SOPHOS

pmc

The State of Ransomware 2023

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

A Sophos Whitepaper. May 2023

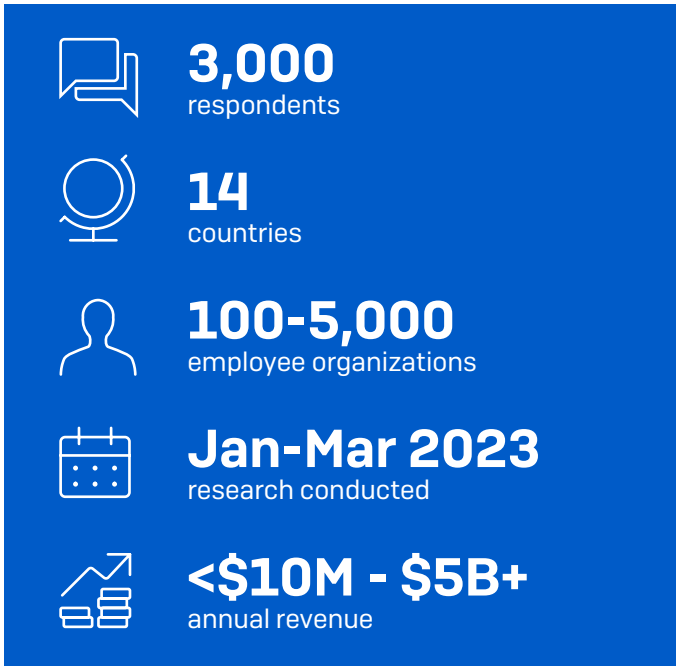
Introduction

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 organization revenue. 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 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.

Within the education sector, respondents were split into lower education (catering to students up to 18 years) and higher education (for students over 18 years).



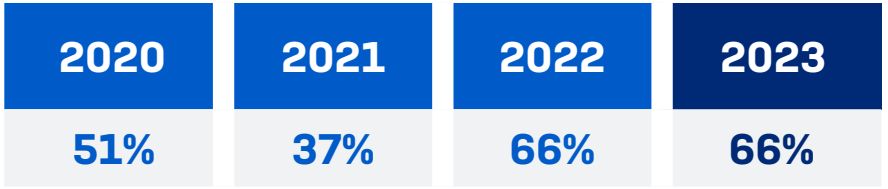
Contents

Introduction 2
Rate of Ransomware Attacks 4
Root Causes of Ransomware Attacks 6
Rate of Data Encryption 8
Data Theft 9
Data Recovery 9
The Impact of Cyber Insurance on Data Recovery 11
Ransom Payments 12
Recovery Costs 14
Recovery Cost by Revenue 15
Business Impact 16
Loss of Business/Revenue by Industry 17
Recovery Time 18
Conclusion 19
Additional Charts 20
Research Methodology 26

Rate of Ransomware Attacks

The research revealed that the rate of ransomware attacks has remained level, with 66% of respondents reporting that their organization was hit by ransomware in the previous year, the same as in our 2022 survey. With adversaries now able to consistently execute attacks at scale, ransomware is arguably the biggest cyber risk facing organizations today.

Cyber criminals 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.



In the last year, has your organization been hit by ransomware?
Yes. n=3000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020)

Attacks by Country

While the overall reported ransomware rate remains flat compared to 2022, the survey revealed variations at a country level. Singapore reported the highest rate of ransomware attacks in this year's study, with 84% of organizations being hit in the previous year. Conversely, the UK reported the lowest rate of attack (44%).

Austria reported the biggest drop in rate of attack, down from 84% of organizations hit to 50%. South Africa had the biggest increase in attack rate, with 78% of organizations hit in our 2023 survey compared to 51% in 2022.

For further details, see Rate of Ransomware Attacks by Country: 2022 vs 2023 on page 20.

Attacks by Industry

The education sector was the most likely to have experienced a ransomware attack in the last year with 80% (lower education) and 79% (higher education) reporting being hit. Education traditionally struggles with lower levels of resourcing and technology than many other industries, and the data shows that adversaries are exploiting these weaknesses.

IT, technology, and telecoms reported the lowest level of attack (50%), indicating a higher level of cyber readiness and cyber defenses.

For further details, see Rate of Ransomware Attacks by Industry on page 21.

66% hit by ransomware

Singapore highest rate of attack (country)

UK lowest level of attack (country)

Education highest level of attack (industry)

IT, Technology, and Telecoms lowest level of attack (industry)

Attacks by Organization Size: Employees vs. Revenue

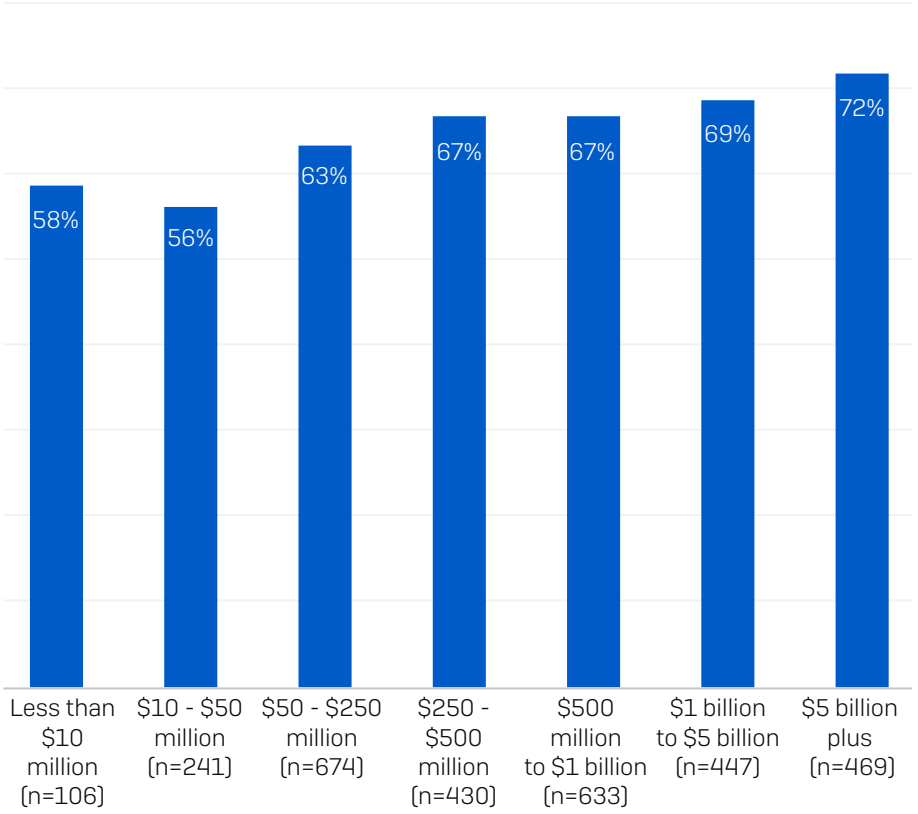
The research revealed a clear correlation between annual revenue and propensity to experience a ransomware attack, with the percentage of organizations hit by ransomware increasing progressively with revenue. 56% of organizations with revenue of $10-$50 million experienced a ransomware attack in the last year, rising to 72% of those with revenue of $5 billion plus.

Conversely, there was little clear relationship between experiencing ransomware and the number of employees in an organization. Outside the 1,001-3,000 employee segment, the rate of ransomware attack was very consistent:

- 100-250 employees 62%
- 251-500 employees 62%
- 501-1,000 employees 62%
- 1,001 – 3,000 employees 73%
- 3,001 – 5,000 employees 63%

The data makes clear that in the context of organization size, annual revenue is a much greater indicator of likelihood of experiencing an attack than number of employees.

