SOPHOS

The State of Ransomware 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity across 14 countries, conducted in January-February 2024.

A Sophos Whitepaper. April 2024

Introduction

The fifth Sophos annual study of the real-world ransomware experiences of organizations around the globe explores the full victim journey, from root cause through to severity of attack, financial impact, and recovery time. Fresh new insights combined with learnings from our previous studies reveal the realities facing businesses today as well as how the impact of ransomware has evolved over the last five years.

This year's report also incorporates brand new areas of study, including exploration of ransom demands vs. ransom payments, together with a heightened focus on the impact an organization's revenue has on their ransomware outcomes. Plus, for the first time, it shines a light on the role of law enforcement in ransomware remediation.

A note on reporting dates

To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2024. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2023.

About the survey

The report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. All respondents represent organizations with between 100 and 5,000 employees. The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants 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).

Rate of Ransomware Attacks

59% of organizations were hit by ransomware last year, a small but welcome drop from the 66% reported in both the previous two years. While any reduction is encouraging, with more than half of organizations experiencing an attack, this is no time to lower your guard.

2020	2021	2022	2023	2024
51%	37%	66%	66%	59%

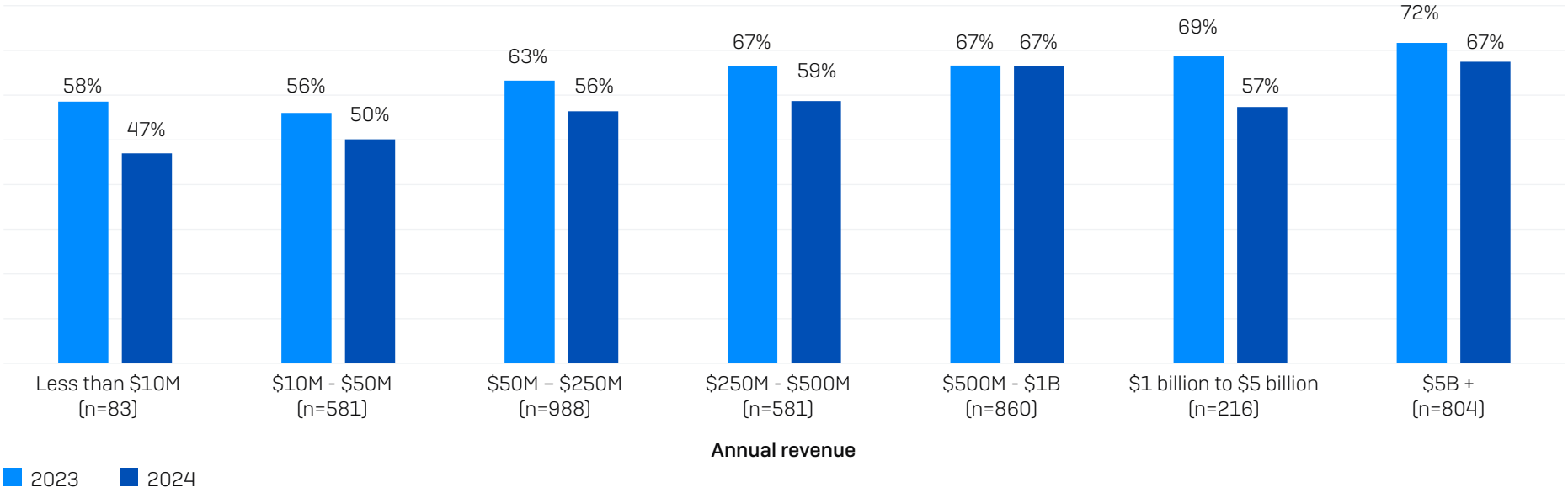
In the last year, has your organization been hit by ransomware?
Yes. n=5,000 (2024), 3,000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020).

Attacks by Revenue

Encouragingly, all revenue segments reported a reduction in ransomware attack rate in the last year (although for $500M - $1B it was less than one percentage point).

The propensity to be hit by ransomware generally increases with revenue, with $5B+ organizations reporting the joint highest rate of attack (67%). However, even the smallest organizations (less than $10M revenue) are still regularly targeted, with just under half (47%) hit by ransomware in the last year. While many ransomware attacks are executed by sophisticated, well-funded gangs, the use of crude, cheap ransomware by lower-skilled threat actors is on the rise.

Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2024), 3,000 (2023). 2024 segment base numbers in chart.

Attacks by Industry

With a few exceptions, ransomware attack rates were broadly consistent across the different sectors, with between 60% and 68% of organizations hit in 11 of the 15 industries covered. The notable winners in this year's study are *state/local government* (34%) and *retail* (45%) where fewer than half of respondents reported being hit in the last year.

Interestingly, the two government sectors occupy opposing positions, with *central/federal government* reporting the highest attack rate across all industries (68%), double the rate reported by *state/local government* (34%). At the same time, reflecting the general downward trend in attacks, the *central/federal government* rate is lower than the sector's 2023 figure of 70%.

There are several possible reasons behind this government variance. In a year of widespread unrest, it may be that central governments have experienced an increase in politically motivated attacks. The results could also reflect efforts over the last year by state/local government organizations to strengthen their resilience to attack – or a shift in approach by adversaries in response to the state/local government sector's limited ability to pay ransoms.

Other notable industry changes over the last year include:

- Reduction in the highest individual rate of attack reported, down from 80% (*lower education*) to 69% (*central/federal government*)
- The education sector no longer reports the two highest rates of attack, coming in at 66% (*higher education*) and 63% (*lower education*) this year vs. 79% and 80% respectively last year
- *Healthcare* was one of five sectors that reported an increase in attack rate over the last year, up from 60% to 67%
- *IT, telecoms, and technology* no longer has the lowest attack rate with 55% of organizations hit in the last year, an increase from the 50% reported in 2023

See the appendix for a detailed breakdown of rate of ransomware attacks by industry.

Attacks by Country

France reported the highest rate of ransomware attacks in 2024 with 74% of respondents saying they had been hit in the last year, followed by South Africa (69%) and Italy (68%). Conversely, the lowest reported attack rates were by respondents in Brazil (44%), Japan (51%), and Australia (54%).

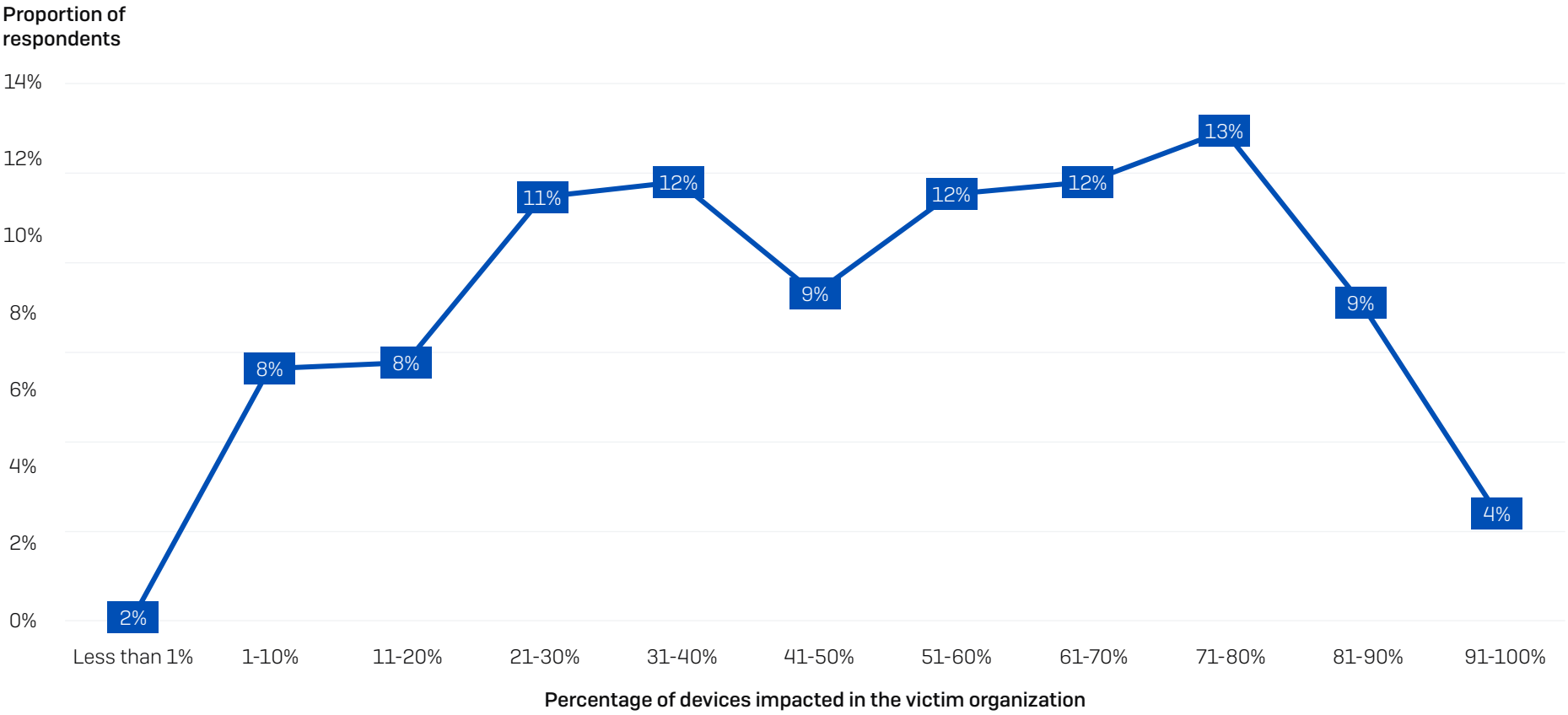
Overall, nine countries reported a lower attack rate than in 2023. The five countries that reported a higher rate of attack than in 2023 are all in Europe: Austria, France, Germany, Italy, and the UK (Germany's increase was less than 1%). This may reflect an increase in targeting of European organizations or that European defenses have been less able to keep pace with the evolving attacker behaviors than in other geographies.

See the appendix for a detailed breakdown of rate of ransomware attacks by country.

Percentage of Computers Impacted

On average, just under half (49%) of an organization's computers are impacted by a ransomware attack. Having your full environment encrypted is extremely rare, with only 4% of organizations reporting that 91% or more of their devices were impacted. At the other end of the scale, while some attacks do impact only a handful of devices, this too is highly unusual, with only 2% of affected organizations saying that fewer than 1% of their devices were affected.

Percentage of devices impacted in the victim organization



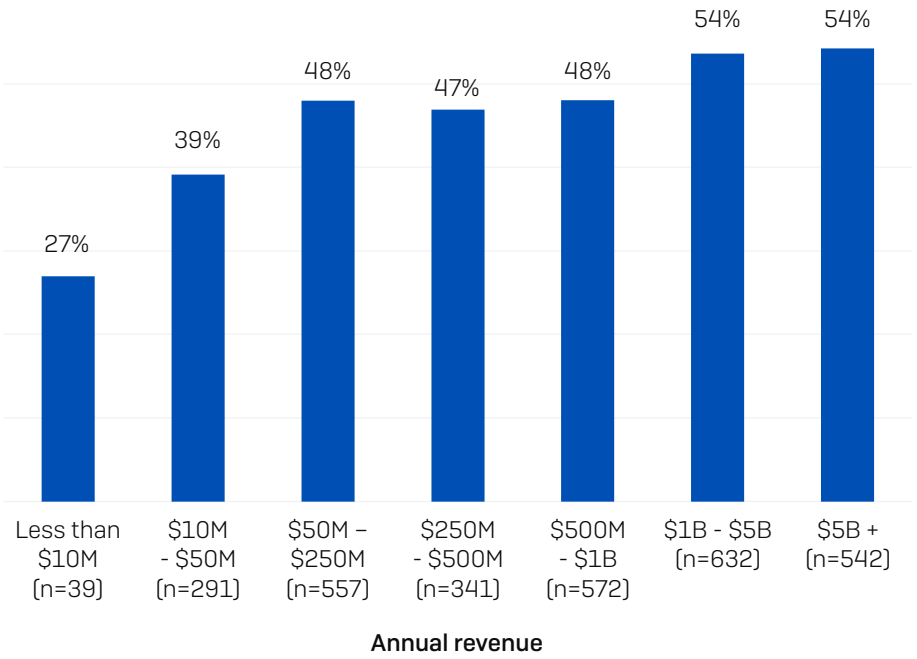
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware.

Percentage of Computers Impacted by Revenue

While globally, across all respondents, the distribution was broad, we see considerable variation in devices impacted both by organization size and industry.

As revenue increases, so does the proportion of the computer estate that was impacted in the ransomware attack, with the smallest organizations (less than $10M) reporting half the percentage of devices impacted compared to those with revenue of $1B or more (27% vs. 54%).

There are several factors that may contribute to this finding. Smaller organizations are less likely to centrally manage all their devices, reducing the opportunity for attacks to spread across the estate. Additionally, most small businesses and startups are heavy users of SaaS platforms, reducing the risk of business outage from threats like ransomware.



What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware.

