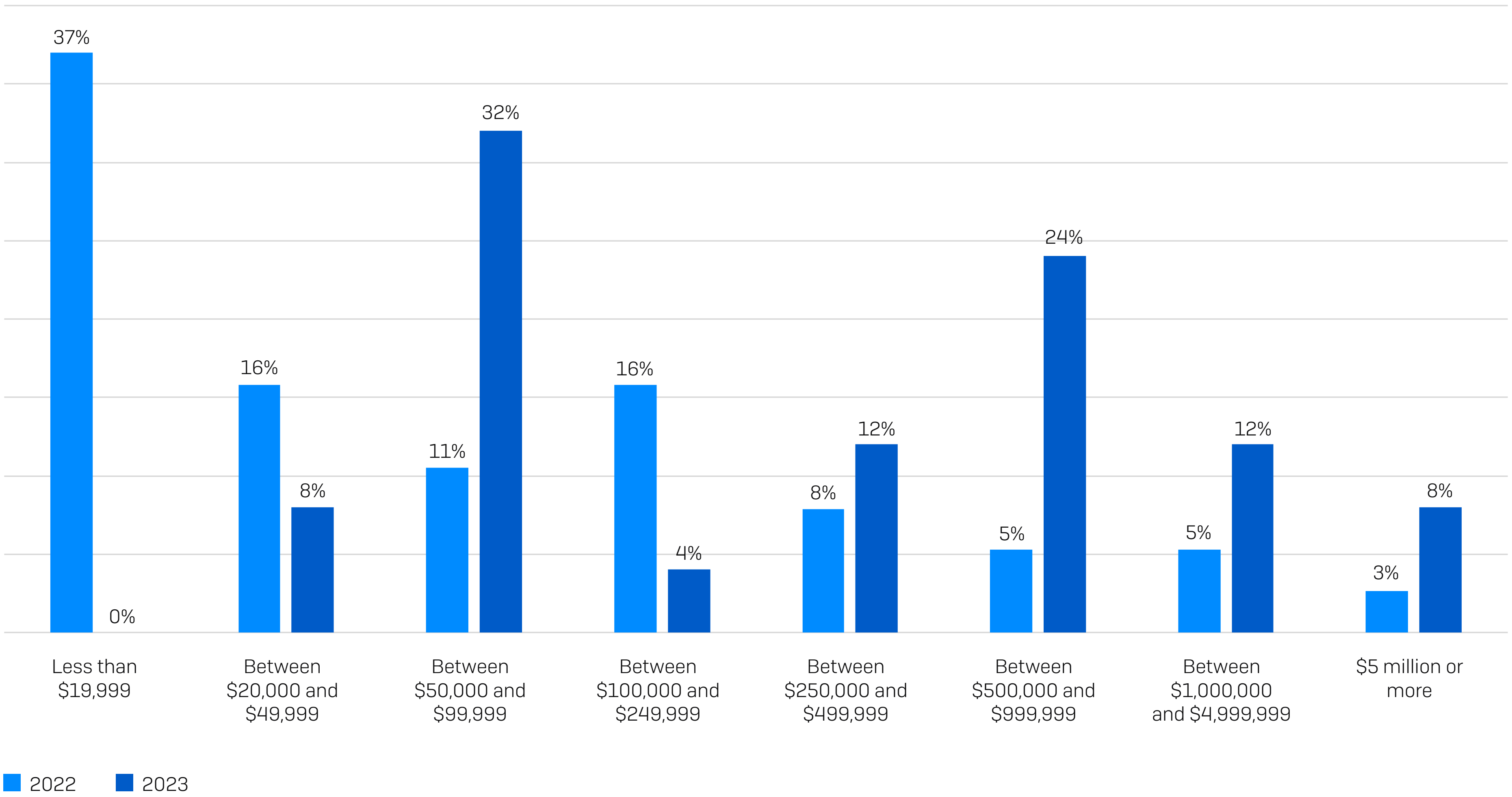
For manufacturing and production organizations, the mean ransom payment was lower than the global average [$1,260,207 in manufacturing vs. $1,542,330 globally], but the median ransom payment was higher than the global average [$450,000 in manufacturing vs. $400,000 globally].

Cross-sector Average	Cross-sector Average	Manufacturing And Production
2022	2023	2023
$812,360 (mean) $76,500 (median)	$1,542,330 (mean) $400,000 (median)	$1,260,207 (mean) $450,000 (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); Manufacturing: n=25 (2023)/ 38)(2022). Manufacturing has low base numbers so the findings should be considered indicative.

The proportion of manufacturing organizations paying higher ransoms has increased from our 2022 study, with 40% paying a ransom between $100,000 and $999,999 vs. 29% who paid this amount in 2022. In addition, 20% reported payments of $1 million or more compared to 8% last year. Conversely, just 40% paid less than $100,000, down from 63% last year.

Ransom Payments by Manufacturing and Production: 2023 vs. 2022



How much was the ransom payment that was paid to the attackers? Excluding 'Don't know' responses. n=25 (2023)/ 38 (2022).