Percentage of Organizations Hit by Ransomware by Revenue

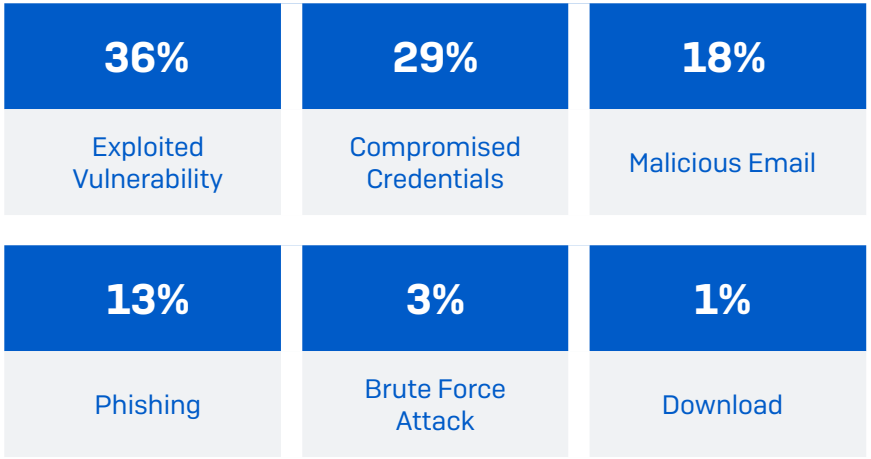


In the last year, has your organization been hit by ransomware? Yes. Base numbers in chart

Root Causes of Ransomware Attacks

Survey respondents reported that an exploited vulnerability was the most common root cause of ransomware attacks (36%), followed by compromised credentials (29%). These findings align almost exactly with Sophos' latest retrospective analysis of 152 attacks that our Incident Response and Managed Detection and Response (MDR) teams were brought in to remediate, where 37% started with an exploited vulnerability and 30% with compromised credentials.

Emails were the root cause of 30% (with rounding) of attacks: 18% started with a malicious email and 13% with phishing. 3% began with a brute force attack and just 1% with a download.



Do you know the root cause of the ransomware attack your organization experienced in the last year? If you were hit more than once, think about the most significant attack. (n=1,974 organizations hit by ransomware in the last year)

Root Causes by Industry

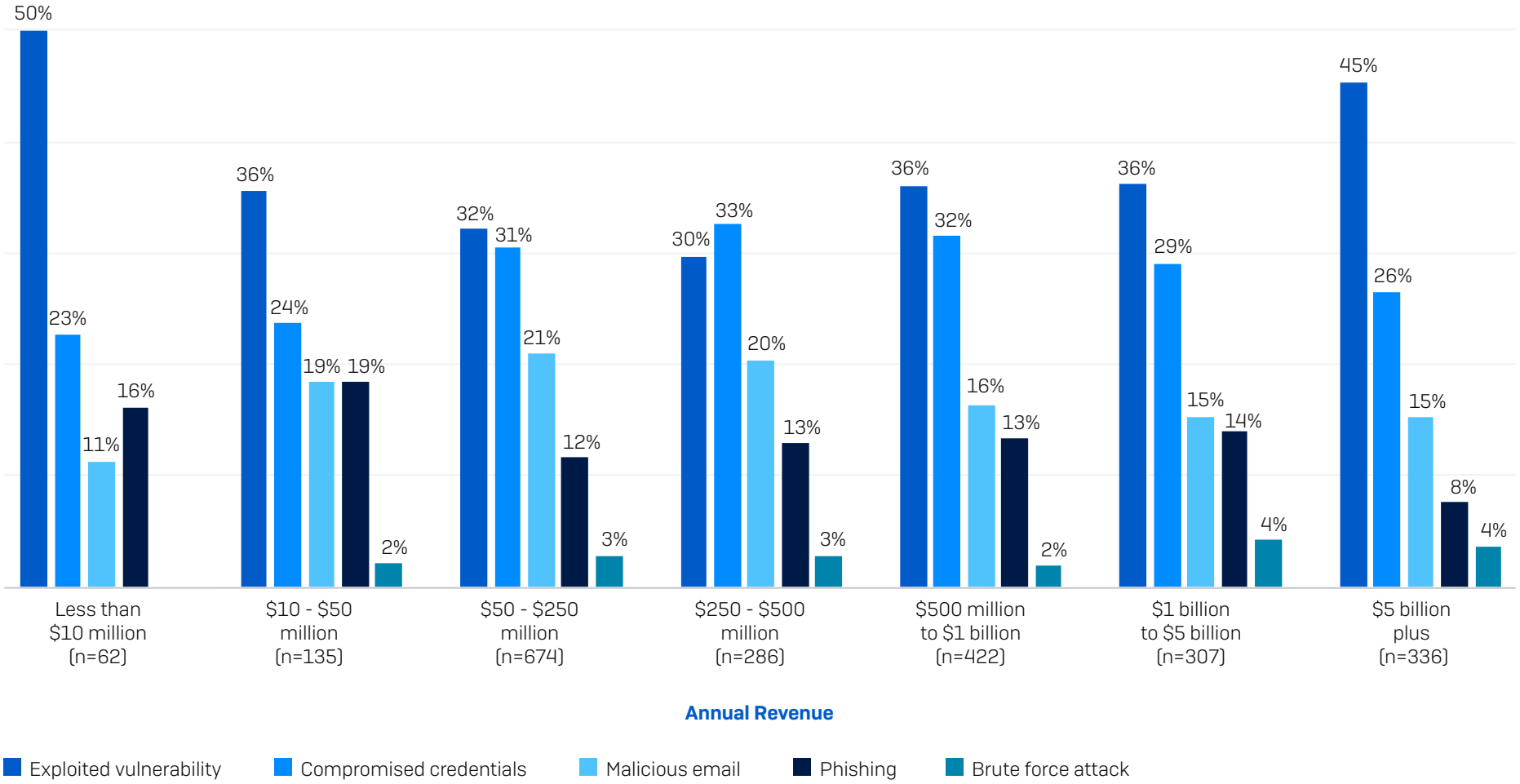
The media, leisure, and entertainment sector reported the highest percentage of attacks where the root cause was an exploited vulnerability (55%), indicating widespread security gaps in this area. Central and federal government had the highest percentage of attacks that started with compromised credentials (41%). This may be due to a higher rate of credential theft in this sector, a lower ability to prevent exploitation of stolen credentials, or a combination of the two.

IT, technology, and telecoms reported the lowest rates for both exploited vulnerabilities (22%) and compromised credentials (22%), which likely reflects strong levels of cyber defenses in this sector. However, it did report the highest rates of email-based attacks, with over half (51%) starting in users' inboxes.

For further details see Root Causes of Attacks by Industry on page 22.

Root Causes by Revenue

Analyzing the root causes by annual revenue reveals that exploited vulnerabilities and compromised credentials follow opposing propensity curves. The highest percentages of attacks that started with an exploited vulnerability were reported by the lowest (less than $10 million: 50%) and highest ($5 billion plus: 45%) revenue cohorts, dipping down to 30% in the middle cohort ($250 - $500 million). Conversely, the use of compromised credentials peaks in the middle revenue cohort (33%), while the lowest usage was reported in the lowest (23%) and highest (26%) revenue cohorts.

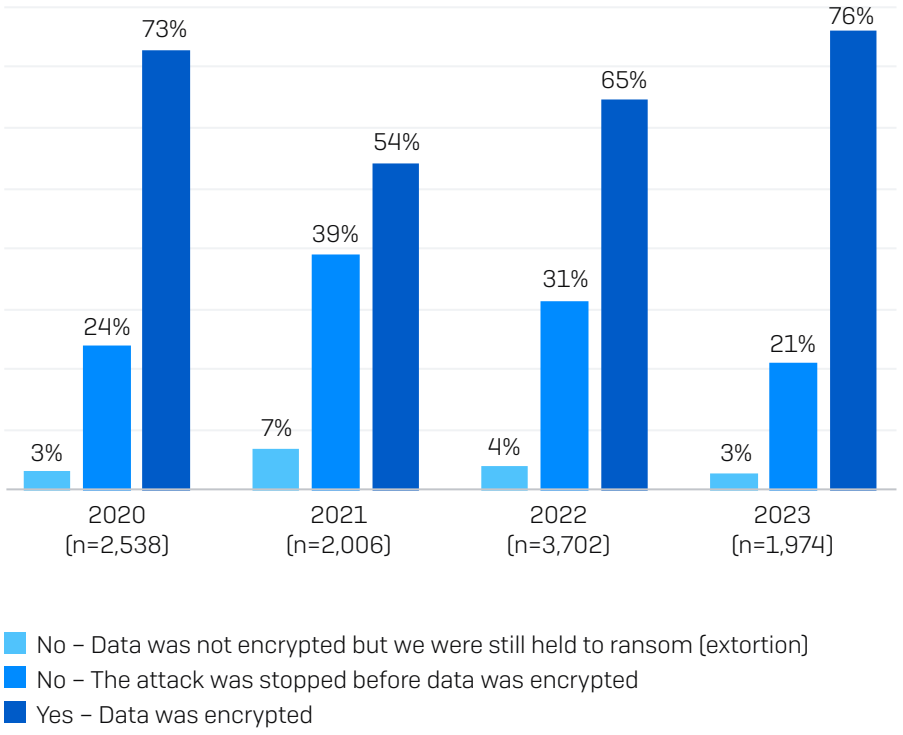


Do you know the root cause of the ransomware attack your organization experienced in the last year? Selection of answer options. Base numbers in chart

Rate of Data Encryption

Data encryption has continued to rise, with adversaries succeeding in encrypting data in over three quarters (76%) of ransomware attacks. In fact, encryption levels are now at their highest point in the last four years. This likely reflects the ever-increasing skill level of adversaries who continue to innovate and refine their approaches.

Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack?



Data Encryption by Industry

Almost all sectors struggle to stop attacks before data can be encrypted: with just one exception, in every sector, over two thirds of attacks resulted in data encryption. The highest frequency of data encryption (92%) was reported by business and professional services.

IT, technology, and telecoms is the sector that bucks the trend, with adversaries succeeding in encrypting data in fewer than half (47%) of attacks. This is another indicator of the high level of cyber defenses and response preparation by this sector.

For further details see Data Encryption by Industry on page 23.

Data Theft

In 30% 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.

30%
Of ransomware attacks where data was encrypted reported that data was also stolen

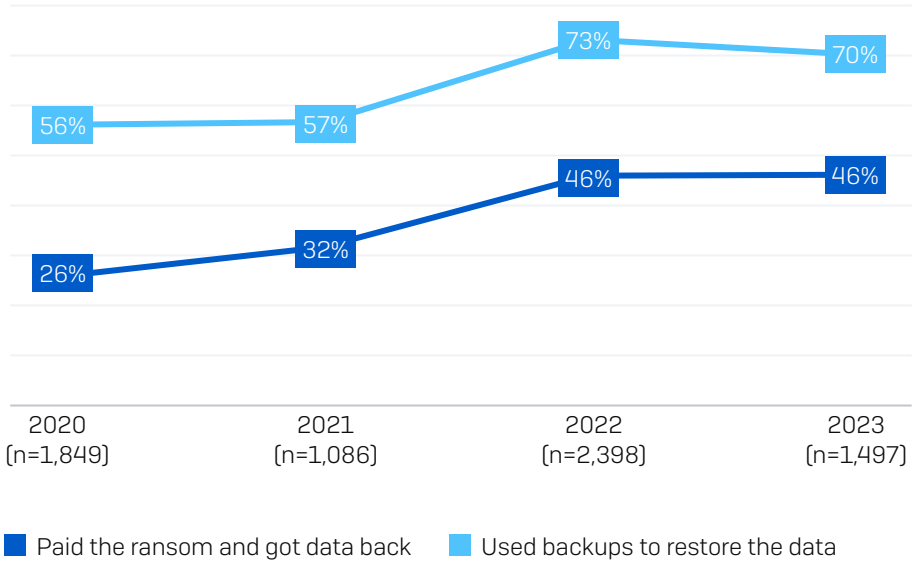
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Yes; Yes, and the data was also stolen. n=1,497

Data Recovery

97% of organizations that had data encrypted got data back. Backups were the most common approach, used in 70% of incidents. 46% paid the ransom and got data back, while 2% used other means. Overall, one in five (21%) used multiple methods to restore their data. 1% of organizations that had data encrypted paid the ransom but didn't get data back.

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
70%	46%	2%

Concerningly, use of backups to recover data has dropped in the last year when it was used to recover data in 73% of cases. Ransom payment rate has remained level from last year.



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

Data Recovery by Country

Overall, respondents in EMEA reported higher aggregate levels of backup use (75%) and lower aggregate levels of ransom payments (40%) than those in the Americas (65%/55%) and Asia Pacific (67%/49%). At a country level, France has the highest level of backup use (87%), closely followed by Switzerland (84%).

The importance of backups is demonstrated when we see that the two countries least able to use backups to restore data, Italy (55%) and Singapore (57%), are also the two countries that reported the lowest overall data recovery rates (93% and 90%, respectively). Italy also reported the highest propensity to pay the ransom (56%), closely followed by the U.S. and Brazil (both 55%).

In most cases, organizations that paid the ransom were able to recover data. However, in France and the UK, around one in ten organizations that paid the ransom did not get any data back.

For further details see Data recovery by Country on page 24.

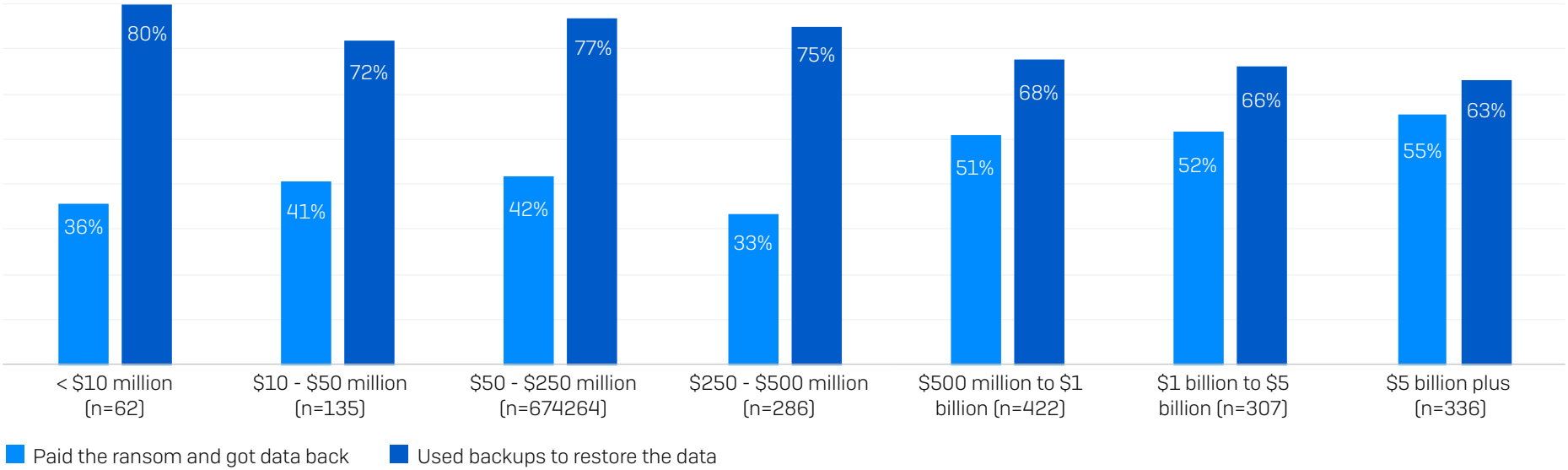
Ransom Payment and Backup Use by Revenue

Generally speaking, as annual revenue increases, so does the propensity of an organization to recover data by paying the ransom. At the same time, frequency of backup use drops.

Of the organizations with revenue of over $5 billion, 55% got data back by paying the ransom and 63% used backups. At the same time, 36% of organizations with revenue of less than $10 million recovered data by paying the ransom, while 80% used backups – the highest rate of backup use of all revenue cohorts.

Organizations with lower annual revenue have less money to fund ransom payments, forcing them to focus on backups for data recovery. At the same time, larger revenue organizations typically have complex IT infrastructures which may make it harder for them to use backups to recover data in a timely fashion. They are also the businesses most able to buy their way out of such situations.

Ransom Payment and Backup Use by Revenue



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 Cyber Insurance on Data Recovery

Organizations with cyber insurance were considerably more likely to recover encrypted data than those without such policies. However, the type of cyber coverage made very little difference: 98% of those with a standalone policy and 97% of those with a wider insurance policy that covers cyber got data back. In comparison, 84% of those without a policy were able to get encrypted data back.

Percentage of ransomware victims that recovered encrypted data

Did your organization get any data back? n=1,497 organizations that were hit by ransomware in the last year and had data encrypted

There are likely several factors behind this variance. First, cyber insurance typically requires organizations to have backups and recovery plans as conditions of coverage. 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 the ransom to recover data than those without a policy.