Percentage of Computers Impacted by Industry

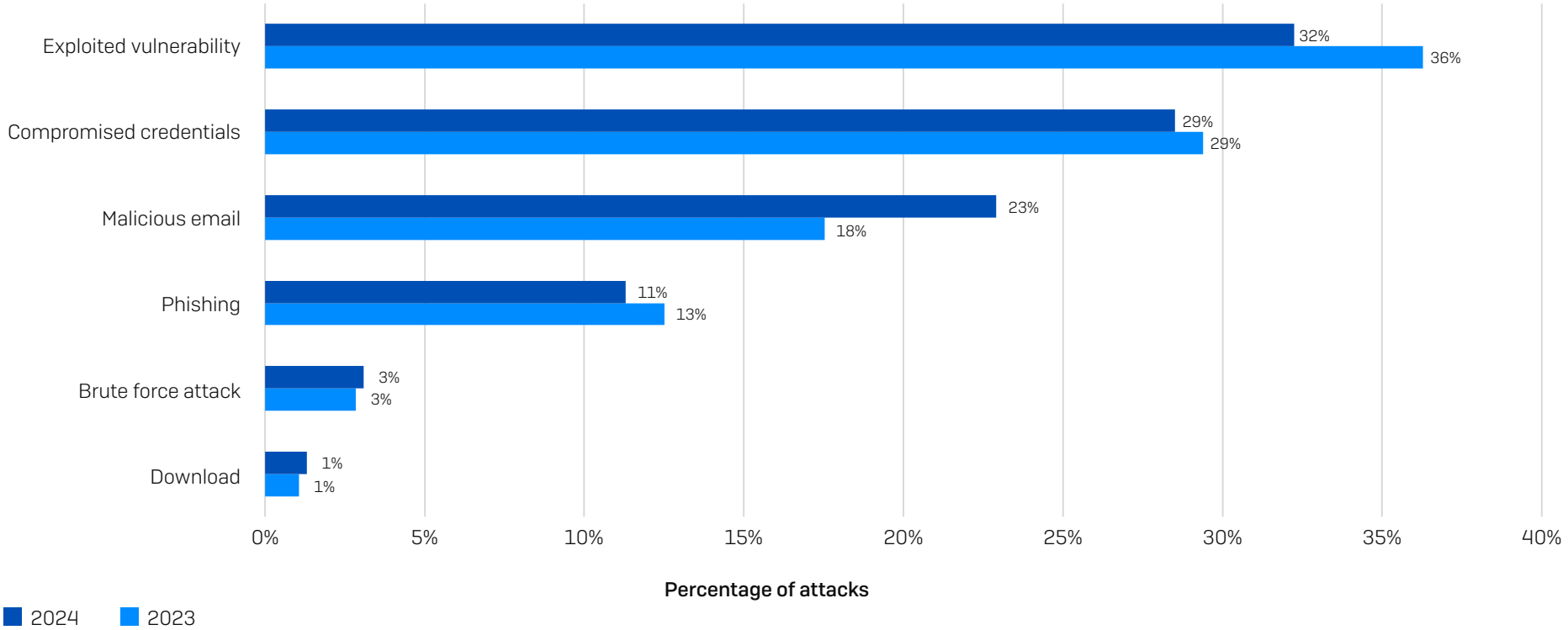
IT, technology and telecoms reported the smallest percentage of devices impacted (33%), reflecting the strong cyber posture that is often seen in this sector. Conversely, *energy, oil/gas and utilities* is the sector where the effects of an attack are most broadly experienced, with 62% of devices impacted, on average, followed by *healthcare* (58%). Both industries are challenged by higher levels of legacy technology and infrastructure controls than most other sectors, which likely makes it harder to secure devices, limit lateral movement, and prevent attacks from spreading.

See the appendix for a detailed breakdown of percentage of computers impacted by industry.

Root Causes of Ransomware Attacks

99% of organizations hit by ransomware were able to identify the root cause of the attack, with exploited vulnerabilities the most commonly identified starting point for the second year running. Overall, the running order remained consistent with our 2023 study.

Email-based approaches were identified as the root cause of attack by 34% of respondents, with around twice as many starting with a malicious email (i.e., a message with a malicious link or attachment that downloads malware) as phishing (i.e., a message designed to trick readers into revealing information). It's worth noting that phishing is typically used to steal log-in details and as such can be considered the first step in a compromised credentials attack.



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=2,974 organizations hit by ransomware.

Exploited Vulnerability Attacks

While all ransomware attacks have negative outcomes, some are more devastating than others. Organizations whose attacks began with exploitation of an unpatched vulnerability report considerably more severe outcomes than those where the attack started with compromised credentials, including a higher propensity to:

- Have backups compromised (75% success rate vs. 54% for compromised credentials)
- Have data encrypted (67% encryption rate vs. 43% for compromised credentials)
- Pay the ransom (71% payment rate vs. 45% for compromised credentials)
- Cover the full cost of the ransom in-house (31% funded the full ransom in-house vs. 2% for compromised credentials)

They also reported:

- 4X higher overall attack recovery costs ($3M vs. $750K for compromised credentials)
- Slower recovery time (45% took more than a month vs. 37% for compromised credentials)

For a deeper dive, read Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector.

Root Cause by Industry

Certain weaknesses in cyber defenses are more prevalent in some sectors than others, and adversaries are quick to take advantage. As a result, the root cause of ransomware attacks varies considerably by industry:

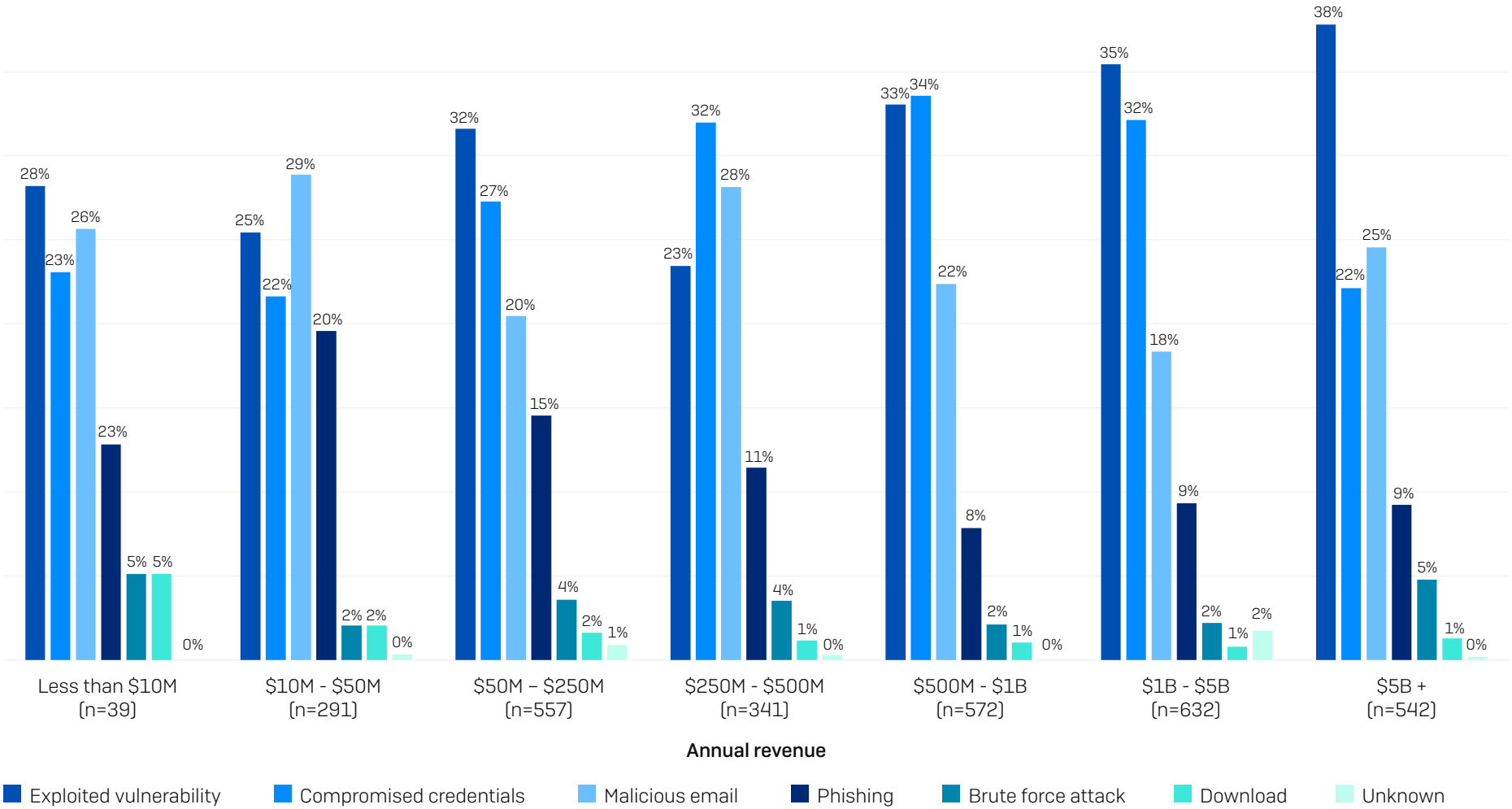
- *Energy, oil/gas and utilities* is the sector most likely to fall victim to the exploitation of unpatched vulnerabilities, with almost half (49%) of attacks beginning in this way. This industry typically uses a higher proportion of older technologies more prone to security gaps than many other sectors, and patches may not be available for legacy and end-of-life solutions
- Government organizations are particularly vulnerable to attacks that start with abuse of compromised credentials: 49% (*state/local*) and 47% (*central/federal*) of attacks began with the use of stolen login data
- *IT, technology and telecoms* and *retail* both reported that 7% of ransomware incidents began with a brute force attack – it may be that their reduced exposure to unpatched vulnerabilities and compromised credentials forces adversaries to focus, in part, on other approaches

See the appendix for a detailed breakdown of rate of the root cause of attack by industry.

Root Cause by Revenue

Generally speaking, larger organizations are more likely to experience an attack that starts with an unpatched vulnerability, with the $5B+ segment reporting the highest percentage of attacks that started in this way (38%). It is likely that IT infrastructures increase in both size and complexity as organizations grow, making it harder for IT teams to see all their exposures and patch before they are exploited.

Compromised credentials as a ransomware attack vector peaks in the mid/high revenue cohorts and is the top cause of attack in both the $250M-$500M and $500M-$1B segments. While vulnerabilities and compromised credentials rightly get a lot of focus, malicious email is the top reported root cause in $10M-$50M organizations. Overall, email-based threats account for just under half (49%) of attacks in this space.



Do you know the root cause of the ransomware attack your organization experienced in the last year? n=2,974 organizations hit by ransomware.

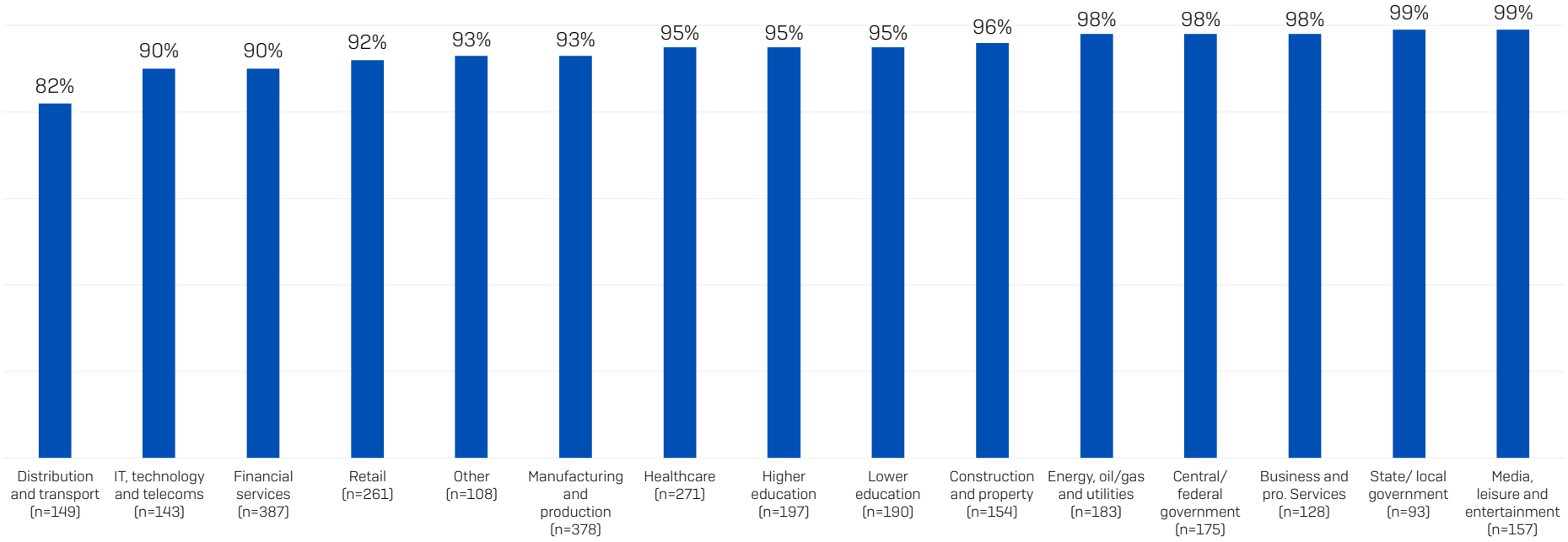
Backup Compromise

There are two main ways to recover encrypted data in a ransomware attack: restoring from backups and paying the ransom. Compromising an organization's backups enables adversaries to restrict their victim's ability to recover encrypted data and dials up the pressure to pay the ransom.

Attempted Backup Compromise

94% of organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. This rose to 99% in both *state/local government*, and the *media, leisure and entertainment* sector. The lowest rate of attempted compromise was reported by *distribution and transport*, however even here more than eight in ten (82%) organizations hit by ransomware said the attackers tried to access their backups.

Percentage of attacks where adversaries attempted to compromise backups



Did the cybercriminals try to compromise your organization's backups? Yes. Base number in chart.