Manufacturing 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. 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 figure, including ransom payments of $1.4 million, and in line with the $1.85 million including ransom reported in 2021.

Defying this global trend, the recovery cost for manufacturing has come down over the years, likely due in part to the increased use of backups by manufacturing organizations to recover their encrypted data.

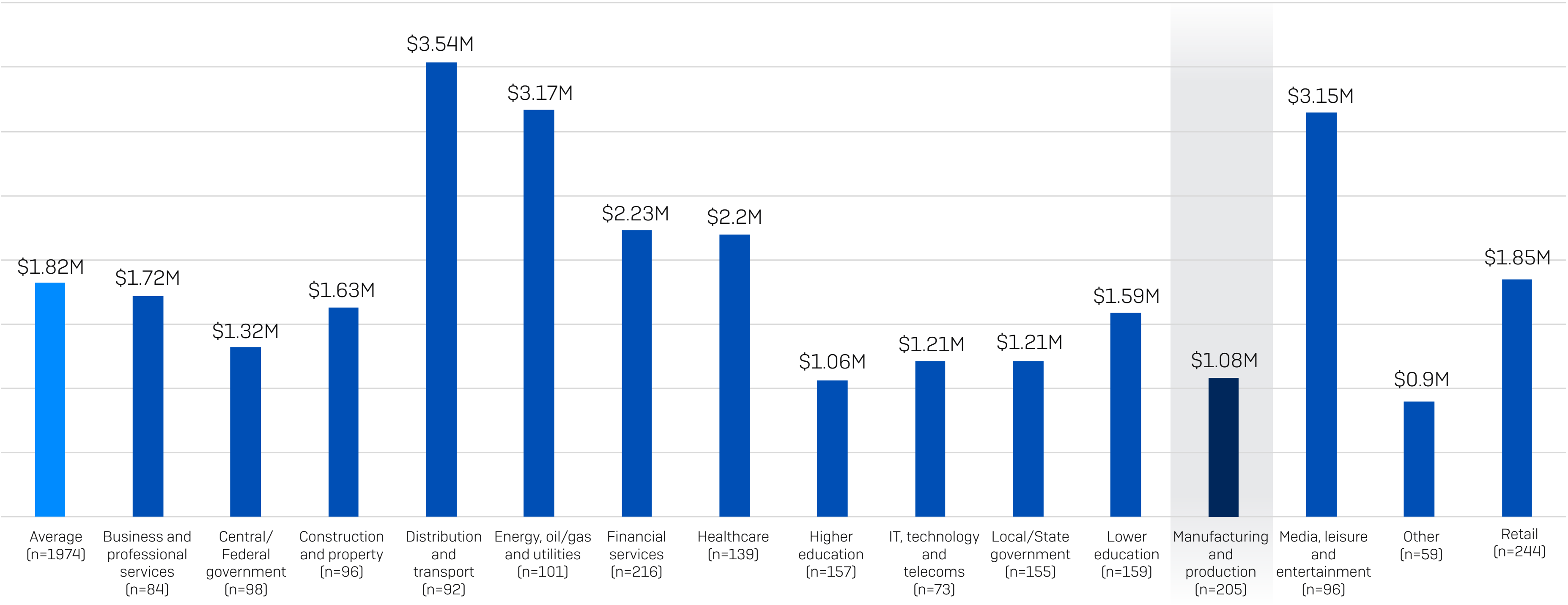
	2021	2022	2023
Cross-sector Average	$1.85M	$1.4M	$1.82M
Manufacturing	$1.52M	$1.23M	$1.08M

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); Manufacturing: n=205 (2023)/ 230 (2022)/ 158 (2021)

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

Across all sectors, manufacturing and production organizations were among those who spent the least to recover from an attack with a recovery cost of $1.08M. Distribution and transport reported the highest recovery cost ($3.54M), which is almost double what many other sectors incurred.

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

Backups turn out to be a cheaper way to recover data than paying a ransom. Across 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 than paid the ransom.