Impact of insurance on propensity to pay ransom

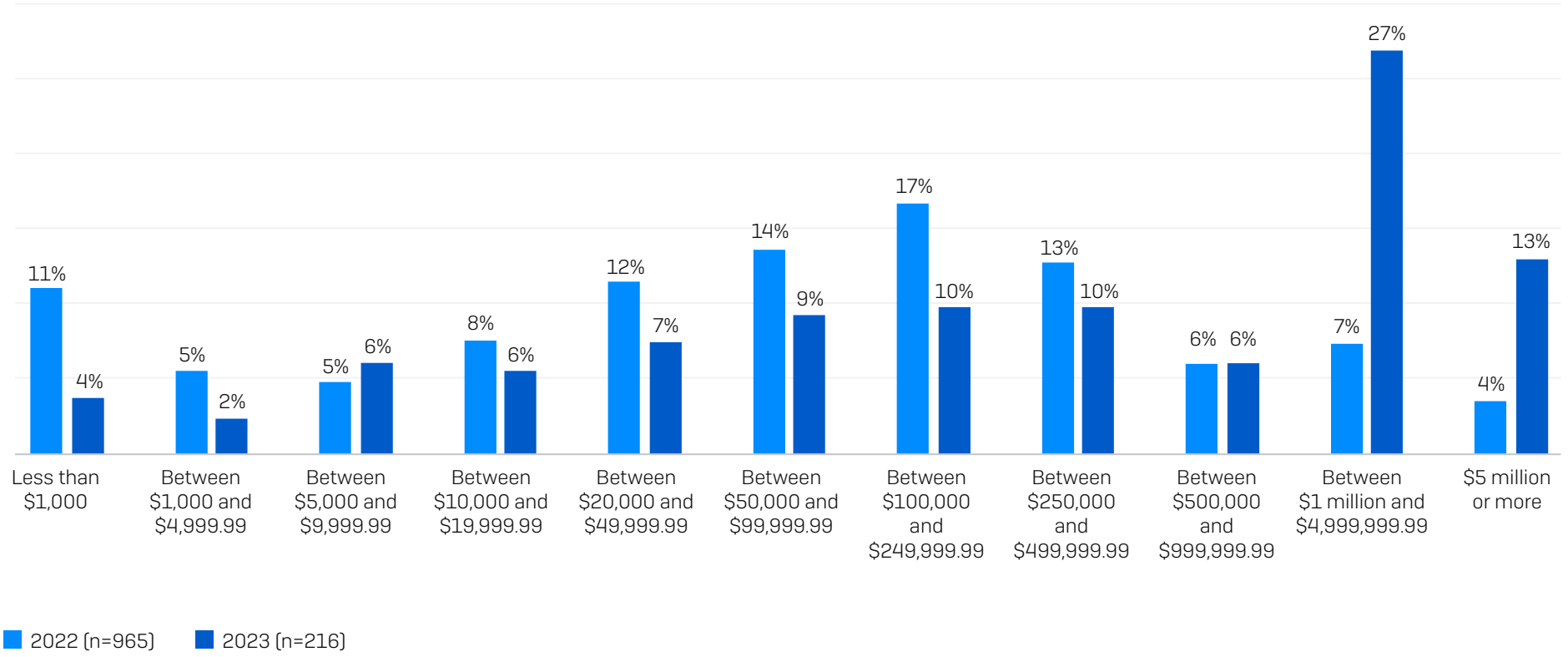
Did your organization get any data back? Yes, we paid the ransom and got data back. n=1,497 organizations that were hit by ransomware in the last year and had data encrypted (771 standalone policy, 658 cyber as part of wider policy, 67 no cyber policy)

Ransom Payments

While overall propensity to pay ransom remains level with last year's study, the payments themselves 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 reported in this year's study was $400,000.

The study revealed a wide distribution of payments, however the proportion of organizations paying higher ransoms has increased from our 2022 study, with 40% reporting payments of $1 million or more compared to 11% last year. Conversely, just 34% paid less than $100,000, down from 54% last year.

Ransom Payments: 2023 vs 2022



How much was the ransom payment that was paid to the attackers? Excluding "Don't know" responses.

Ransom Payments by Revenue

Perhaps unsurprisingly, the largest revenue organizations were most likely to pay the highest ransoms, reflecting that adversaries will adjust the amount they will accept based on ability to pay. The study did not distinguish between payments funded internally and those funded by insurance providers.

Interestingly, there was very little difference in both the mean and median ransom payments for organizations with $250 million - $500 million revenue and those with $500 million - $1 billion revenue.

	$50-$250 MILLION (N=37)	$250-$500 MILLION (N=33)	$500 MILLION TO $1 BILLION (N=72)	$1 BILLION - $5 BILLION (N=45)	$5 BILLION PLUS (N=21)
Mean ransom payment	$690,996	$1,523,652	$1,466,240	$2,049,817	$2,464,339
Median ransom payment	$145,000	$428,000	$425,000	$1,000,000	$3,000,000

How much was the ransom payment that was paid to the attackers? Excluding "Don't know" responses. Excluding organizations with below $50 million annual revenue due to very low base numbers. Base numbers in chart. Data for segments with fewer than 30 responses should be considered indicative only.

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, organizations reported an estimated mean cost to recover from ransomware attacks of $1.82 million, an increase from the 2022 figure of $1.4 million and in line with the $1.85 million reported in 2021.

Note: the 2021 and 2022 study question wording included ransom payments in the estimated costs, but they were removed from the 2023 survey wording. As a result, the year-on-year comparison should be considered indicative only.

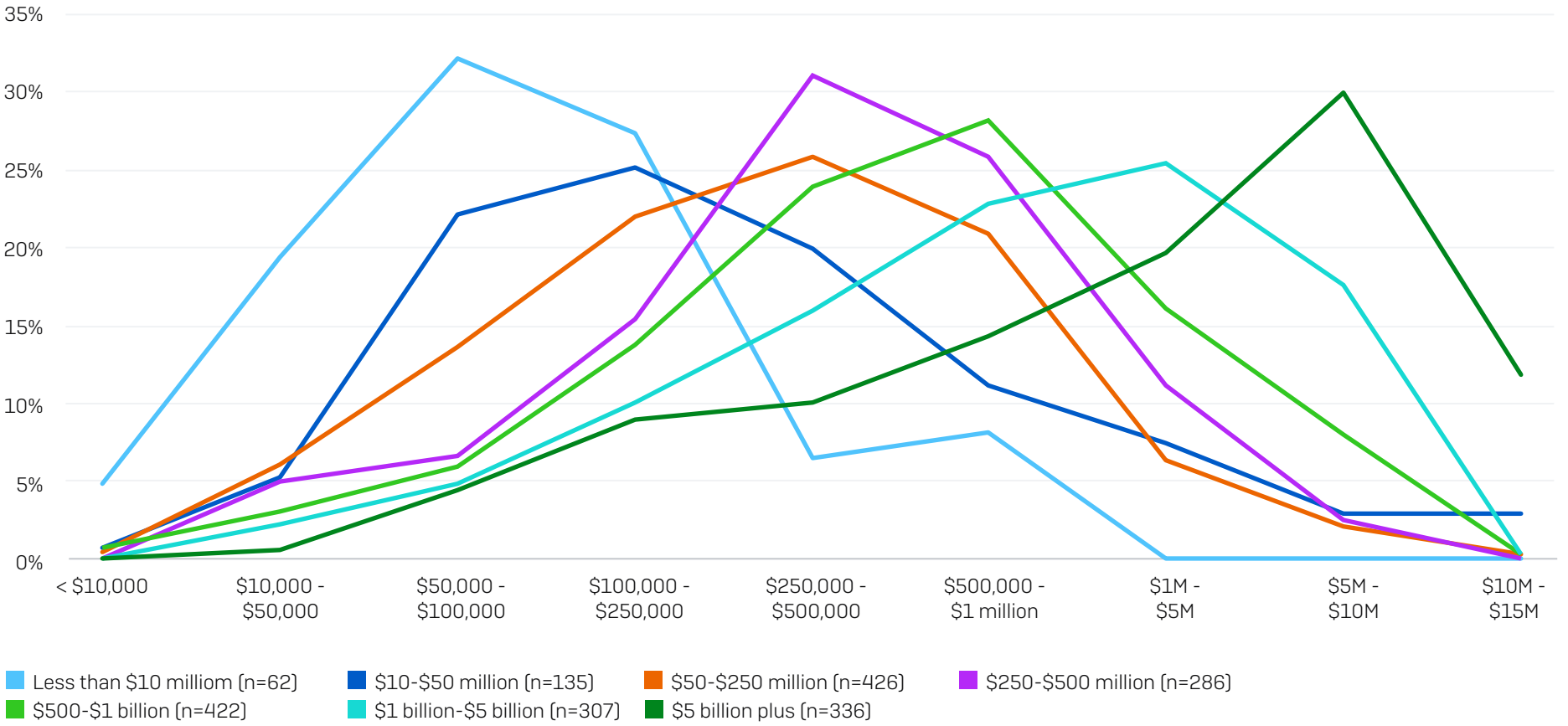
Mean Recovery Cost

2021	2022	2023
$1.85M	$1.4M	$1.82M

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.)? n=1,974 (2023)/ 3,702 (2022)/ 2,006 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