Success Rate of Backup Compromise Attempts

Across all sectors, 57% of backup compromise attempts were successful, meaning that adversaries were able to impact the ransomware recovery operations of over half of their victims. The analysis revealed considerable variation in adversary success rate by sector:

- Attackers were most likely to successfully compromise their victims' backups in the *energy, oil/gas and utilities* (79% success rate) and *education* (71% success rate) sectors
- *IT, technology and telecoms* (30% success rate) and *retail* (47% success rate) reported the lowest rates of successful backup compromise

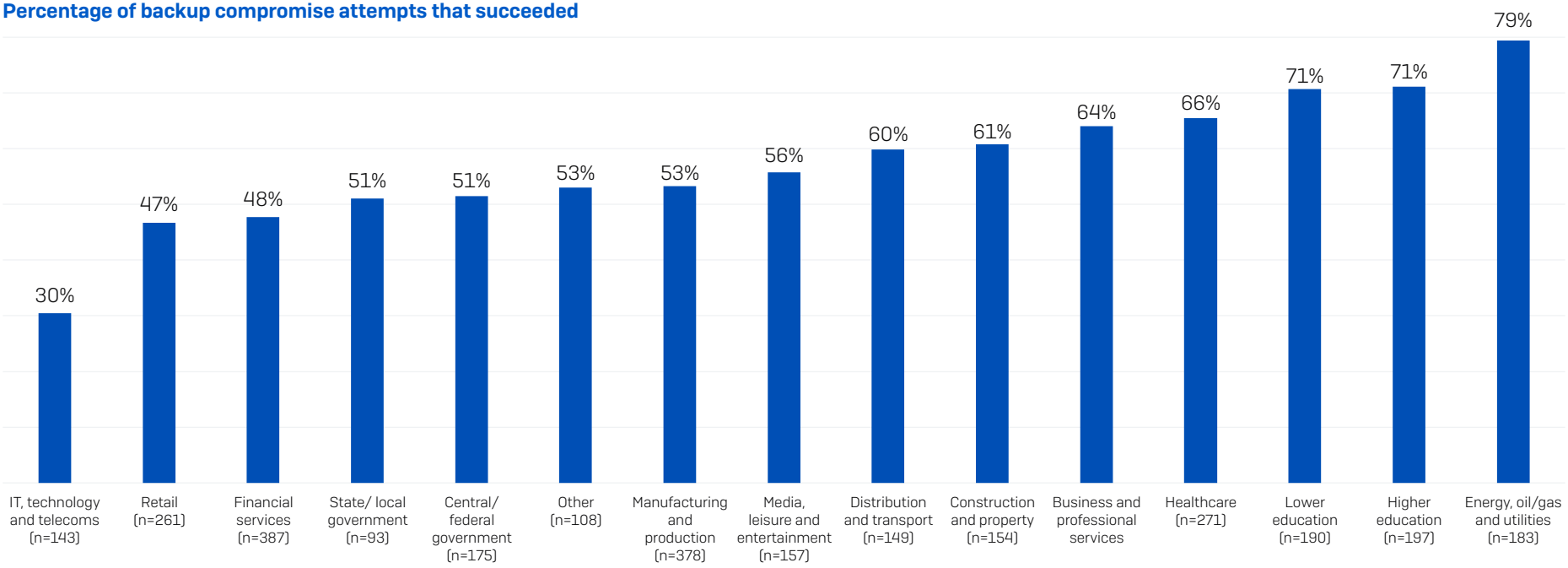
There are several possible reasons behind the differing success rates. It may be that *IT, telecoms and technology* had stronger backup protection in place to start with so was more resilient to attack than other sectors. They may also be more effective at detecting and stopping attempted compromise before the attackers could succeed.

Whatever the cause, organizations that had backups compromised reported considerably worse outcomes than those whose backups were not breached:

- Ransom demands were, on average, more than double that of those whose backups weren't impacted ($2.3M vs. $1M median initial ransom demand)
- Organizations whose backups were compromised were almost twice as likely to pay the ransom to recover encrypted data (67% vs. 36%)
- Median overall recovery costs came in eight times higher ($3M vs. $375K) for those that had backups compromised

For a deeper dive, read The Impact of Compromised Backups on Ransomware Outcomes.

Percentage of backup compromise attempts that succeeded



Did the cybercriminals try to compromise your organization's backups? Yes, Base number in chart.

Rate of Data Encryption

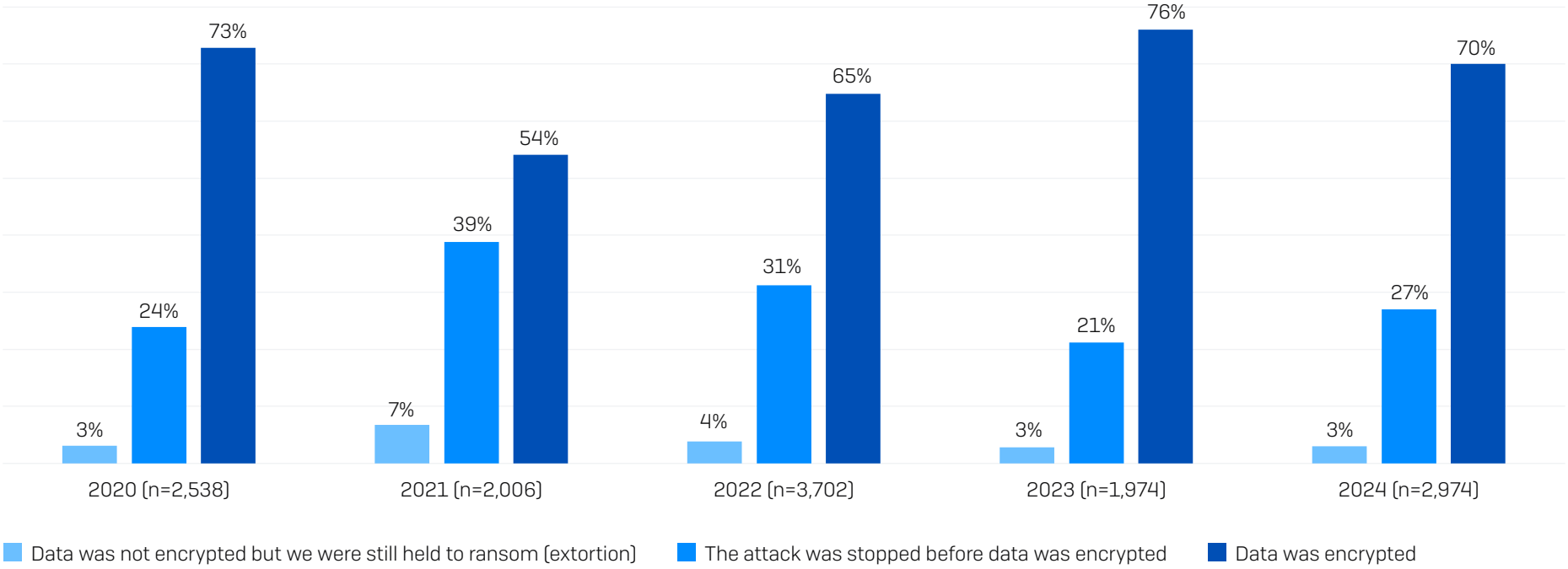
Seven in ten (70%) ransomware attacks in the last year resulted in data encryption. While high, this rate represents a small drop from the 76% of attacks where adversaries succeeded in encrypting data that was reported in 2023.

Data Encryption Rate by Industry

The 2024 survey reveals considerable variation in encryption rate across industries.

- While *state/local government* reported the lowest frequency of attack this year (34% hit by ransomware), it also reported the **highest rate of data encryption**, with 98% of attacks resulting in data being encrypted
- *Financial services* (49%) followed by retail (56%) reported the **lowest rates of data encryption**
- *Distribution and transport* is the sector most likely to have experienced an **extortion-based attack** with 17% saying that data was not encrypted but they were held to ransom anyway – almost three times the rate of any other sector

See the appendix for a detailed breakdown of data encryption rates by industry.



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base number in chart.

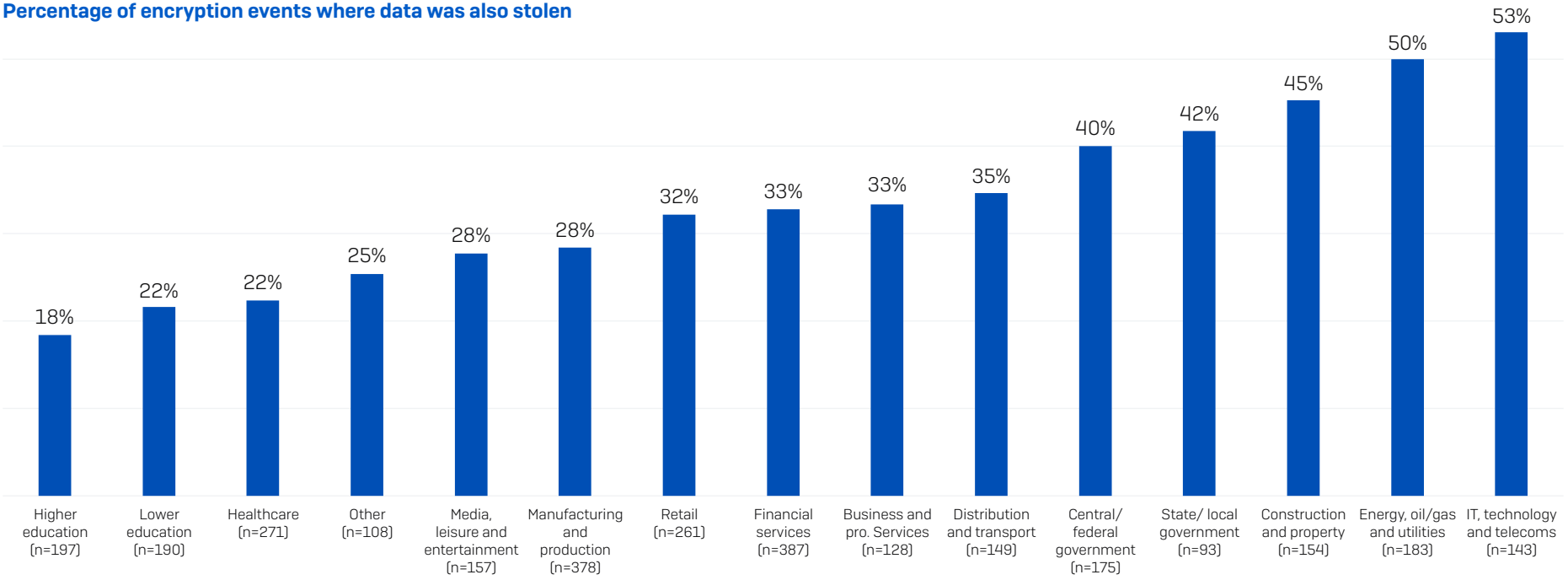
Data Theft

Adversaries don't just encrypt data; they also steal it. In 32% of incidents where data was encrypted, data was also stolen – slightly above last year's rate of 30%. Data theft increases attackers' ability to extort money from their victims, while also enabling them to further monetize the attack by selling the stolen data on the dark web.

Again, there is considerable variation by industry. On the surface *IT, technology and telecoms* fares worst, with 53% of attacks where data was encrypted reporting that it was also stolen. *Energy, oil/gas and utilities* is in second position, with data stolen in 50% of encryption events. Conversely, the education sector is least likely to report data theft in an attack, with *higher education* reporting the lowest overall propensity to have data encrypted and stolen (18%), followed by *lower education*, which shares second spot with healthcare (both 22%).

The findings may reflect differing levels of investigation capabilities across the sectors, and differing priorities. Determining whether data has been exfiltrated requires higher levels of forensic capabilities and often relies on logs from EDR/XDR tools. It may be that the *IT, technology and telecoms* sector is simply better able to identify data theft than other industries. The simplicity of many *energy, oil/gas and utilities* environments may also make theft easier to detect in this sector. Conversely, schools often lack the skills and tools to determine whether data has been stolen. At the same time, some organizations may prefer not to know if data has been exfiltrated as a data breach would require them to undertake expensive disclosures.

Percentage of encryption events where 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. Base number in chart.

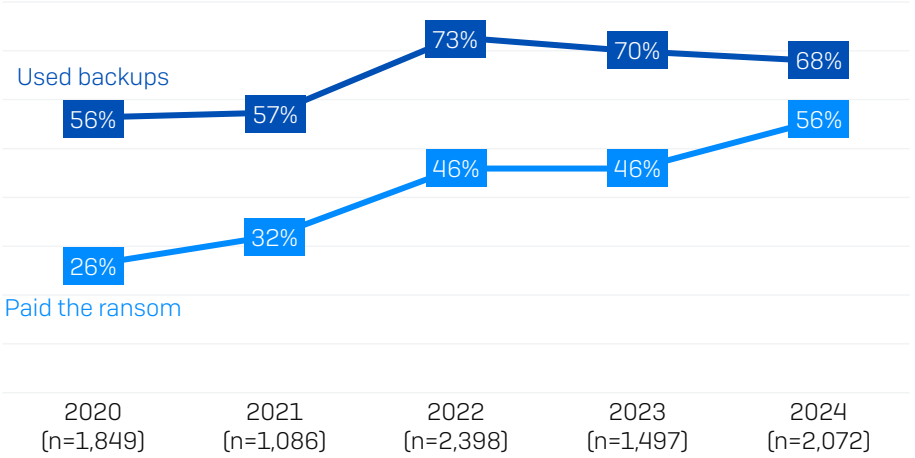
Data Recovery

98% of organizations that had data encrypted got data back. The two primary ways of recovering data were restoring from backups (68%) and paying the ransom to get the decryption key (56%). 26% of those that had data encrypted indicated that they used "other means" to get data back – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
68%	**56%**	**26%**

A notable change over the last year is the increase in propensity for victims to use multiple approaches to recover encrypted data (e.g., paying the ransom and using backups). Almost half of organizations that had data encrypted reported using more than one method (47%) this time around, more than double the rate reported in 2023 (21%).

The five-year view reveals that the gap between use of backups and payment of the ransom continues to shrink. Backup use has fallen, albeit slightly, for the second consecutive year. At the same time, there has been a 10-percentage point increase in ransom payments since the 2023 study. Propensity to pay the ransom depends on many factors, including availability of backups. However, this is a worrying trend and it is concerning that over half of victims are resorting to paying for the decryption key.