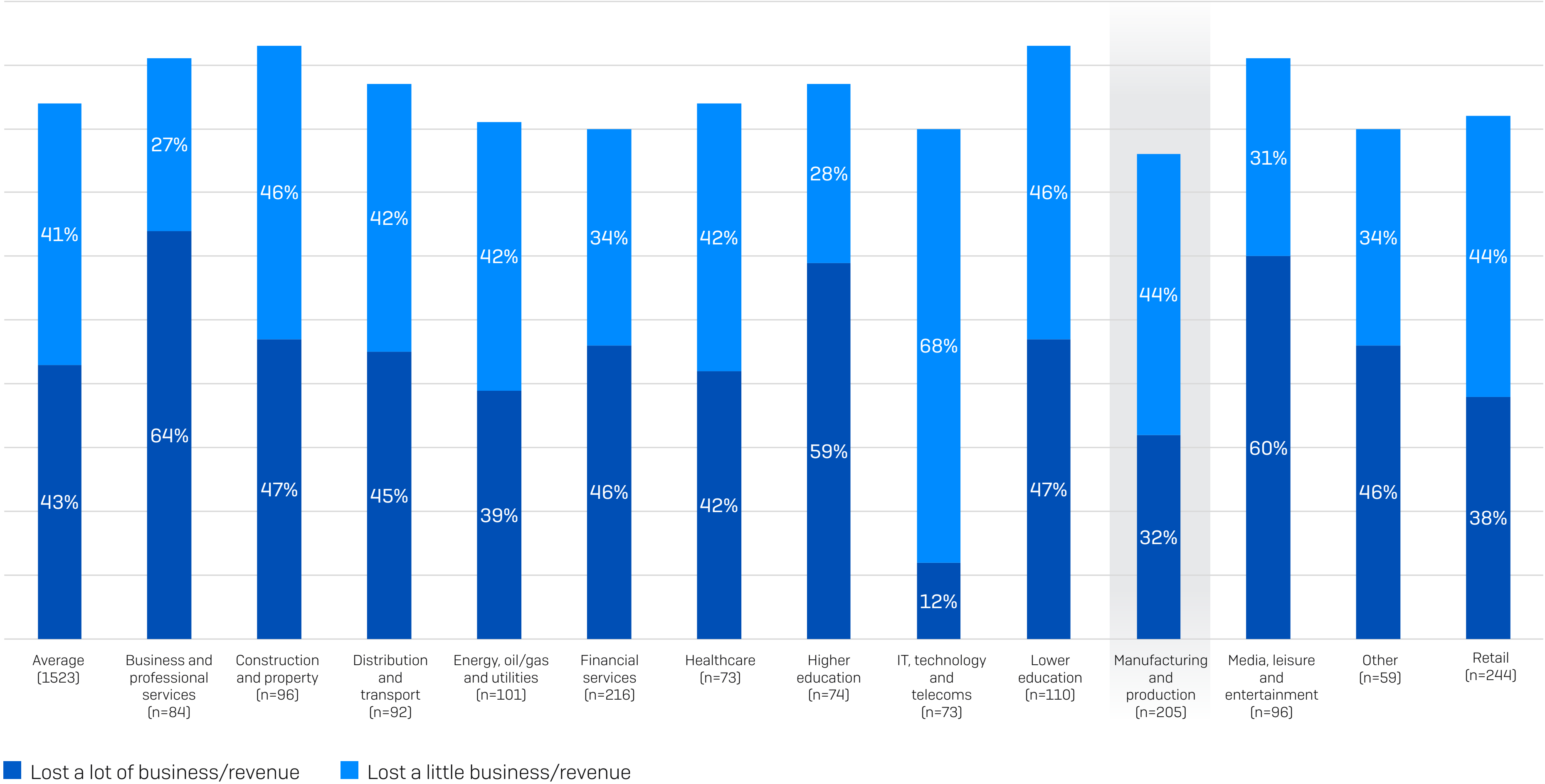
Manufacturing tells a similar story with the median recovery cost for those using backups coming to half of the median recovery cost for those who paid the ransom. The mean recovery cost with backups was $50K less than by paying the ransom.

	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
Manufacturing	**$750,000** median **$1.79M** mean	**$375,000** median **$1.29M** 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; Manufacturing: n=47 that paid the ransom and got data back and 101 that used backups to restore the data.

Business Impact

The manufacturing and production sector was least likely (77%) to report loss of business/revenue due to attacks. Lower education (94%) and construction and property (93%) were most likely. Across sectors, 84% of private sector organizations hit by ransomware reported that the attack caused them to lose business/revenue.

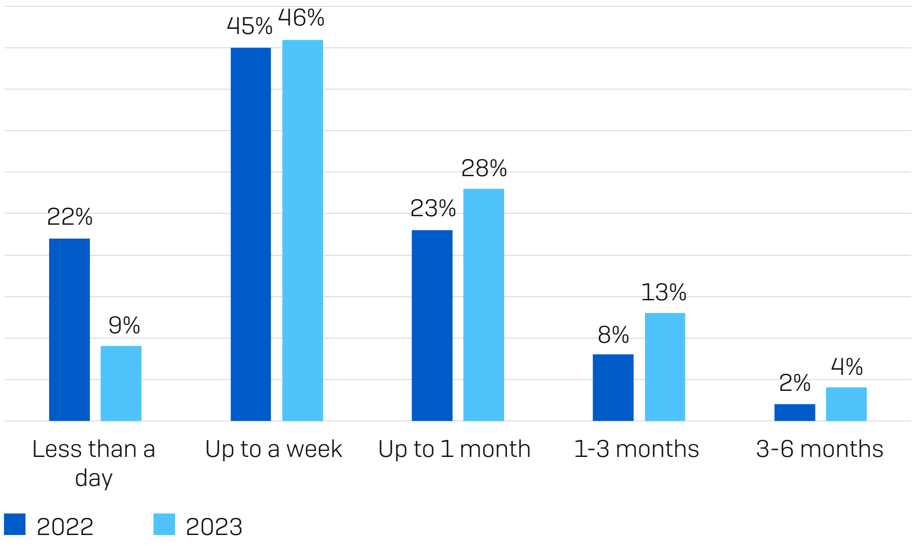


Did the ransomware attack cause your organization to lose business/revenue? Yes, we lost a lot of business/ revenue, Yes, we lost a little business/ revenue.
Private sector organizations that were hit by ransomware, base numbers in chart

Recovery Time

While the time to recover from a ransomware attack in manufacturing is broadly in line with the 2022 findings, the percentage that recovered in less than a day has dropped considerably to 9% in the last year (vs. 22% in the last survey).