Mean reported recovery costs started at $165,520 for organizations with annual revenue of less than $10 million, rising to $4,496,086 in the $5 billion plus cohort. While these numbers mask a range of recovery costs, there is a clear pattern of recovery costs increasing with revenue, as indicated in the chart on the following page.

Recovery Cost by Revenue



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

Whichever way you look at the data, it is considerably cheaper to use backups to recover from a ransomware attack than to pay the ransom. 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. If further evidence were needed of the financial benefit of investing in a strong backup strategy, this is it.

Paid the ransom and got data back	Used backups to restore data
$750,000 median	**$375,000** median
$2.6M mean	**$1.62M** 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.)? n=694 that paid the ransom and got data back and 1,053 that used backups to restore the data.

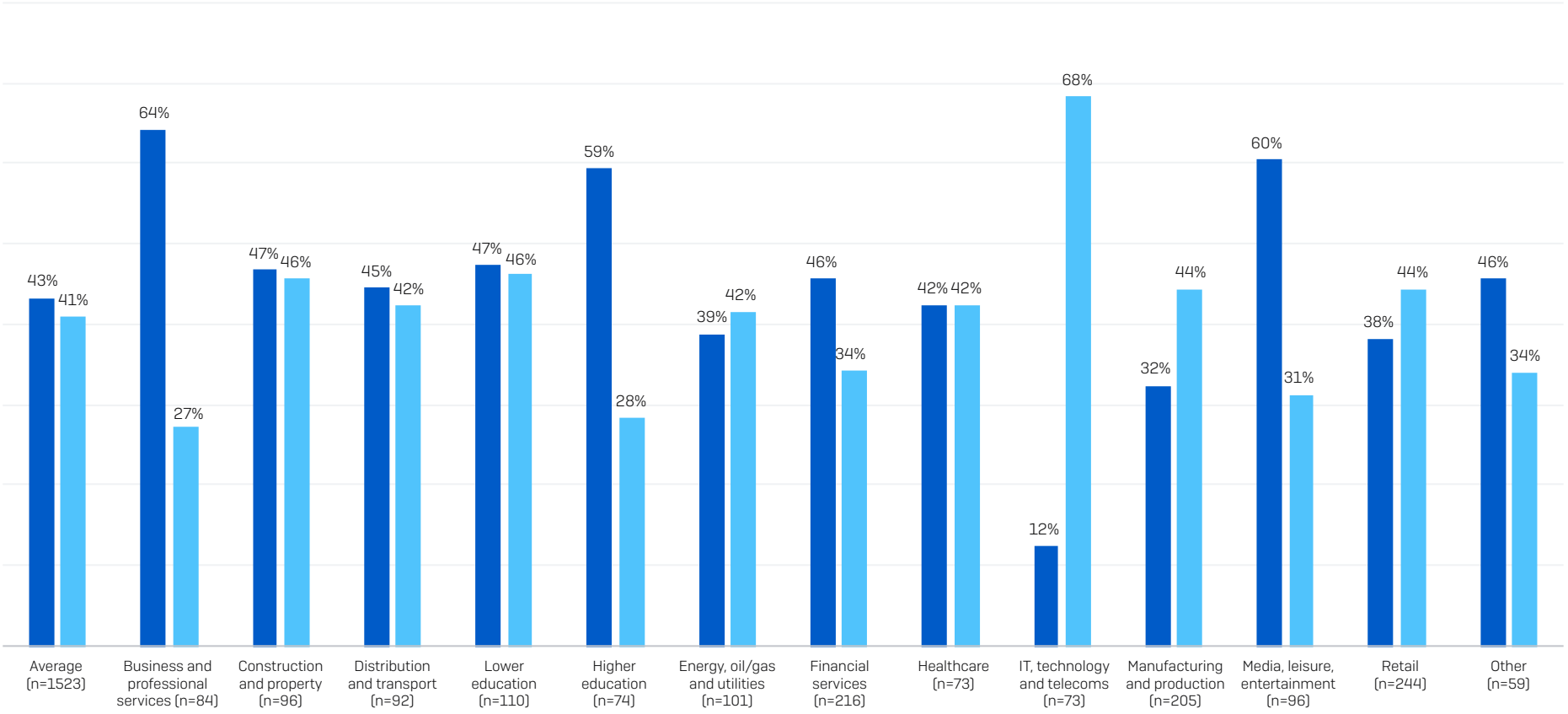
Business Impact

84% of private sector organizations hit by ransomware reported that the attack caused them to lose business/revenue. Annual revenue had a relatively small impact on loss of business, with the lowest rate (79%) reported by the $250 million - $500 million cohort and the highest rate (88%) by those with less than $10 million and those with more than $5 billion revenue.

Industry type played a much greater role in propensity to lose business/revenue. Overall, lower education (94%) and construction and property (93%) were most likely to report some loss of business/revenue due to attacks and the manufacturing and production sector was least likely (77%).

Diving deeper, we see considerable variation in the sectors that reported losing "a lot" of business/revenue, with business and professional services (64%) more than five times more likely than IT, technology, and telecoms (12%) to have experienced this level of impact.