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 Revenue

Propensity to pay the ransom to recover data generally increases with revenue. The smallest revenue organizations (less than $10M) report by far the lowest ransom payment rate (25%) while the largest revenue organizations ($5B+) have the highest payment rate (61%). The fundamental availability of funds to cover the ransom is likely a major factor at play here – many very small businesses are simply unable to find the money to pay a ransom.

However, as we've seen, data recovery is not a case of either backups or ransom. The nuances behind data recovery methods become apparent when we dive deeper into the data and compare the 2024 figures with last year's results.

Outside the sub $10M group, all revenue segments reported an increased ransom payment rate compared to last year, and three of them also reported an increase in the use of backups to restore the data. While the lowest revenue group reported the highest rate of backup use (88%), the $250M-$500M was close behind (85%).

Data Recovery by Industry

Perhaps unsurprisingly, *central/federal government* is the sector least likely to pay the ransom to get data back – no doubt it is highly limited in the ability to pay by regulations – and also reported the highest use of backups to restore data (39% and 81% respectively).

Overall, there is no smooth correlation between backup use and ransom payments:

- *Media, leisure and entertainment* reported the highest rate of ransom payment to recover data (69%) and also one of the higher rates of backup use (74%)
- *Energy, oil/gas and utilities* has the lowest level of backup use (51%) and has a ransom payment rate of 61%, lower than four other sectors

See the appendix for a detailed breakdown of data recovery method by industry.

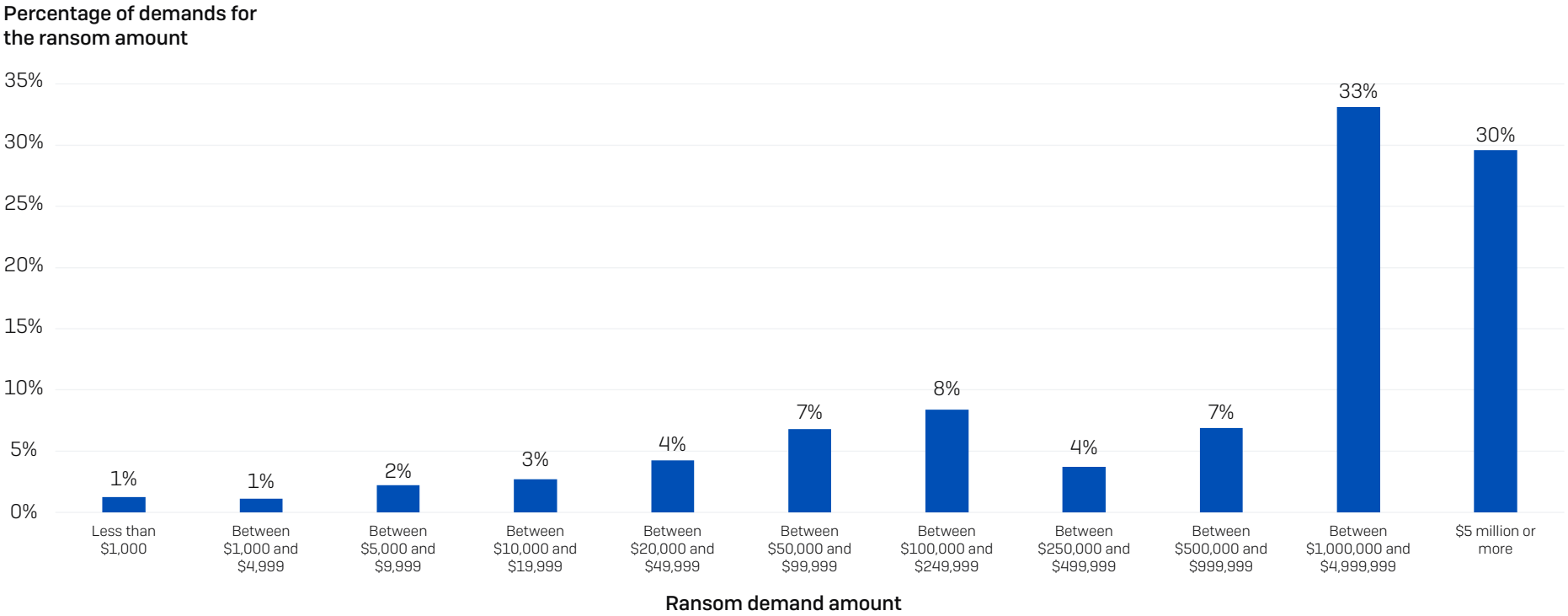
	ANNUAL REVENUE													
	Less than $10M (n=39)		$10M - $50M (n=291)		$50M – $250M (n=557)		$250M - $500M (n=341)		$500M - $1B (n=572)		$1B - $5B (n=632)		$5B + (n=542)	
Data recovery method used	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Used backups to restore the data	80%	88% ▲	72%	68% ▼	77%	60% ▼	75%	85% ▲	68%	70% ▲	66%	65% ▼	63%	66% ▲
Paid the ransom and got data back	36%	25% ▼	41%	49% ▲	42%	57% ▲	33%	50% ▲	51%	59% ▲	52%	56% ▲	55%	61% ▲

Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. 2024 base numbers in chart. Arrow indicates increase/decrease vs. 2023.

Ransom Demands

This year, for the first time, we included both ransom demands and payments in this report. Across the 1,701 organizations that had their data encrypted and were able to share the initial ransom demand from the attackers, the average ask was $4,321,880 (mean) and $2M (median).

One of the most notable findings in this year's study is that 63% of ransom demands are for $1M or more, with 30% of demands for $5M or more. While a small number of respondents reported four-figure ransom demands, these are very much in the minority.



How much was the ransom demand from the attacker(s)? n=1,701

Ransom Demand by Revenue

Looking at both mean and median data, the ransom demand trends upward with revenue, indicating that adversaries adjust their ransom demand based – in part, at least – on likely ability to pay.

Huge ransom demands are no longer the preserve of the highest-revenue organizations, and $1M or more asks are now commonplace across the board: 47% of organizations with revenue of $10M-$50M received a seven-figure ransom demand in the last year.

Ransom Demand by Industry

There are no winners here, with all named sectors (excluding "other") reporting median ransom demands of $1M or higher.

- *Retail* and *IT, technology and telecoms* received the lowest median demands ($1M), followed by *construction* ($1.1M)
- *Central/federal government* is the sector with the biggest target on its head, reporting the highest median ($7.7M) and mean (9.9M) demands

See the appendix for a detailed breakdown of ransom demand by industry.

	ANNUAL REVENUE					
Ransom Demand	**$10M - $50M (n=207)**	**$50M – $250M (n=288)**	**$250M - $500M (n=158)**	**$500M - $1B (n=268)**	**$1B - $5B (n=366)**	**$5B + (n=398)**
Mean average	$1,774,941	$1,704,853	$3,407,796	$5,184,024	$4,281,258	$7,467,294
Median average	$330,000	$220,000	$840,000	$2,000,000	$3,000,000	$6,600,000

How much was the ransom demand from the attacker(s)? Base numbers in chart. N.B. "Less than $10M" has been excluded from this table due to the low number of respondents in this revenue segment.

Ransom Payments

1,097 respondents whose organization paid the ransom shared the actual sum paid. Looking at both median and mean averages, we see that ransom payments have increased considerably in the last year:

- Median payment: $2,000,000 (a 5X increase on the $400,000 reported in 2023)
- Mean payment: $3,960,917 (a 2.6X increase on the $1,542,330 reported in 2023)

The chart below makes clear how the proportion of lower ransom payments has steadily decreased over the last three years, while the proportion of very high payments has soared. Paying a seven-figure or more ransom sum is now the norm.

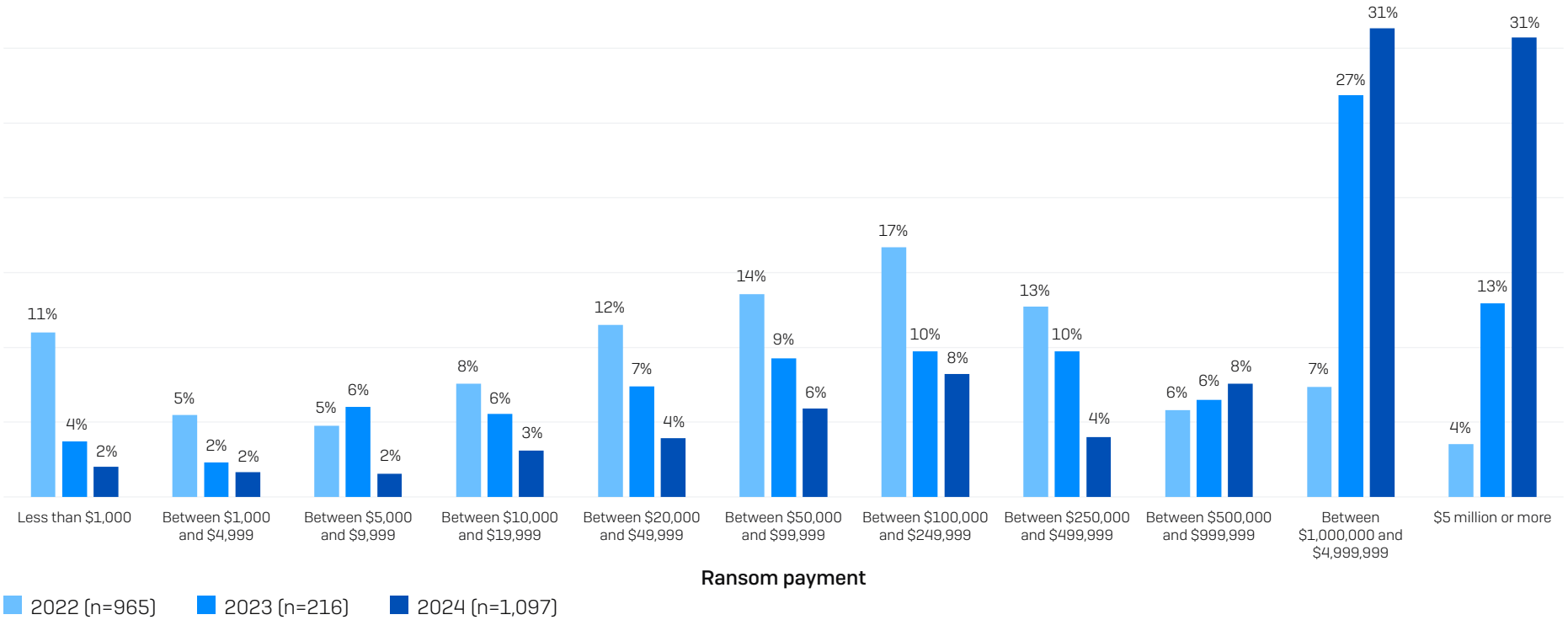
Ransom Payments by Industry

Just as average ransom demands vary considerably by industry, so too do the ransom payments. *IT, technology and telecoms* reported the lowest median ransom payment ($300,000), followed by *distribution and transport* ($440,000). At the other end of the scale, both *lower education* and *central/federal government* paid median ransoms of $6.6M.

While there is a broad correlation between lower demands and lower payments (and vice versa), there are exceptions – notably *distribution and transport*, whose median ransom demand was north of $2.8M but paid, on average, $440,000.

See the appendix for a detailed breakdown of average ransom payment by industry.

Distribution of ransom payments 2022-24



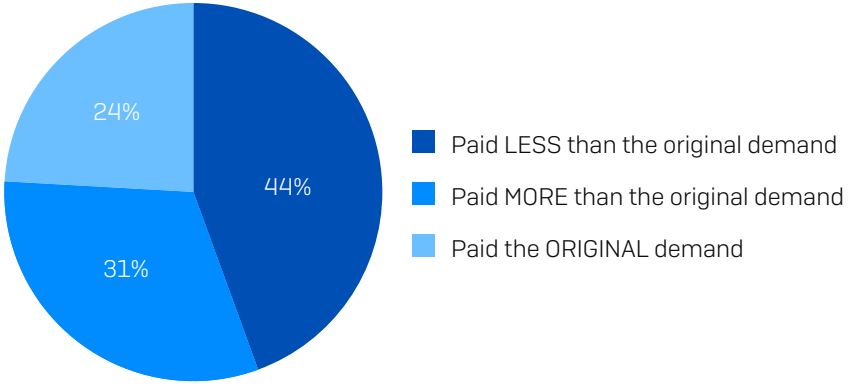
How much was the ransom payment that was paid to the attackers? Base numbers in chart.

Ransom Demand vs. Ransom Payment

When data has been encrypted, it is an incredibly high-pressure time for everyone involved, with both sides trying to optimize their outcomes. Organizations whose data has been encrypted look to minimize the financial impact, while adversaries attempt to secure as much money as possible in the shortest possible timeframe, often using the threat that the ransom will increase if payment is not made by a certain time to pile on further pressure.

Propensity to Negotiate Ransom Amounts

The study has revealed that victims rarely pay the initial sum demanded by the attackers, with only 24% of respondents saying that their payment matched the original request. 44% paid less than the original demand, while 31% paid more.



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097.

Looking at the data by industry, we see that the two services sectors – *business and professional services* and *financial services* – are most likely to negotiate down the ransom payment, with 67% saying that they paid less than the original demand. *Manufacturing and production* is close behind with 65% of organizations paying less than the initial ask.

Conversely, the sectors most likely to pay more than the original demand are those with a high proportion of public sector organizations:

- *Higher education* is most likely to pay more than the original demand (67% paid more), and least likely to pay less than the original demand (20% paid less)
- *Healthcare* was second most likely to pay more than the original demand (57% paid more), followed by *lower education* (55% paid more)

It may be that these industries are less able to access professional ransom negotiators to help reduce their costs. They may also have a greater need to recover the data "at any cost" due to their public remit. Either way, it's clear that there is room for movement between the original demand and the eventual payment.

See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

Proportion of Ransom Demand Paid

While negotiation on the ransom amount occurs in the majority of cases, the eventual movement is relatively small with respondents reporting that 94% of the original demand was paid, on average, across the full cohort.