The percentage of organizations that took more than a month to recover has gone up to 18% (with rounding) compared to 10% (with rounding) in the 2022 survey, which suggests that the recovery time has become longer for this sector.



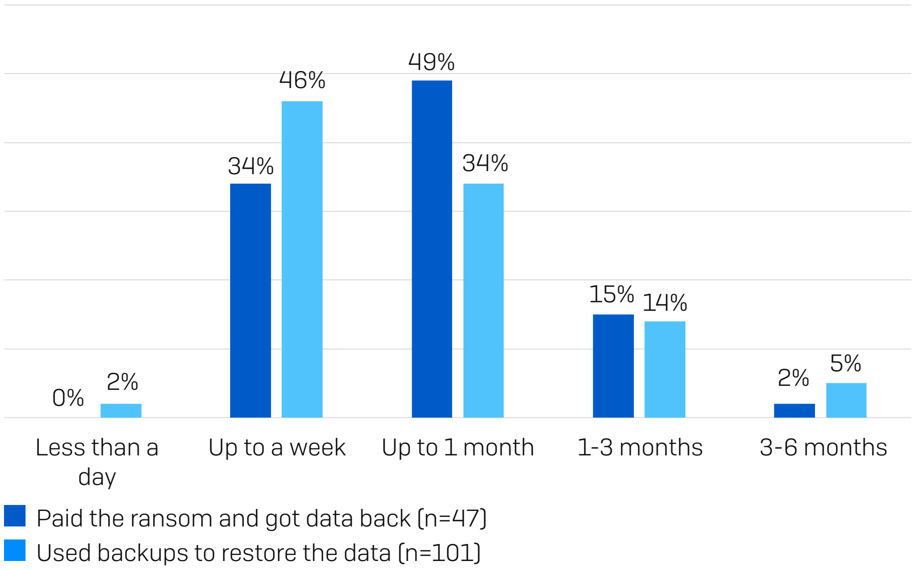
How long did it take your organization to fully recover from the ransomware attack? 205(in 2023) /230 (in 2022) manufacturing and production organizations that were hit by ransomware.

Recovery time by data recovery method

The research revealed that manufacturing organizations that use backups to recover their data, recover from the attack more quickly than those that pay the ransom. 48% of those that used backups recovered within a week, compared with 34% of those that paid the ransom.

At the same time, close to half (52% with rounding) of the manufacturing respondents that used backups took up to a month or more to recover data, while nearly two-thirds (66% with rounding) that paid the ransom took up to a month or more 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 manufacturing and production organizations. As adversaries continue to hone their attack tactics, techniques, and procedures (TTPs), defenders are struggling to keep pace, resulting in increased encryption rates: two in three manufacturing organizations (68%) hit by ransomware reported that adversaries succeeded in encrypting their data. In addition, 32% reported that their encrypted data was also stolen in the last year.

Manufacturing reported a low propensity to pay the ransom (34%) to get their data back, with almost double the number that paid the ransom using backups for data recovery. Encouragingly, the use of backups for data recovery increased to 73% in the 2023 survey from 58% a year before. All said, manufacturing and production reported the lowest data recovery rate (88%) compared to the global average, where 97% of organizations that had data encrypted got their data back.

Insurance had a prominent impact on the rate of data recovery as well as the propensity to pay the ransom. Manufacturing organizations with cyber insurance were considerably more likely to recover encrypted data than those without such policies. Furthermore, manufacturing organizations with cyber insurance were more likely to pay a ransom to recover data than those without a policy.

The recovery cost for manufacturing came down over the year to $1.08M last year, likely influenced by the increase in backup use by manufacturing organizations to recover their encrypted data. The sector was least likely to report loss of business/revenue due to attacks (77%) – another likely reason why recovery costs dropped from previous years.