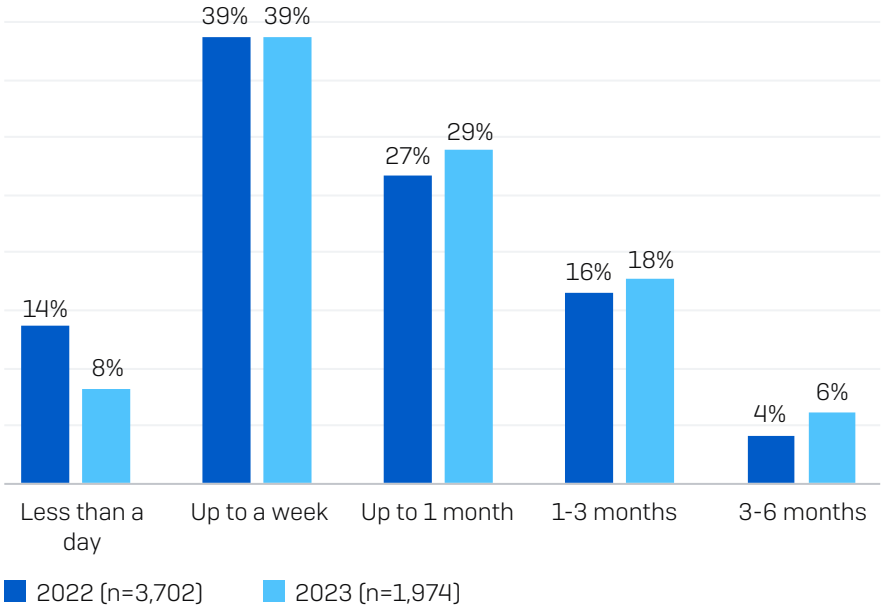
Loss of Business/Revenue by Industry



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

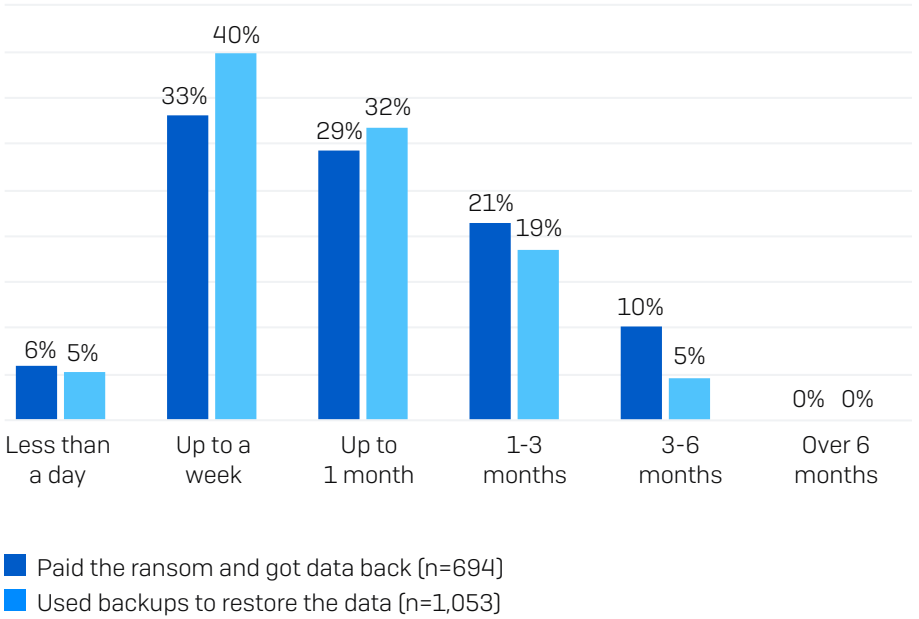
While the time to recover from a ransomware attack is broadly in line with the 2022 report, the percentage that were able to recover in less than a day has dropped from 14% to 8%.



How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart

Recovery time by data recovery method

The research revealed that organizations that use backups to recover their data recover from the attack more quickly than those that pay the ransom. 45% of those that used backups recovered within a week, compared with 39% of those that paid the ransom. Almost one third (32%) of those that paid the ransom took more than a month to recover, while the figure for those that used backups is 23% (with rounding). 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

Independent of revenue, geography, or industry, ransomware continues to be major threat to organizations. As adversaries continue to hone their attack tactics, techniques, and procedures (TTPs), defenders are struggling to keep pace, resulting in increased encryption rates.

The drop in the use of backups to recover encrypted data is considerable cause for concern. If further evidence was needed regarding the financial and operational benefits of investing in a strong backup strategy, this report provides it.

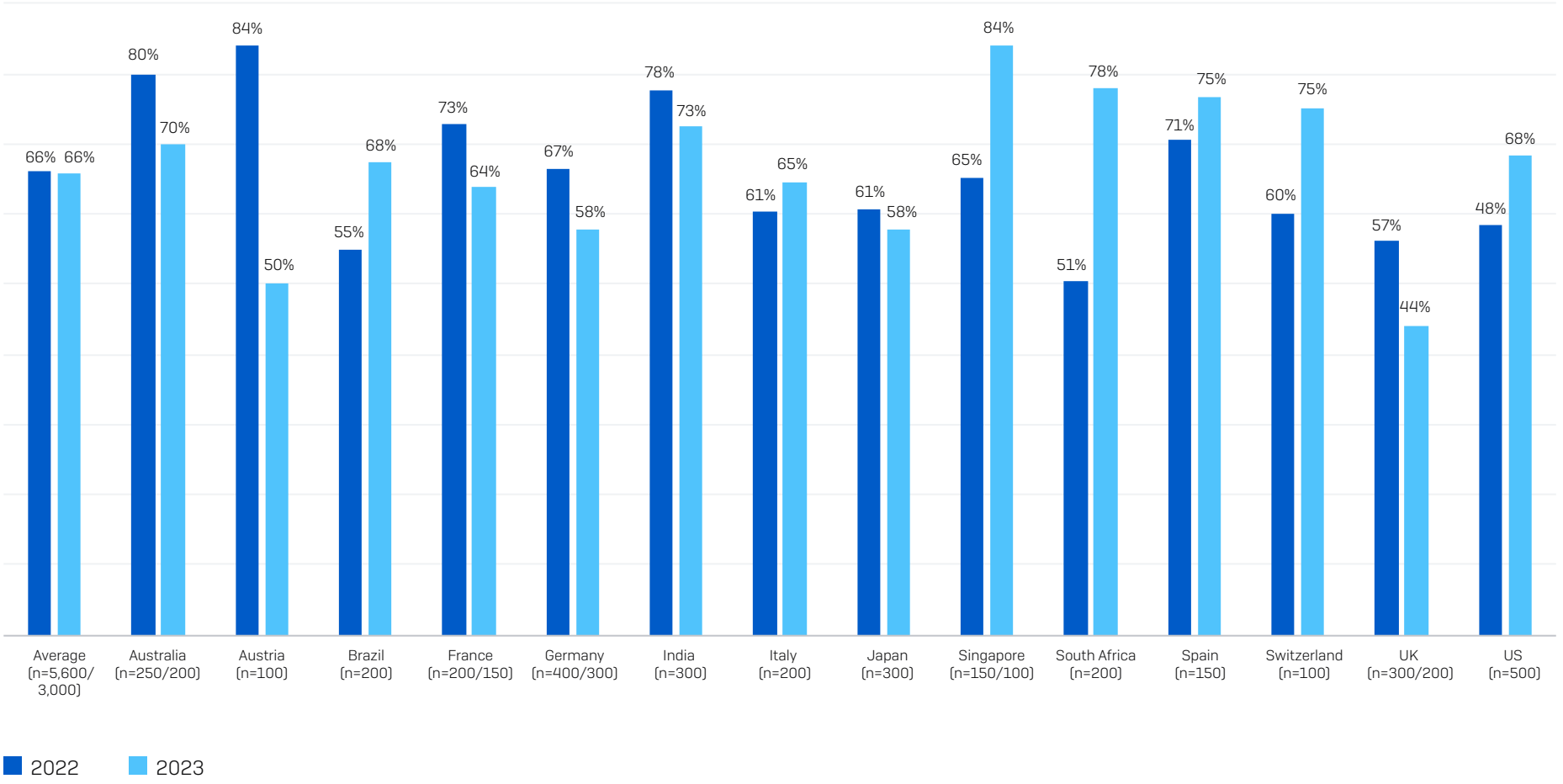
With the growth of the ransomware-as-a-service business model, we do not anticipate a drop in attacks in the coming year. Organizations should focus on:

- 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

Rate of Ransomware Attacks by Country: 2022 vs. 2023

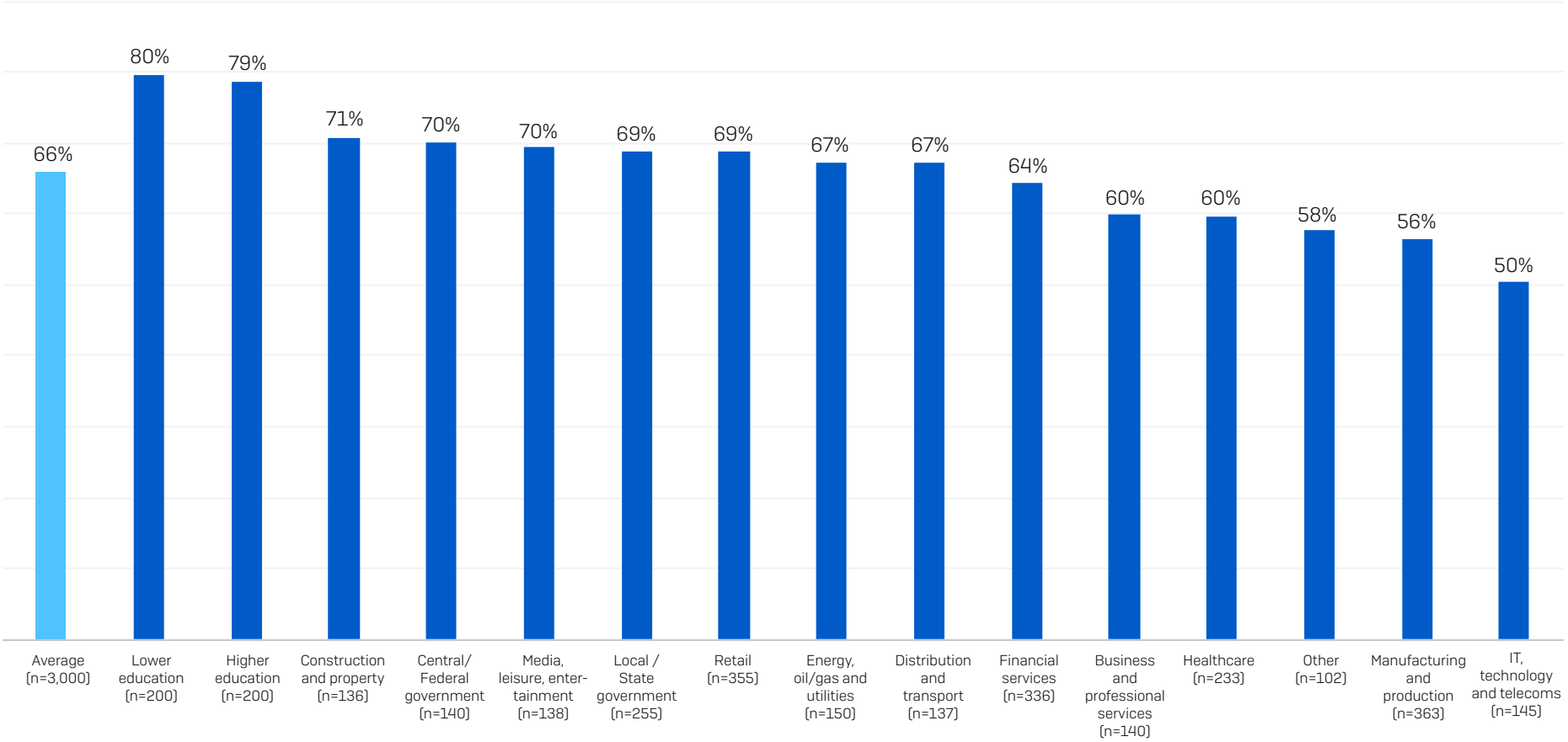
Percentage of Organizations Hit by Ransomware



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

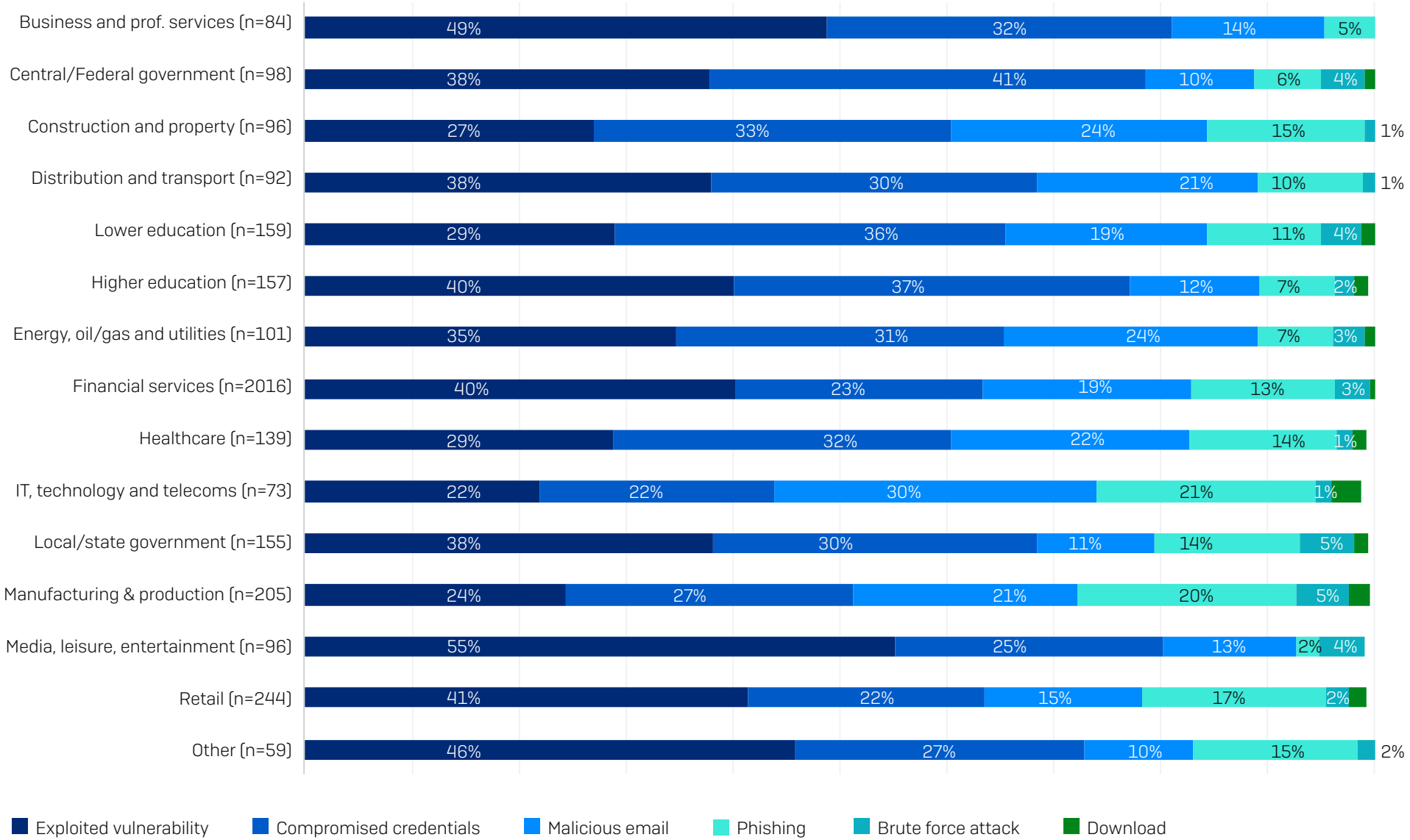
Rate of Ransomware Attacks by Industry

Percentage of Organizations Hit by Ransomware



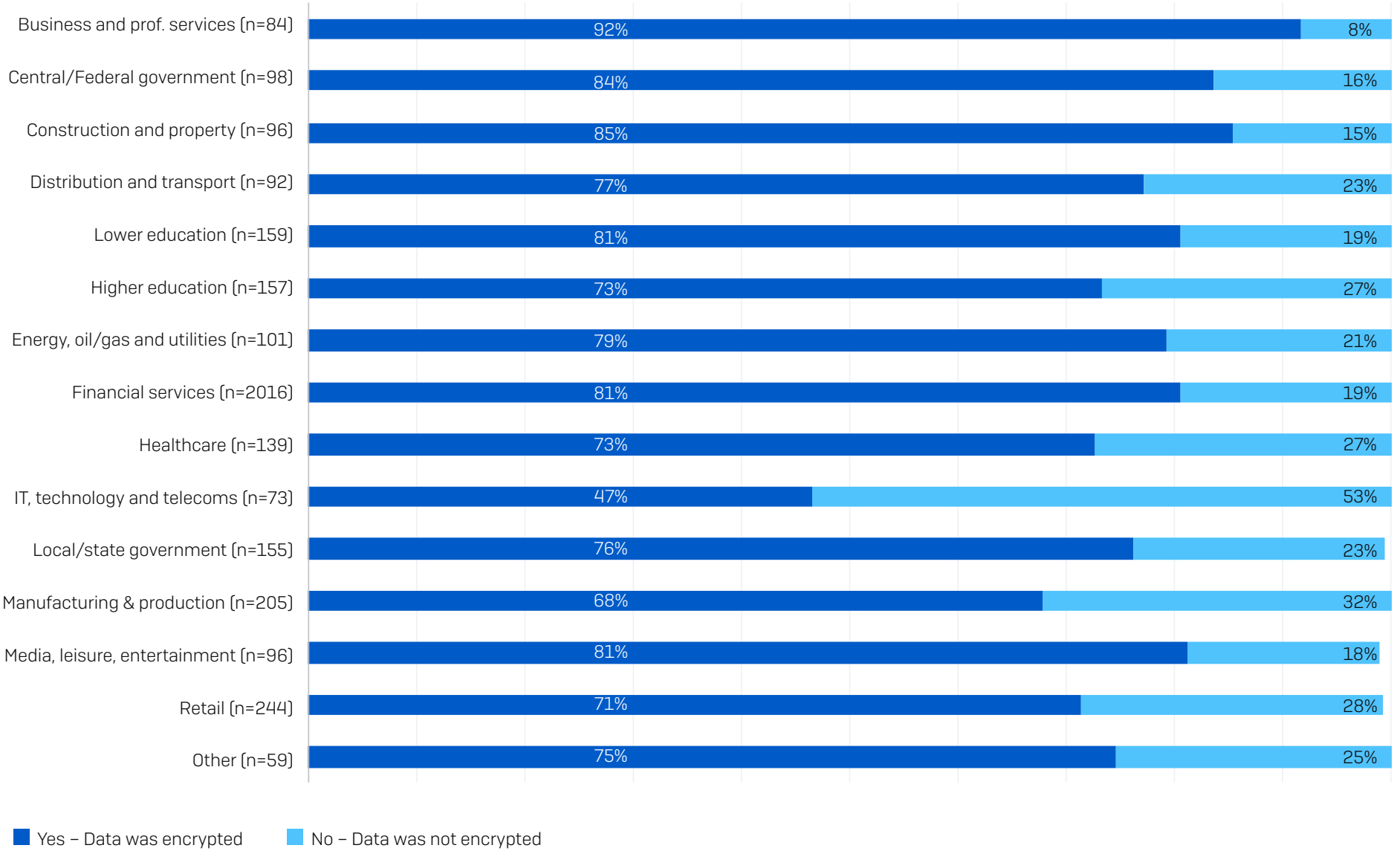
In the last year, has your organization been hit by ransomware? Base numbers in chart