Diving deeper, we see that all revenue groups except the very largest were able to reduce the size of the ransom payment. The $50M-$250M segment paid the lowest proportion of the initial demand (84%). The only group to pay more than the initial ask is the $5B+ segment which covered, on average, 115% of the ransom demand.

	ANNUAL REVENUE					
Cohort	**$10M - $50M (n=100)**	**$50M – $250M (n=206)**	**$250M - $500M (n=104)**	**$500M - $1B (n=175)**	**$1B - $5B (n=233)**	**$5B + (n=275)**
Proportion of ransom demand paid	93%	84%	90%	88%	85%	115%

How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097. Note: the 'less than $10M' cohort is excluded from the annual revenue breakdown due to very low response base.

Proportion of Ransom Demand Paid by Industry

At an industry level, we see that the sectors most likely to negotiate down the ransom amount also pay the lowest percentage of the initial ask – and vice versa.

LESS THAN 100%	MORE THAN 100%
Manufacturing and production (70%)	Higher education (122%)
Business and professional services (74%)	Lower education (115%)
Financial services (75%)	Healthcare (111%)
Other (79%)	State/local government (104%)
IT, telecoms and technology (82%)	Central/federal government (103%)
Retail (84%)	Energy, oil/gas and utilities (101%)
Construction and property (95%)	
Distribution and transport (95%)	
Media, leisure and entertainment (95%)	

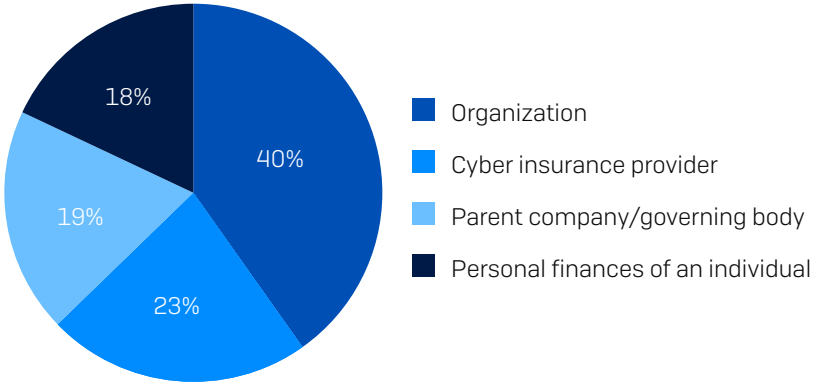
How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=1,097.

Source of Ransom Funding

Who provides the money for the ransom is an area of considerable interest, and the study has revealed a number of insights in this area:

- Funding the ransom is a collaborative effort, with respondents reporting multiple sources of monies in more than four-fifths (82%) of cases
- The primary source of ransom funding is the organization itself, covering 40% of the payment on average; the organization's parent company and/or governing body typically provides 19%
- Insurance providers are heavily involved in ransom payments
  - 23% of all ransom payment funding comes from insurance providers
  - Insurance providers contribute toward the ransom in 83% of attacks
  - However, providers very rarely (1%) cover the full amount and in 79% of cases, the insurer funded less than half of the total payment

Source of ransom payment funding



From which of the following source(s) was the money to fund the ransom payment obtained? n=1,168.

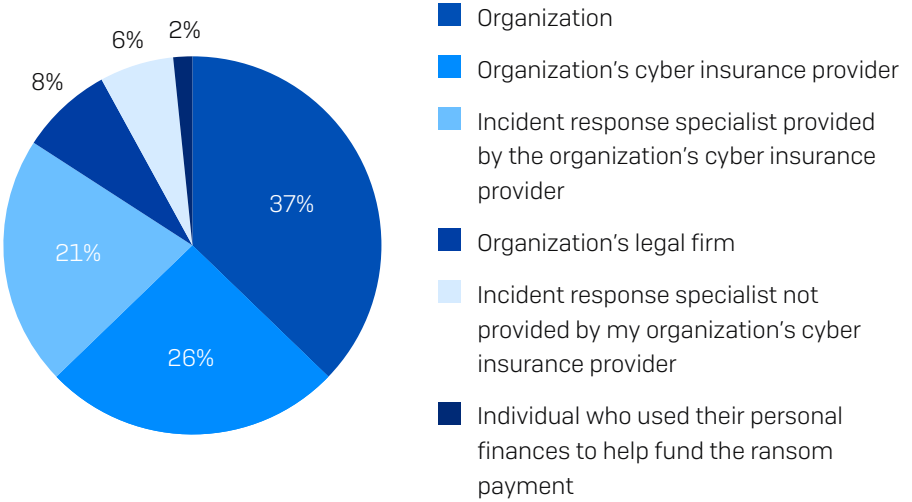
Ransom Transaction Execution

While multiple bodies can contribute to the ransom, funds are typically transferred in a single payment by one party.

Globally, insurance providers transferred the funds for almost half of ransom payments, either directly (26%) or through their appointed incident response specialist (21%). The victim organization made 37% of payments, while 8% were executed by the victim's legal firm.

Overall, 28% (with rounding) of transfers were made by incident response specialists, whether appointed by the insurance provider (21%) or another party, typically the victim (6%).

Executor of ransom payment transfer



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=1,168.

Recovery Costs

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, organizations reported a mean cost to recover from a ransomware attack of $2.73M, an increase of almost $1M from the $1.82M reported in 2023.

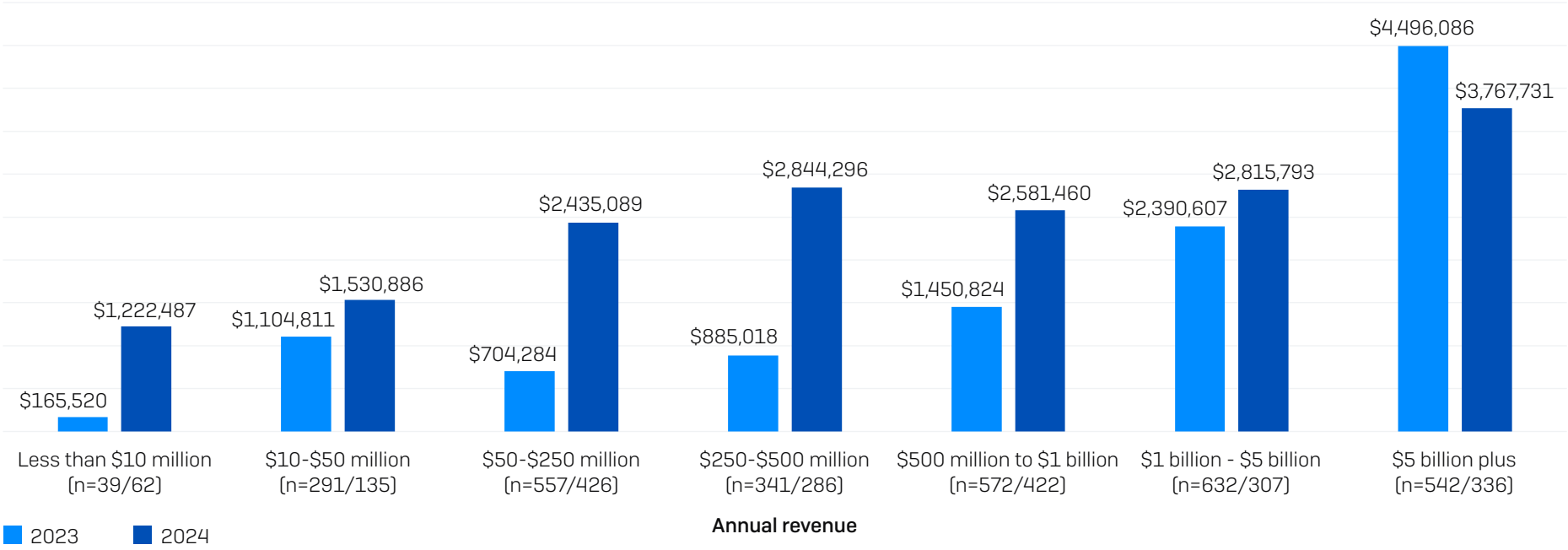
2021	2022	2023	2024
$1.85M	$1.4M	$1.82M	$2.73M

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=2,974 (2024)/ 1,974 (2023)/ 3,702 (2022)/ 2,006 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

The greatest increase in overall recovery costs was experienced by the lower and mid-revenue segments, with the $250M-$500M cohort reporting the biggest individual increase of $2M (from $885,018 to $2,885,296).

Organizations with $1B-$5B revenue reported a (relatively) small increase of just over $400,000, while the largest organizations with $5B+ annual revenue were the only cohort to experience a reduction in recovery cost, down from $4,496,096 to $3,767,731.

Looking at the median recovery cost data confirms the trends. Globally, median recovery costs doubled from $375,000 to $750,000 over the last year. Increases were mostly concentrated in the five lower revenue cohorts who all reported a considerable increase in costs, while remaining relatively flat for the two larger.



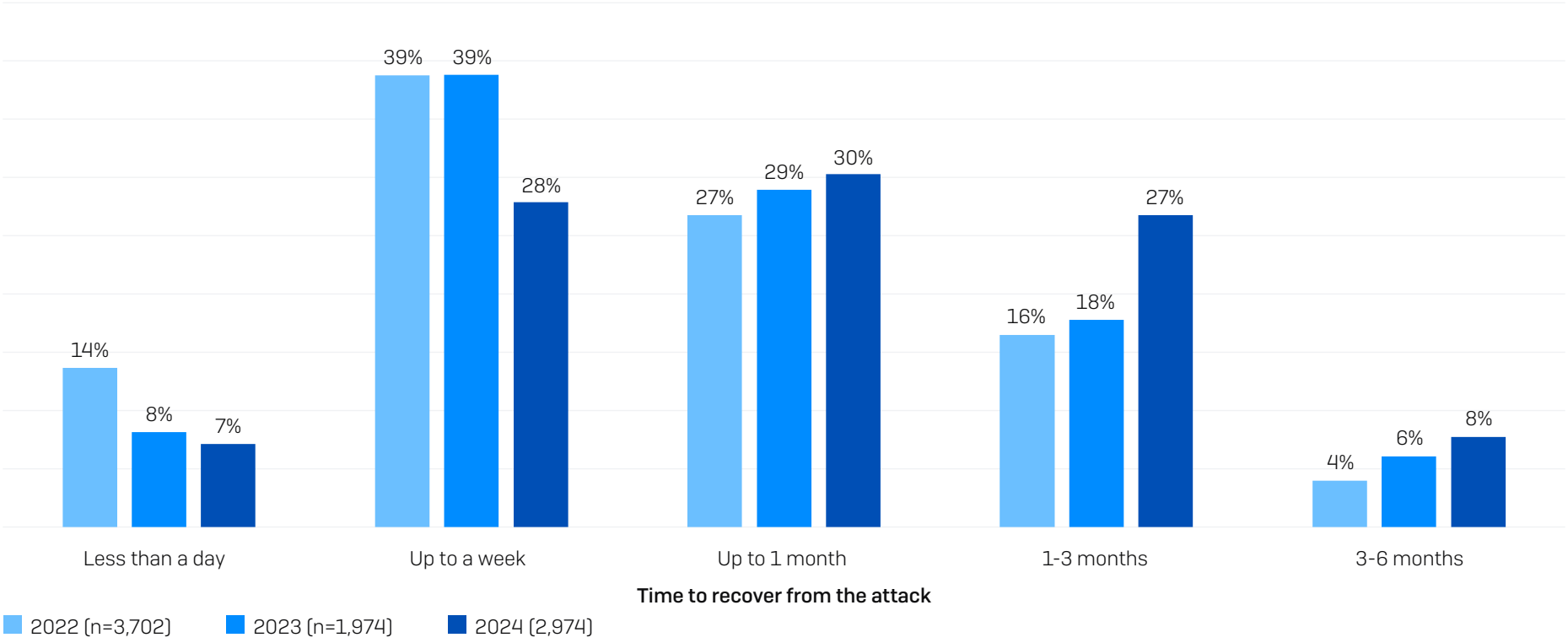
What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=2,974 (2024), 1,974 (2023). 2024/2023 base numbers by revenue in chart

Recovery Time

The time taken to recover from a ransomware attack is getting steadily longer. Our 2024 research revealed:

- 35% of ransomware victims are fully recovered in a week or less, down from 47% in 2023 and 52% in 2022
- One third (34%) now take more than a month to recover, up from 24% in 2023 and 20% in 2022

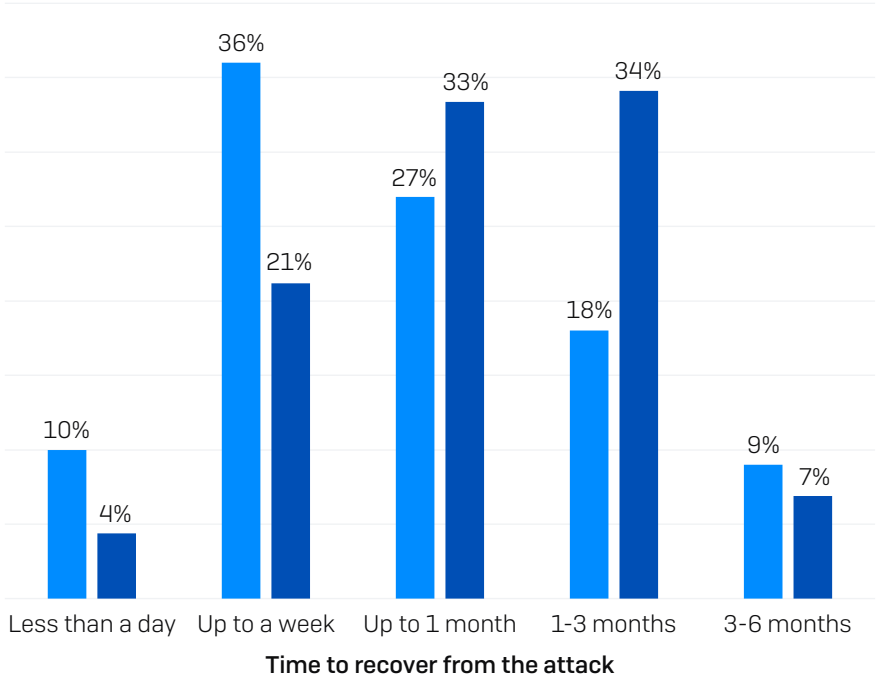
This slowdown may reflect the increased complexity and severity of attacks, necessitating greater recovery work. It may also indicate a growing lack of recovery preparation.