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

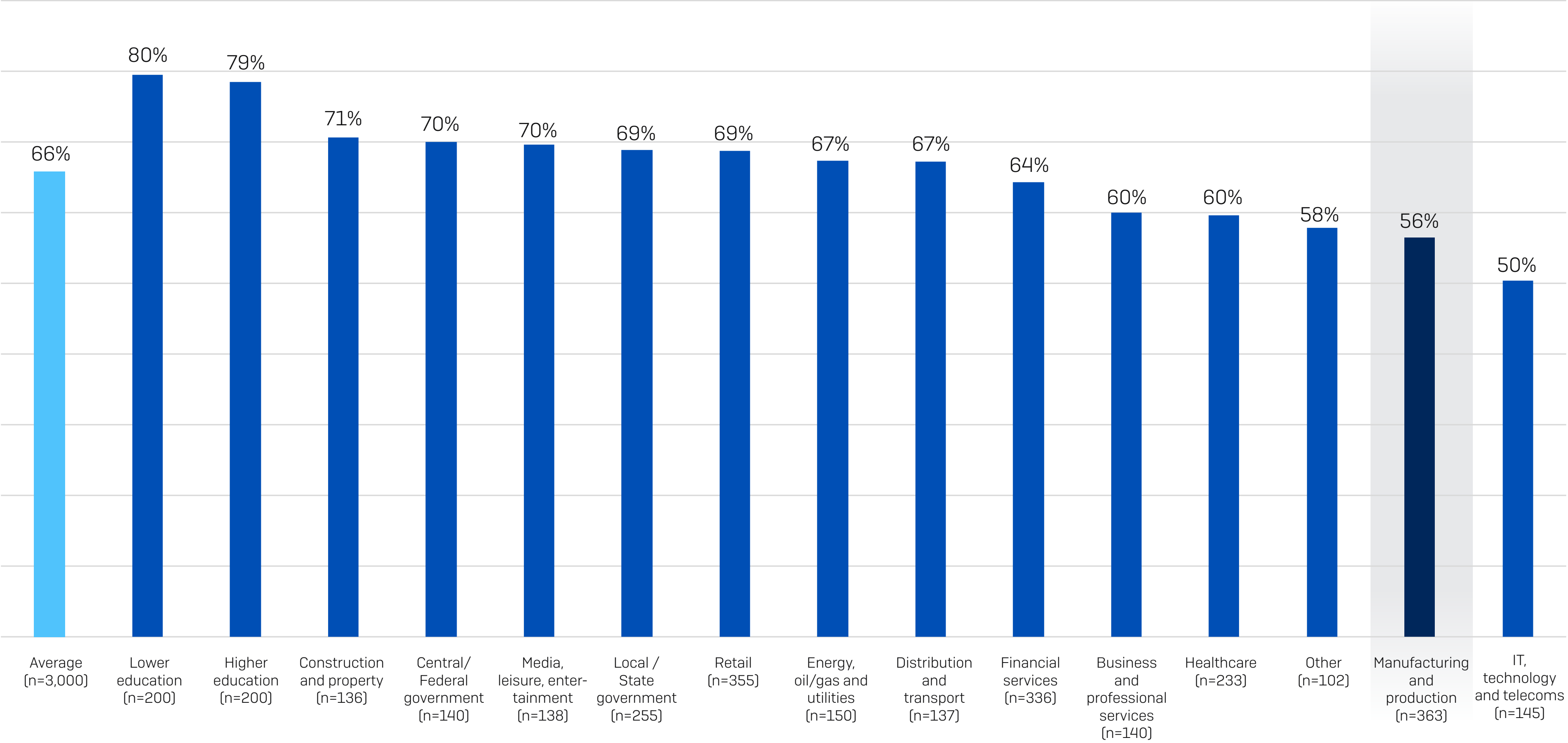
Organizations should focus on:

- 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

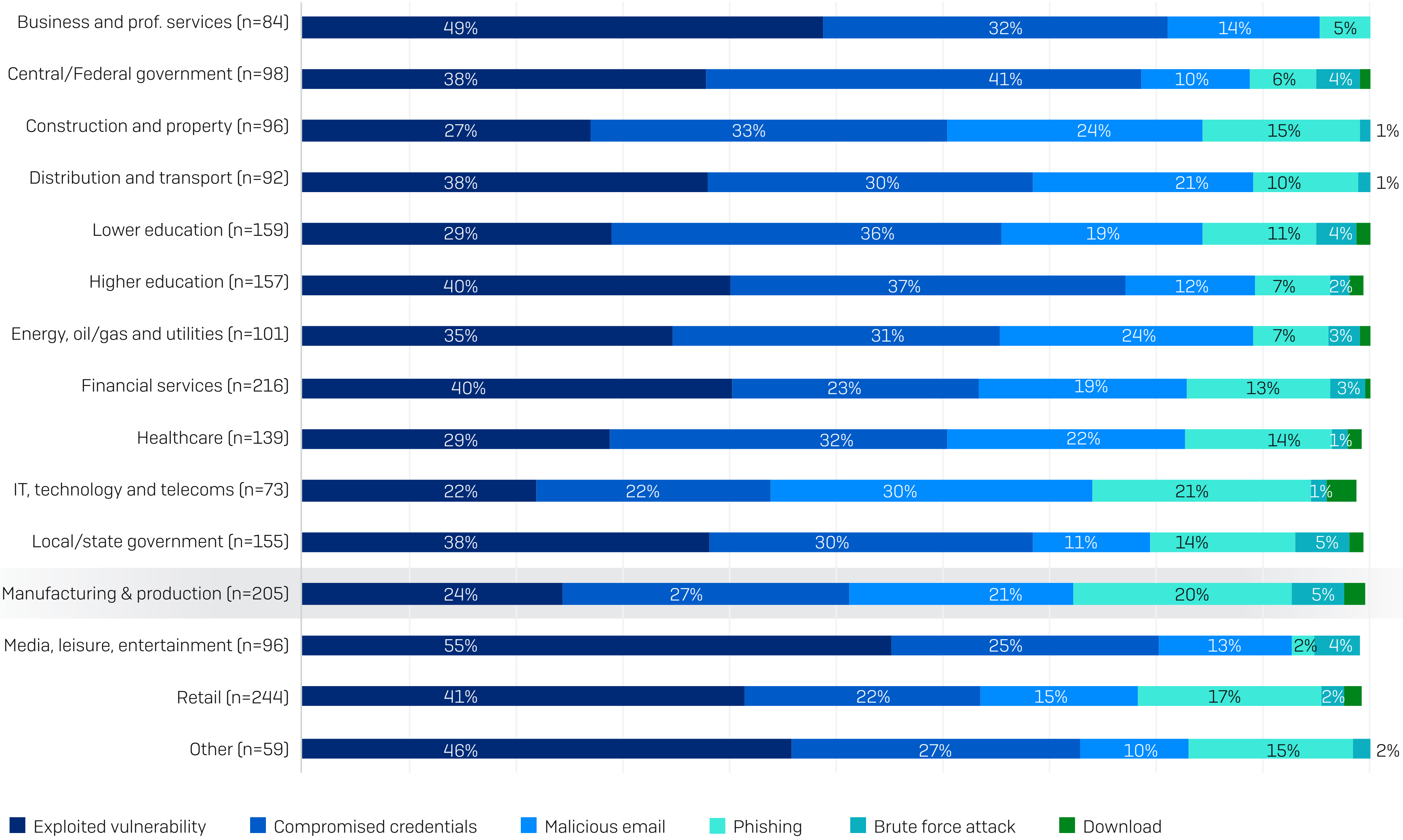
Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