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



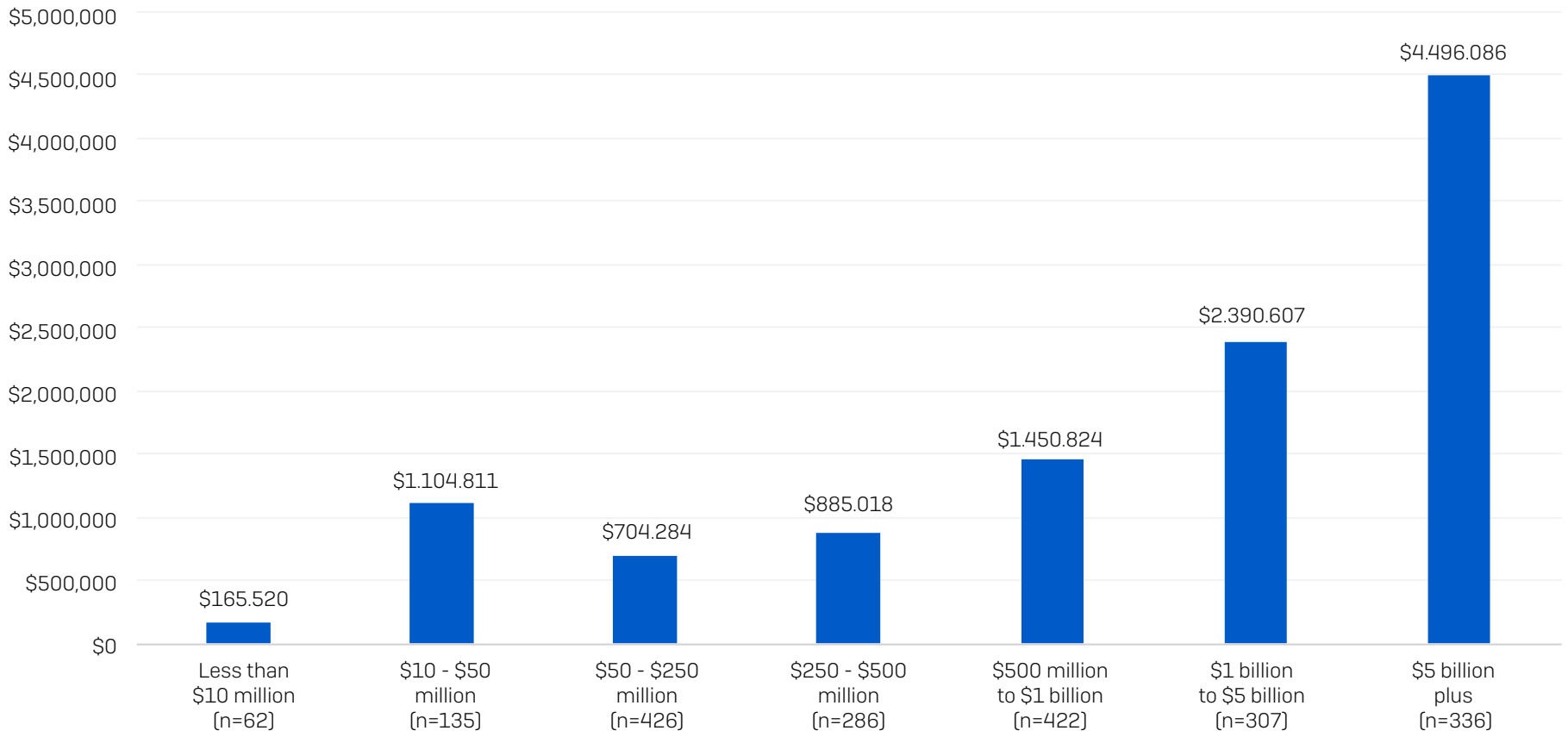
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Consolidation of answer options. Base numbers in chart

Data Recovery by Country

Did your organization get any data back?

	US (N=274)	BRAZIL (N=98)	GERMANY (N=122)	AUSTRIA (N=48)	SWITZER-LAND (N=68)	UK (N=66)	ITALY (N=82)	SPAIN (N=93)	FRANCE (N=68)	SOUTH AFRICA (N=139)	INDIA (N=167)	AUSTRALIA (N=96)	JAPAN (N=125)	SINGA-PORE (N=51)
Yes, we paid the ransom and got data back	54%	55%	44%	42%	38%	44%	54%	29%	22%	45%	43%	53%	52%	53%
Yes, we used backups to restore the data	66%	61%	78%	73%	84%	68%	55%	81%	87%	76%	73%	73%	60%	57%
Yes, we used other means to get our data back	1%	4%	1%	0%	3%	0%	0%	0%	3%	3%	3%	3%	6%	0%
No, even though we paid the ransom	1%	0%	0%	0%	0%	5%	2%	0%	3%	0%	1%	0%	0%	0%
No, we didn't pay the ransom	0%	1%	2%	2%	1%	2%	5%	2%	0%	0%	1%	1%	5%	10%
Don't know	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Got data back via any method	99%	99%	95%	98%	99%	94%	93%	98%	97%	100%	98%	99%	95%	90%
Use more than one method to recover data	22%	21%	27%	17%	26%	18%	16%	12%	12%	24%	20%	29%	22%	20%
Paid the ransom	55%	55%	44%	42%	38%	48%	56%	29%	25%	45%	44%	53%	52%	53%
Percentage of those that paid the ransom that didn't get data back	1%	0%	0%	0%	0%	9%	4%	0%	12%	0%	3%	0%	0%	0%

Mean Recovery Cost by Revenue



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.

Research Methodology

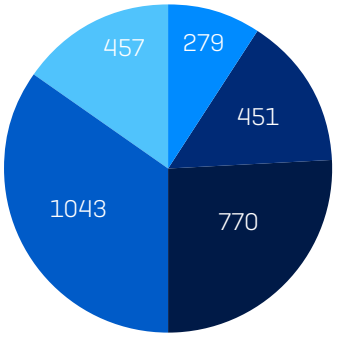
Sophos commissioned an independent, vendor-agnostic survey of 3,000 cybersecurity/IT leaders that was conducted between January and March 2023. Respondents were based in 14 countries across the Americas, EMEA, and Asia Pacific.

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.

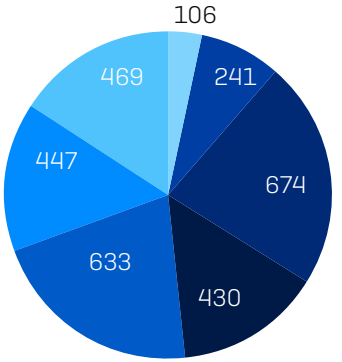
Respondents by Country

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.

2023-05-05 (WP-DD)