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

Recovery Time: Impact of Backup Compromise

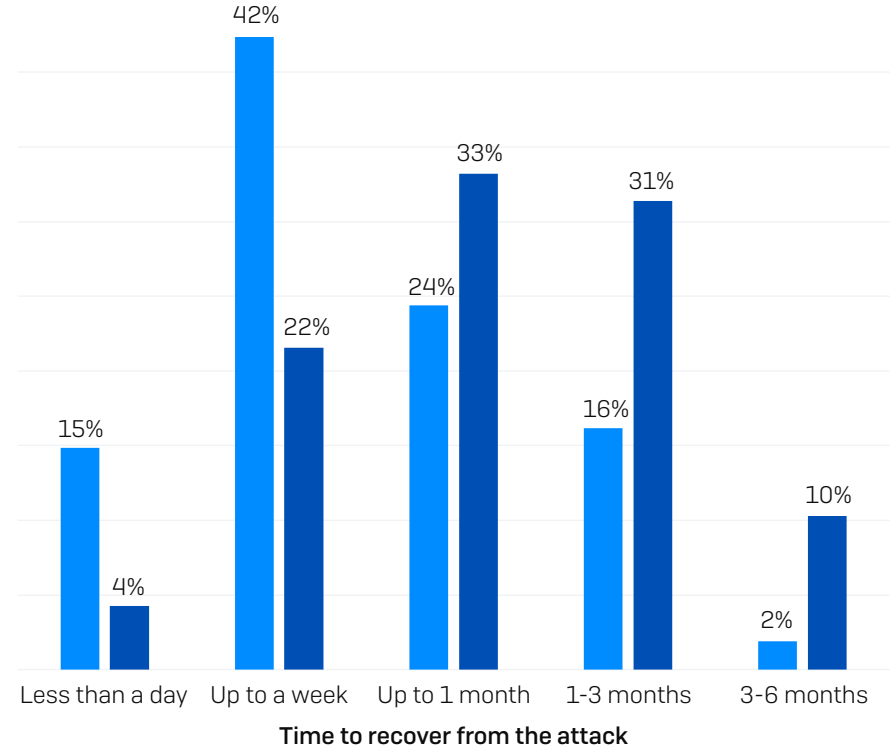
Having your backups compromised has a major impact on overall recovery time. Almost half of organizations whose backups are not compromised recover in a week or less (46%), compared to a quarter (25%) of those whose backups are affected. Having your backups compromised both increases the complexity of recovering encrypted data while adding the overhead of creating and securing new, untainted backups.



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

Recovery Time: Impact of Data Encryption

It is likely no surprise that having data encrypted in an attack significantly increases recovery time. 57% of those who didn't have data encrypted were fully recovered within a week, compared to 25% of those whose data was encrypted.

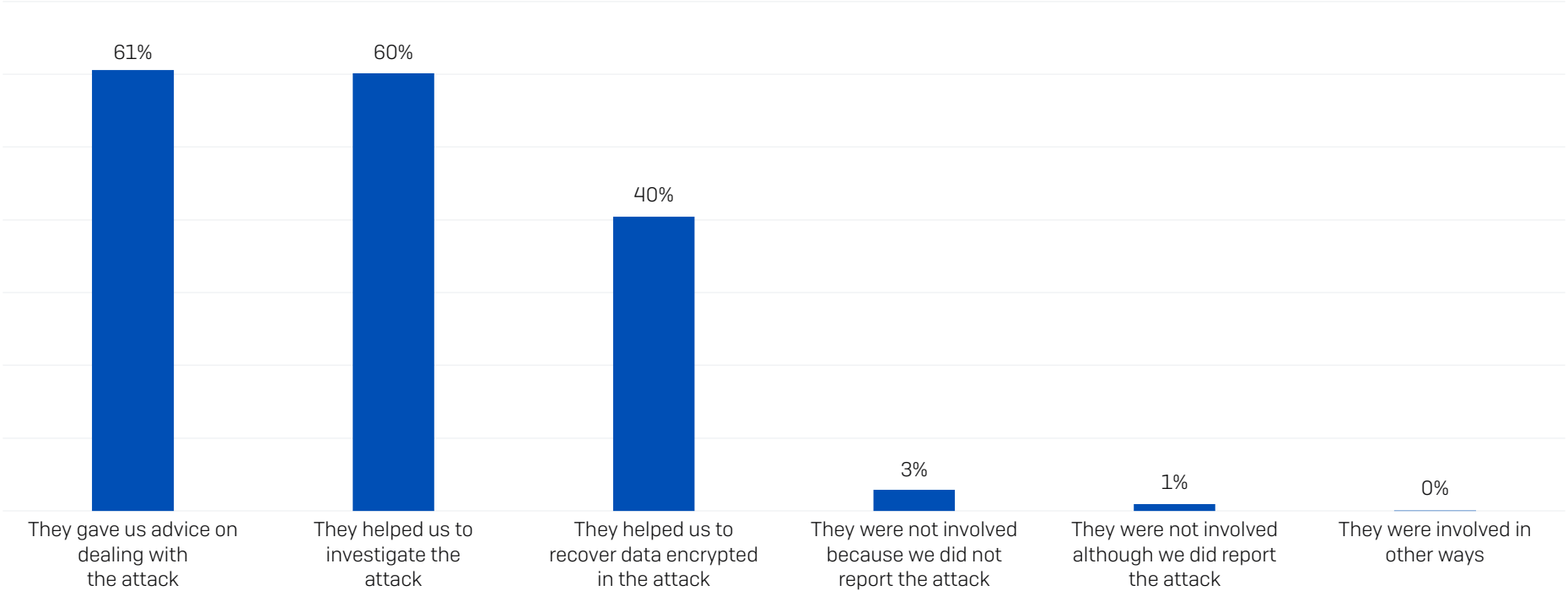


How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

Involvement of Law and Order

The nature and availability of official support when dealing with a ransomware attack vary on a country-by-country basis, as do the tools to report a cyberattack. US victims can leverage the Cybersecurity and Infrastructure Security Agency (CISA); those in the UK can get advice from the National Cyber Security Centre (NCSC); and Australian organizations can call on the Australian Cyber Security Center (ACSC), to name but a few.

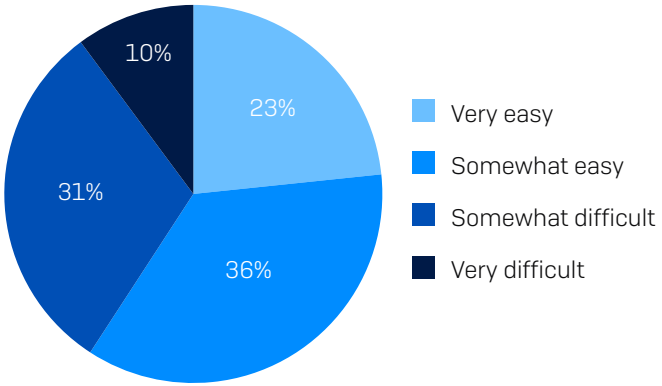
Reflecting the normalization of ransomware, 97% of organizations globally that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 61% reported that they received advice on dealing with the attack, 60% got help investigating the attack, and 40% said they received help recovering from the attack.



If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? n=2,974.

Ease of Engagement

Encouragingly, more than half (59%) of those that engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (23% very easy, 36% somewhat easy). Only 10% said the process was very difficult, while 31% described it as somewhat difficult.



How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=2,874 (excluding 'don't know' responses).

Non-involvement of Official Bodies

There were a range of reasons why 3% (86 respondents) did not report the attack, with the two most common being concern that it would have a negative impact on their organization, such as fines, charges, or extra work (27%), and because they did not think there would be any benefit to them (also 27%). Several respondents provided verbatim feedback that they did not engage official bodies as they were able to resolve the issue in-house.

We were concerned that it would have a negative impact on our organization e.g., fines, charges, extra work	27%
We did not think there would be any benefit to our organization to report the attack	27%
We did not think they would be interested in the attack	22%
We were too busy dealing with the attack to think about involving them	21%
The attackers warned us not to engage them	19%
We did not know which law enforcement or official bodies to involve	10%
We were not legally required to report the attack	9%
Other (please specify)	3%
Don't know	1%

Why didn't you report the attack to law enforcement and/or official bodies? (n=86).

Conclusion

Ransomware remains a major threat to organizations of all sizes around the globe. While the overall attack rate has dropped over the last two years, the impact of an attack on those that fall victim has increased. As adversaries continue to iterate and evolve their attacks, it's essential that defenders and their cyber defenses keep pace.

Prevention. The best ransomware attack is the one that didn't happen because the adversaries couldn't get into your organization. With a third of attacks starting with exploitation of unpatched vulnerabilities, it's important to take control of your attack surface and deploy risk-based prioritization of patching. The use of MFA to limit credential abuse should also be a priority for every single organization. Ongoing user training on how to detect phishing and malicious emails remains essential.

Protection. Strong foundational security is a must, including endpoint, email, and firewall technologies. Endpoints (including servers) are the primary destination for ransomware actors, so ensure that they are well defended, including dedicated anti-ransomware protection to stop and rollback malicious encryption. Security tools need to be correctly configured and deployed to provide optimal protection, so look for solutions that deploy out-of-the-box with straightforward posture controls. Protection that is complicated and hard to deploy can easily increase risk rather than reduce it.

Detection and response. The sooner you stop an attack, the better. Detecting and neutralizing an adversary inside your environment before they can compromise your backups or encrypt your data will considerably improve your outcomes.

Planning and preparation. Having an incident response plan that you are well versed in deploying will greatly improve your outcomes if the worst happens and you experience a major attack. Regularly practice restoring data from backups to ensure speed and fluency should you need to execute in the aftermath of an attack.

To explore how Sophos can help you optimize your ransomware defenses, speak to an adviser or visit www.sophos.com

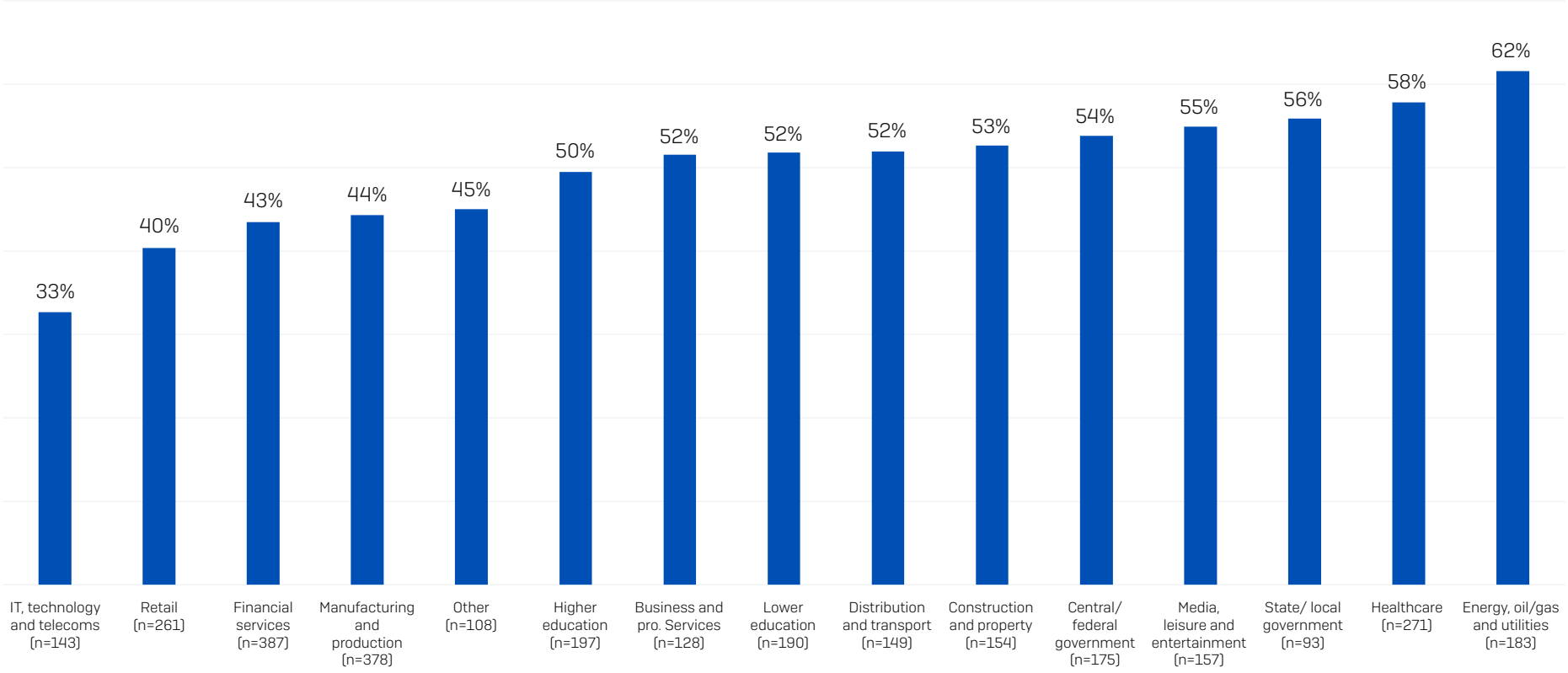
About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com