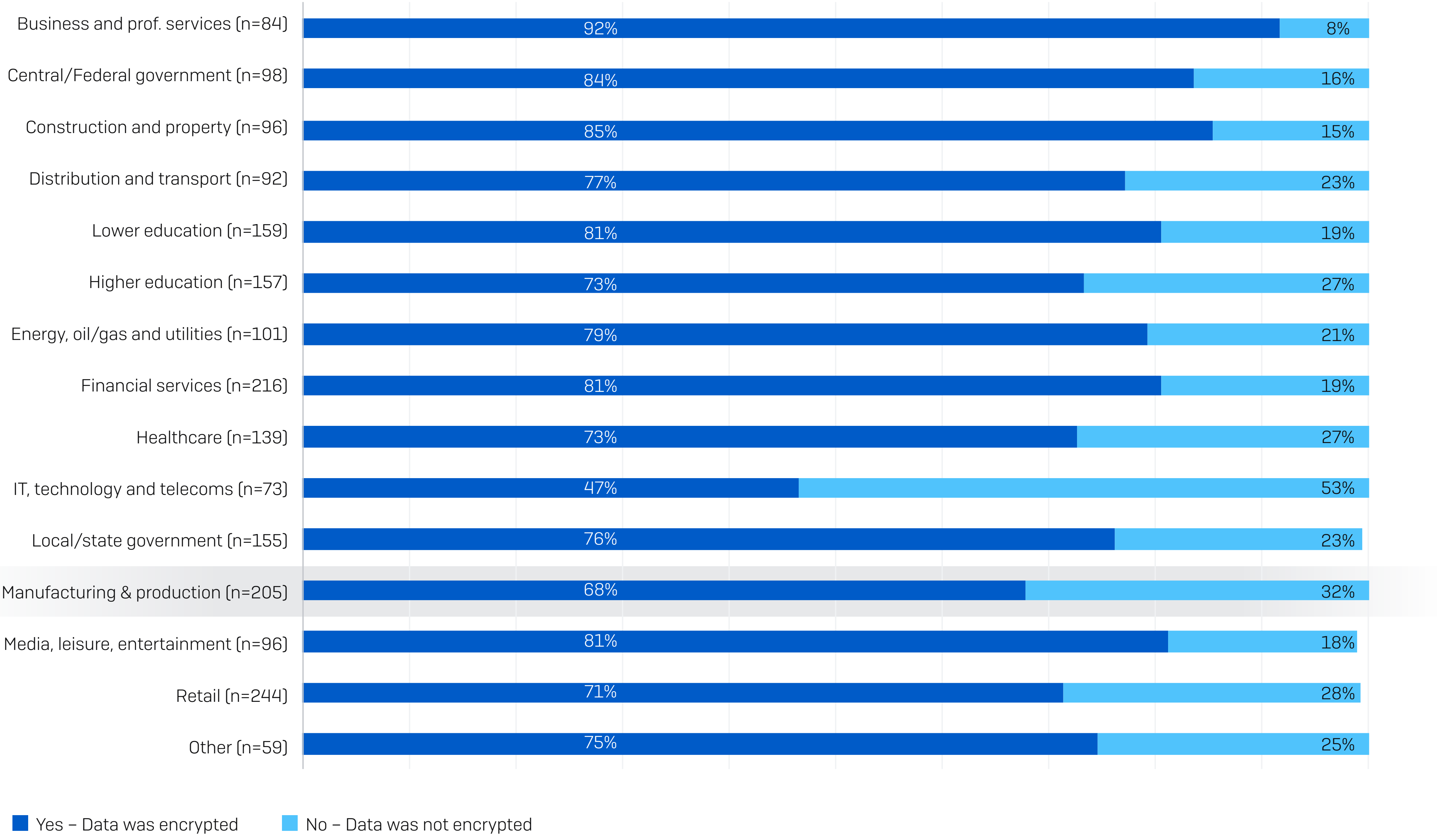
In the last year, has your organization been hit by ransomware? Base numbers in chart

Root Cause of Attack by Industry



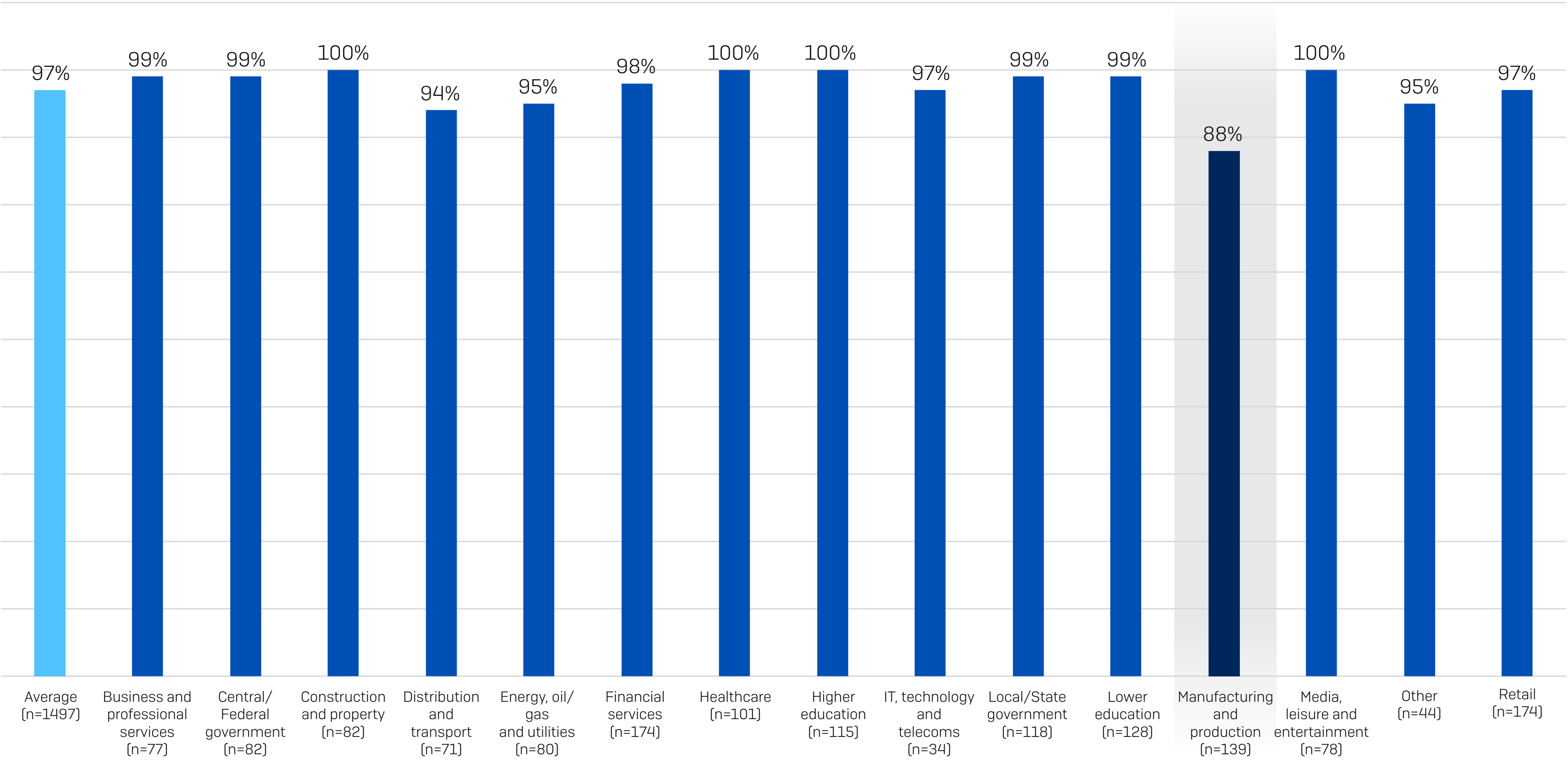
Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Data Encryption by Industry