Appendix

Percentage of Computers Impacted by Industry

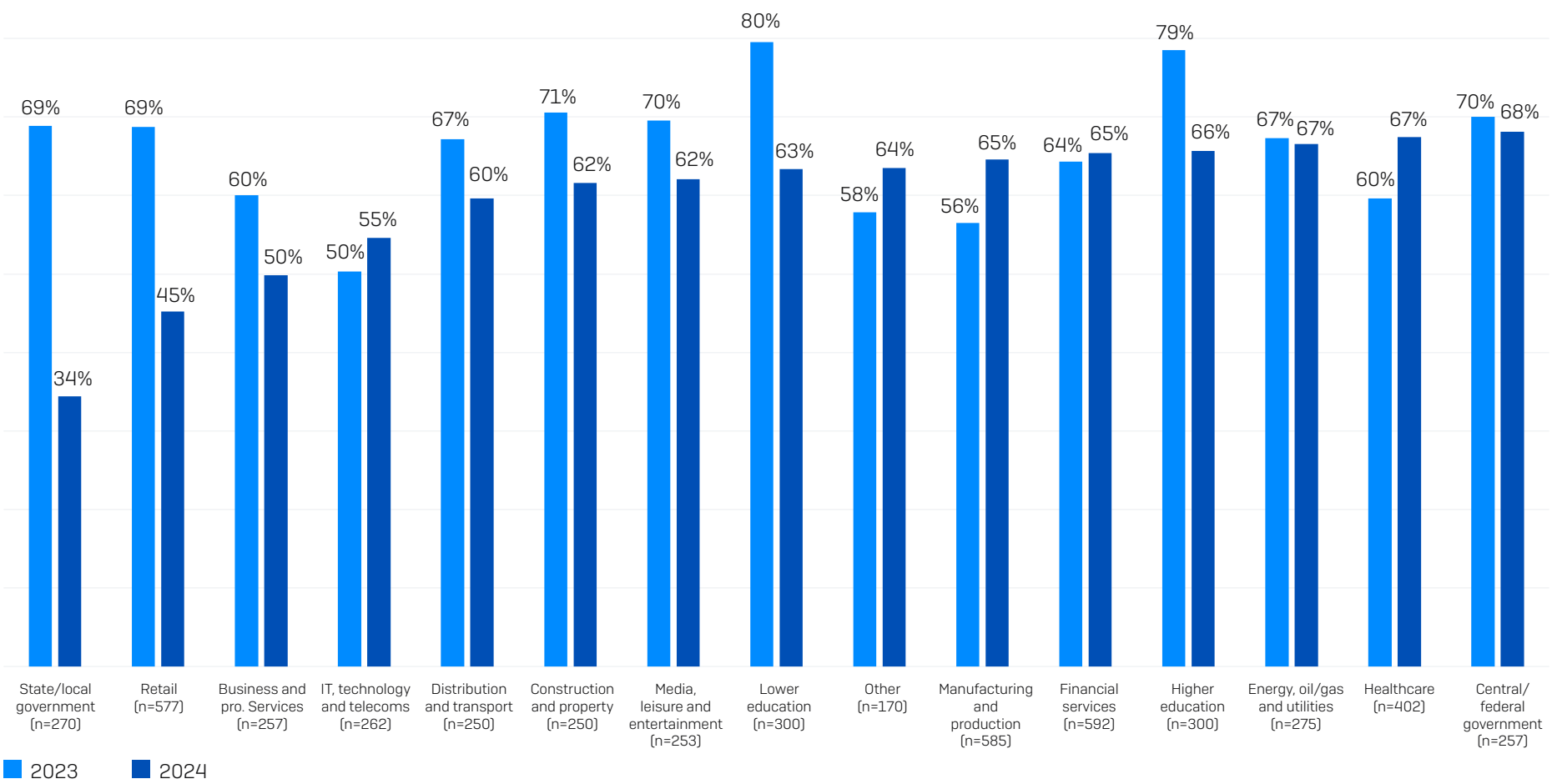
Percentage of devices impacted



What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

Rate of Ransomware Attacks by Industry

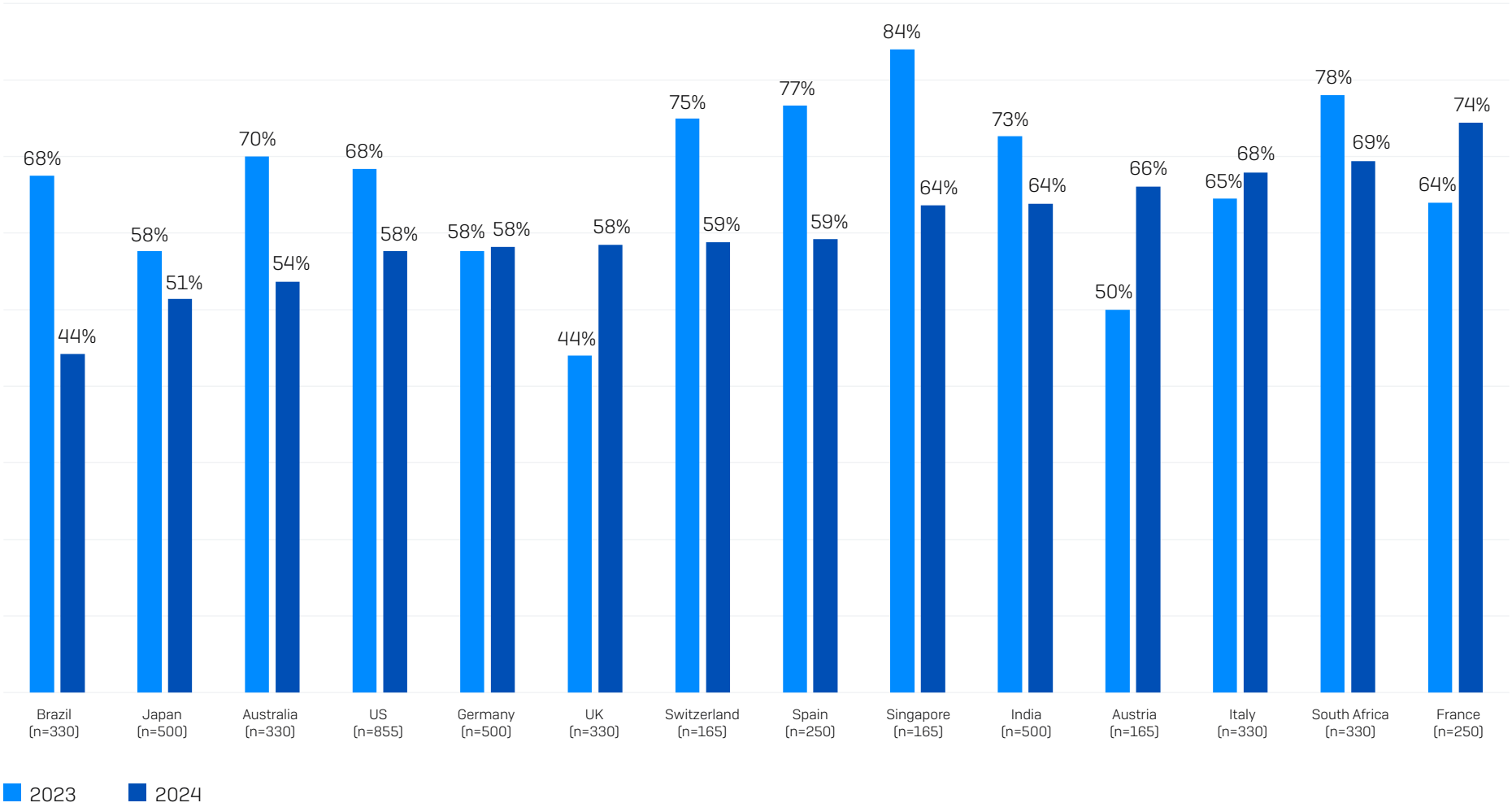
Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2004) n=3,000 (2023), 5,600 (2022). 2024 industry base numbers in chart.

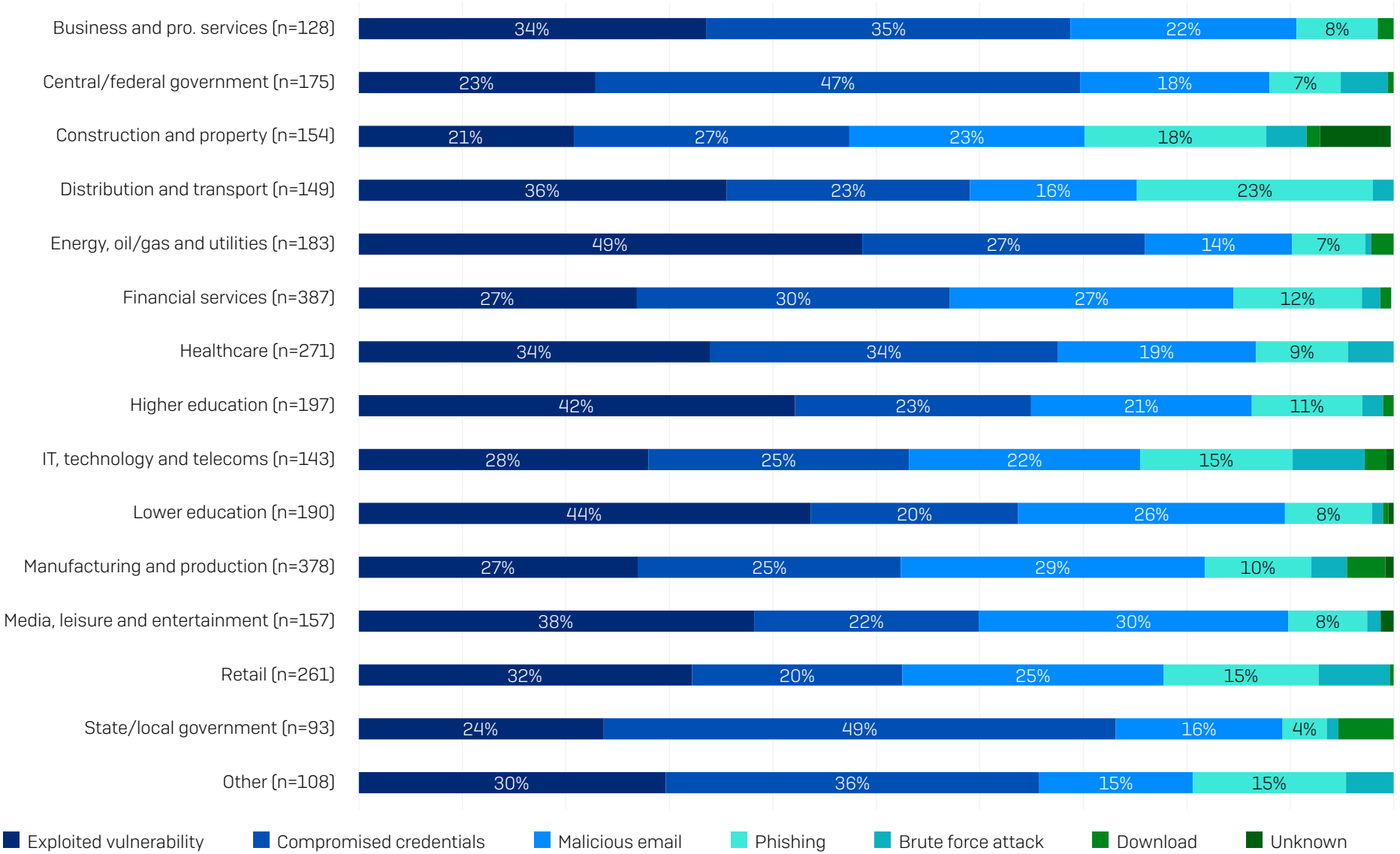
Rate of Ransomwares Attack by Country

Percentage of organizations hit by ransomware in the last year



In the last year, has your organization been hit by ransomware? Yes. n=5,000 (2004) n=3,000 (2023). 2024 country base numbers in chart.