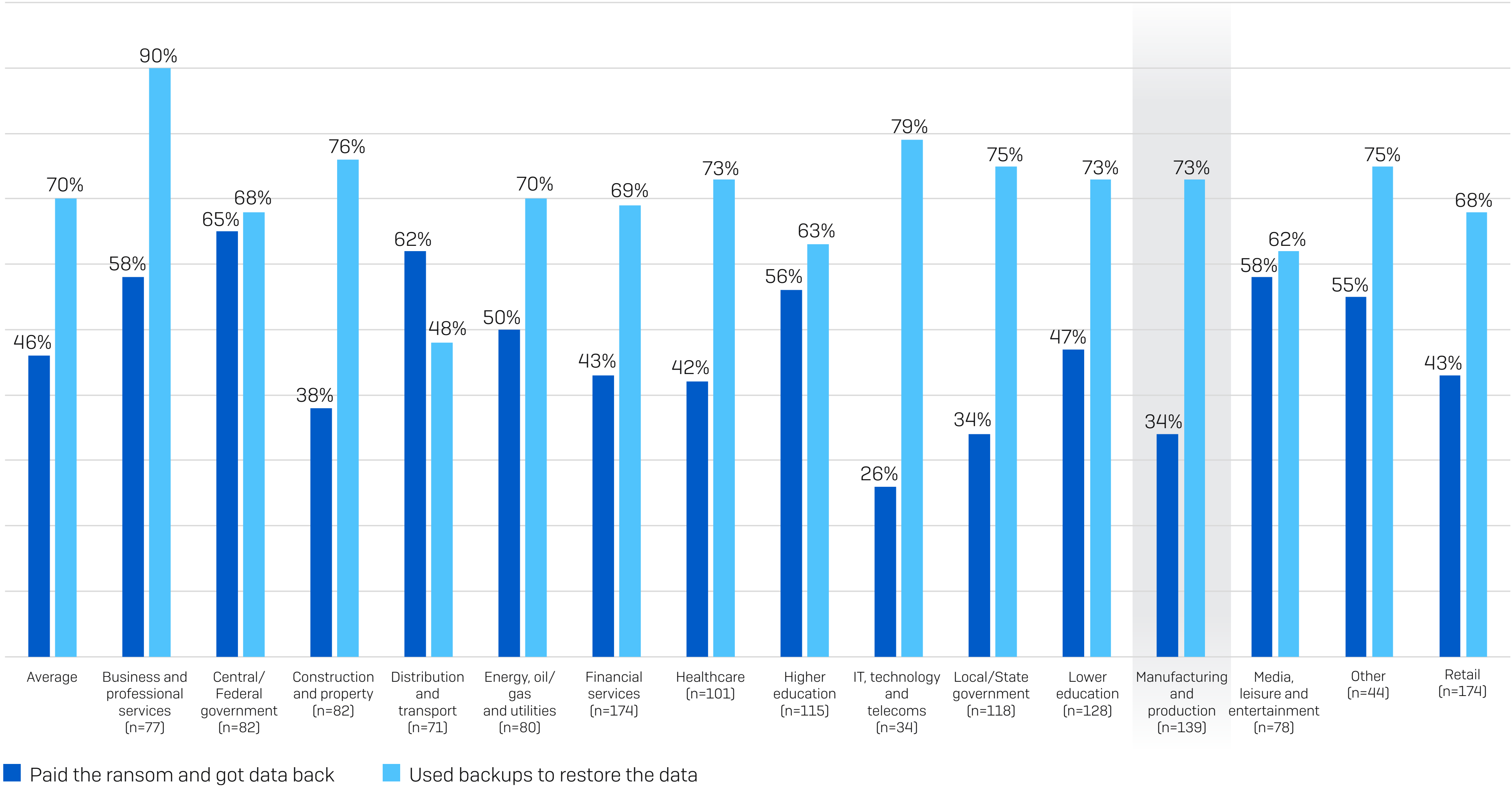
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

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

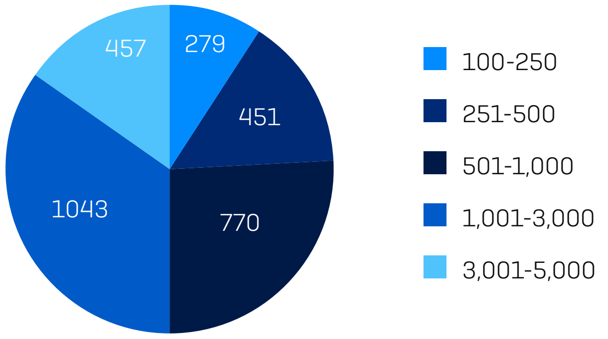
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

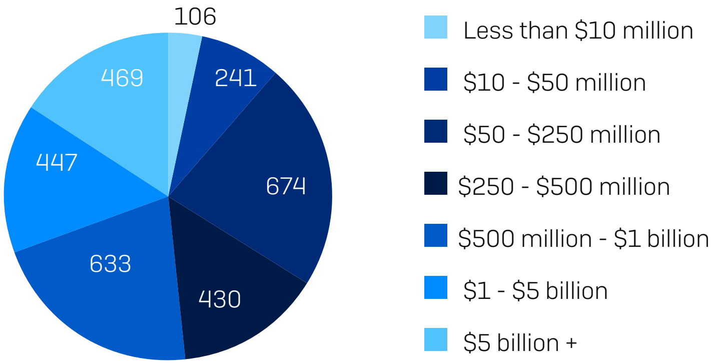
Respondents by Country

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.

2023-06-13 (WP-PC)