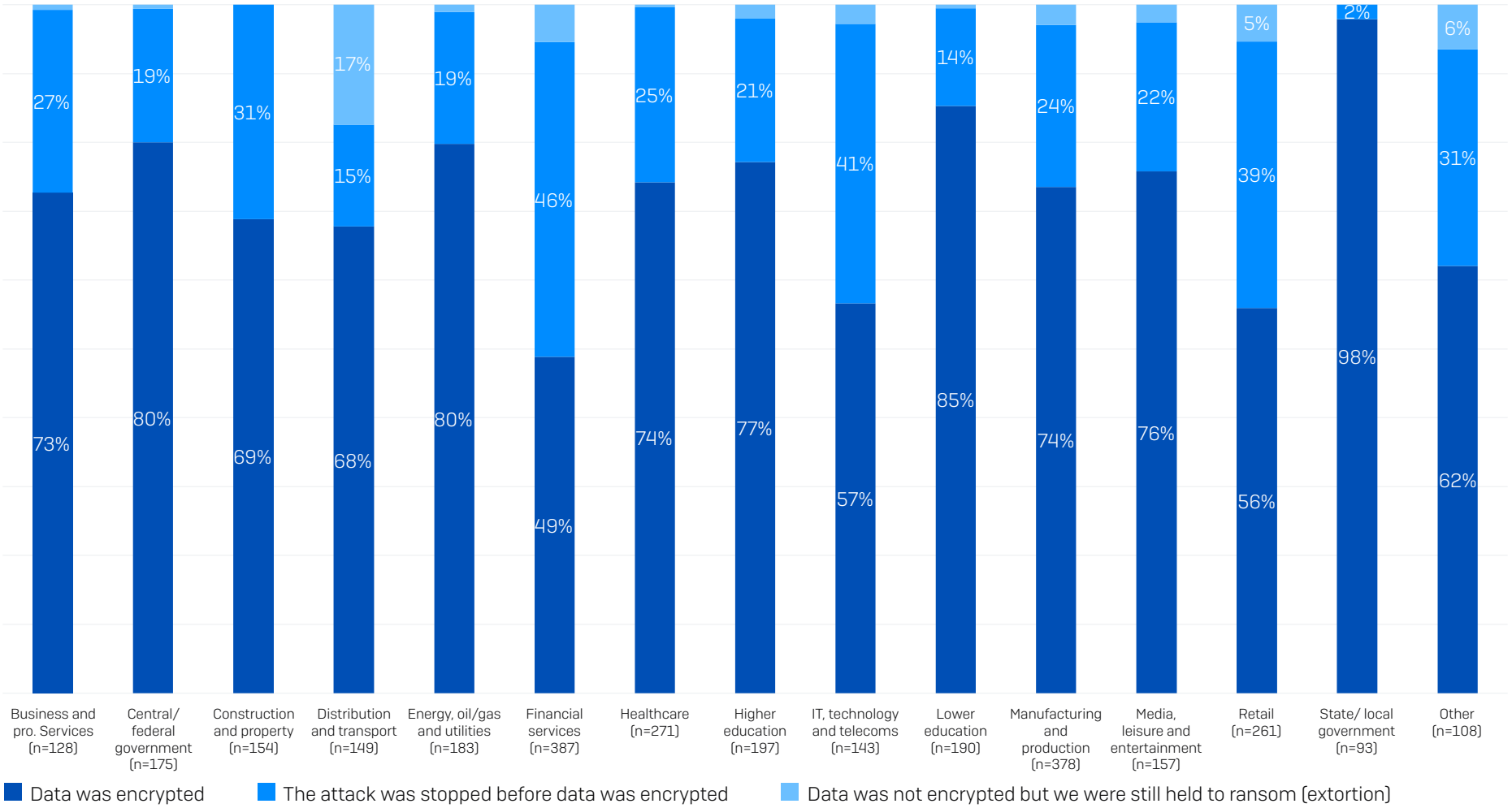
Root Cause of Attack by Industry



Do you know the root cause of the ransomware attack your organization experienced in the last year? n=2,974 organizations hit by ransomware.

Data Encryption Rate by Industry

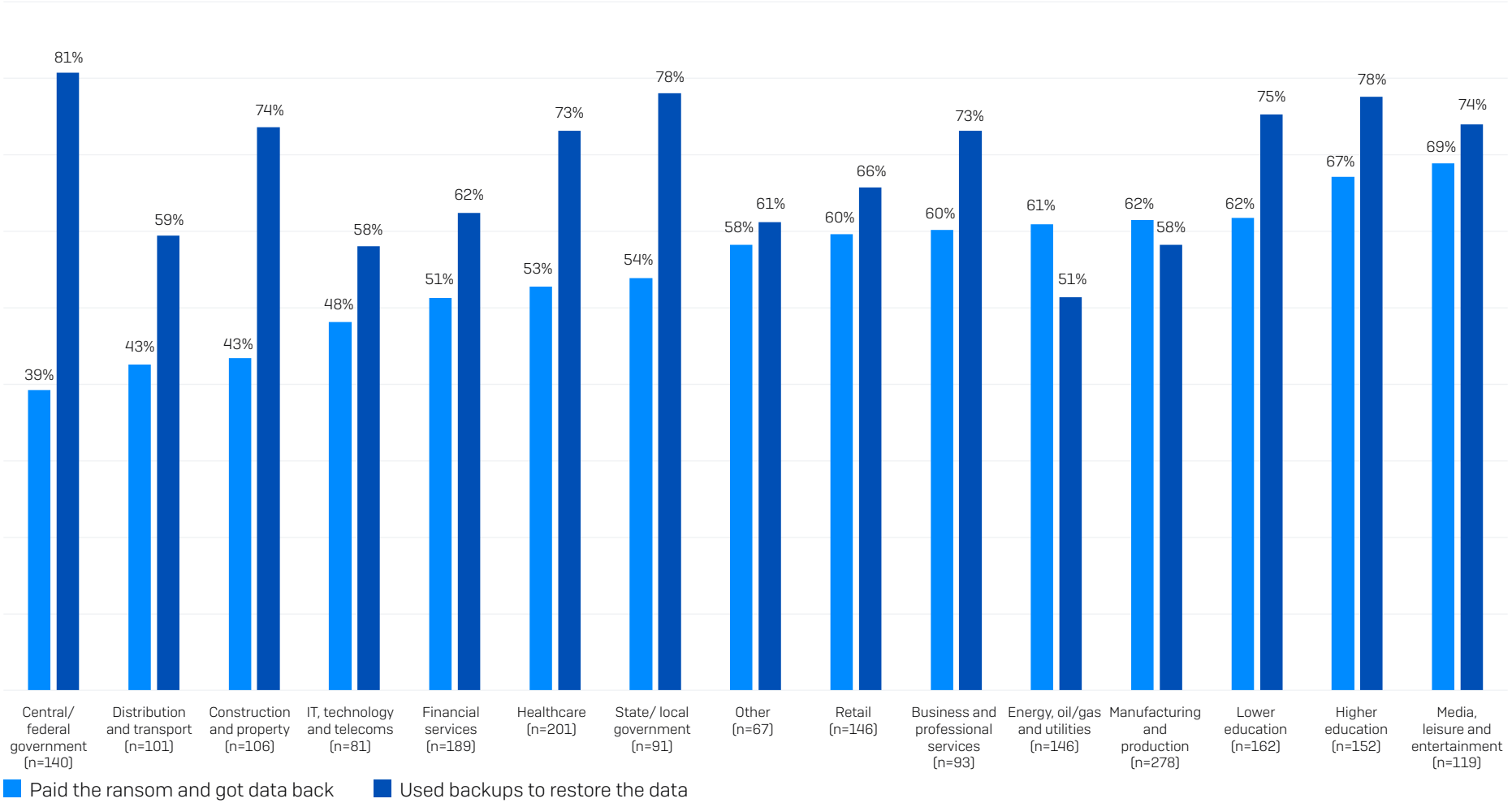
Propensity to have data encrypted in an attack



Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base number in chart.

Data Recovery Method by Industry

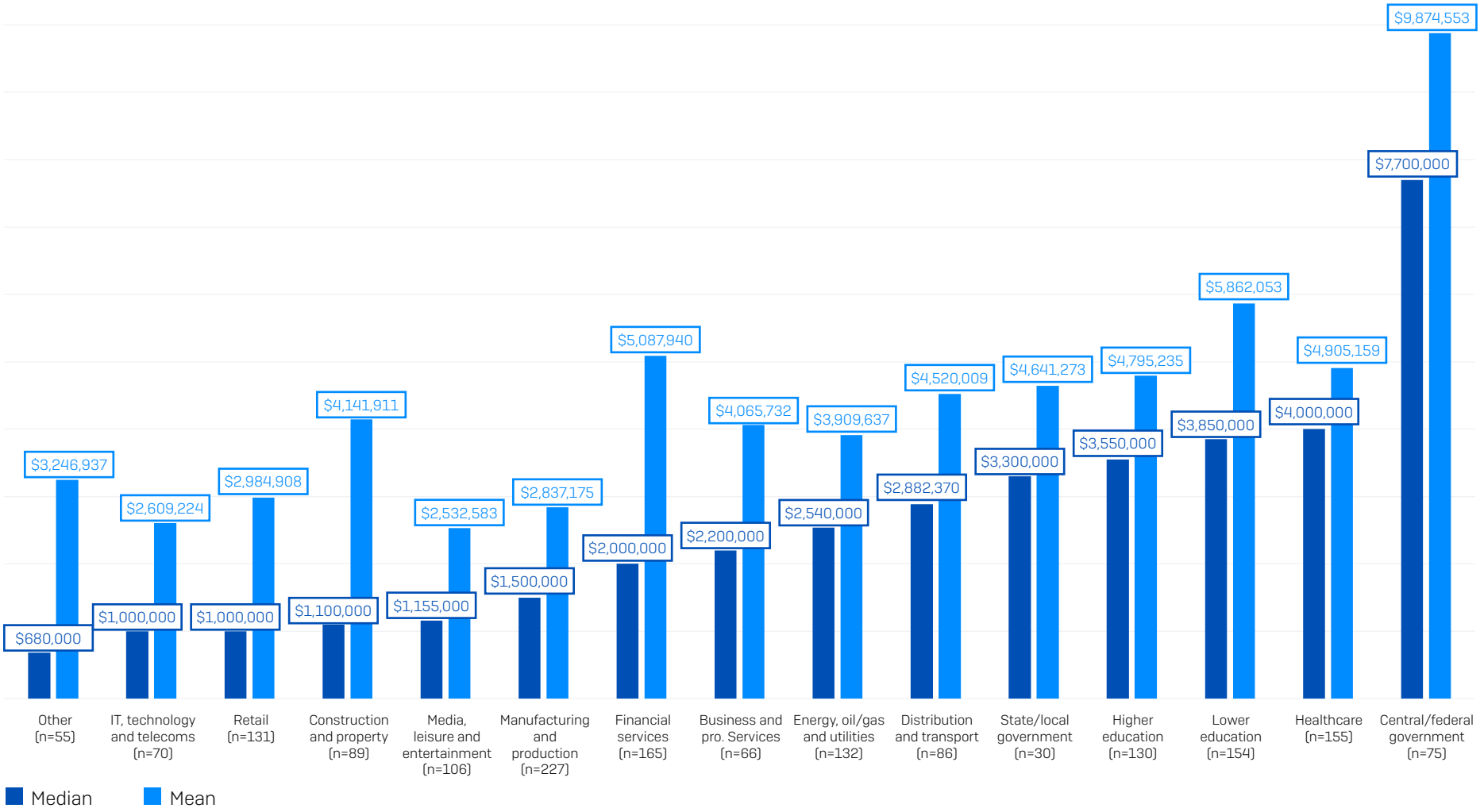
How often data is recovered by using backups and paying the ransom



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. Ordered by propensity to pay the ransom.

Ransom Demand by Industry

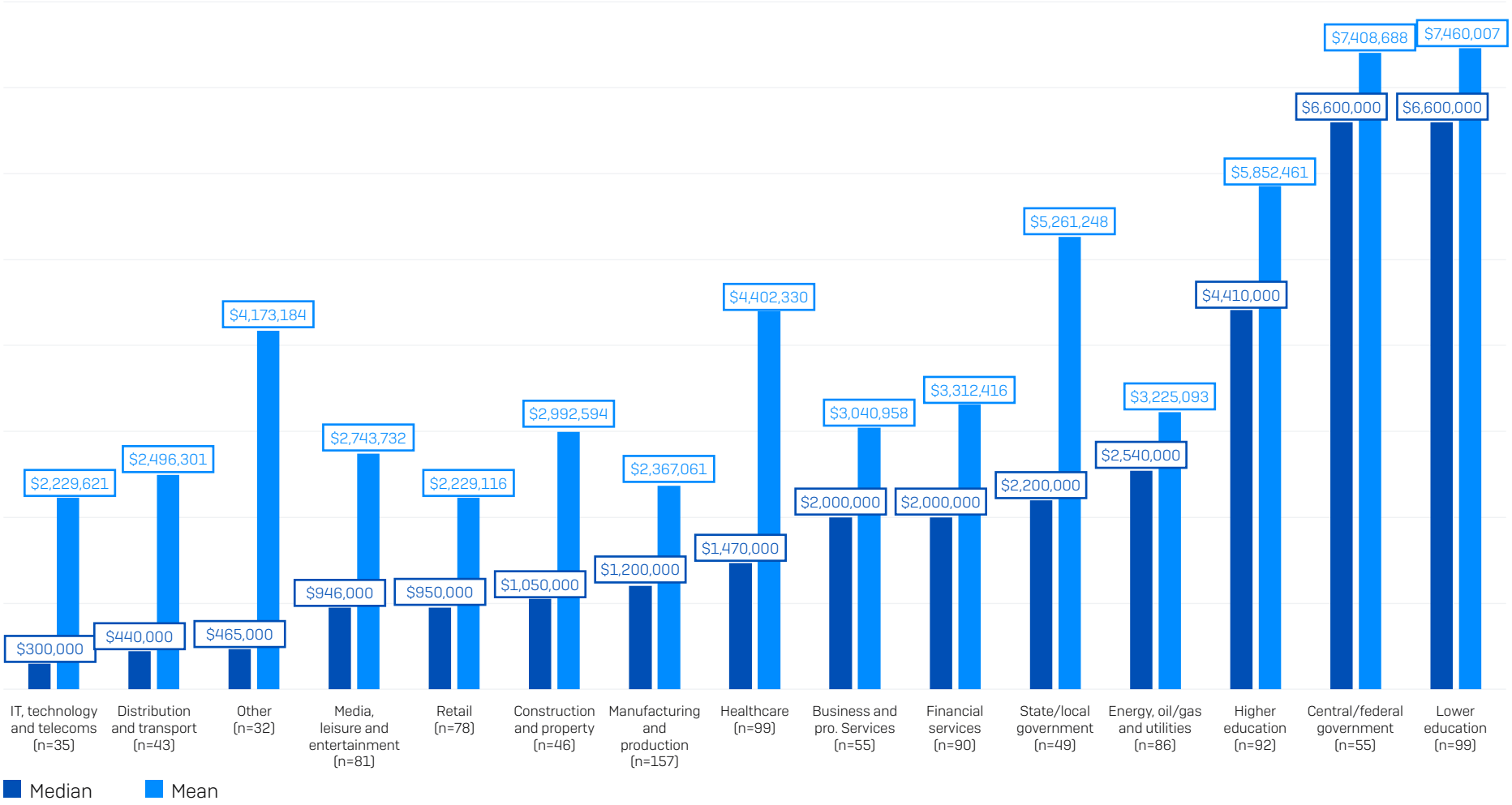
Ransom demand



How much was the ransom demand from the attacker(s)? Base numbers in chart. Ordered by median demand.

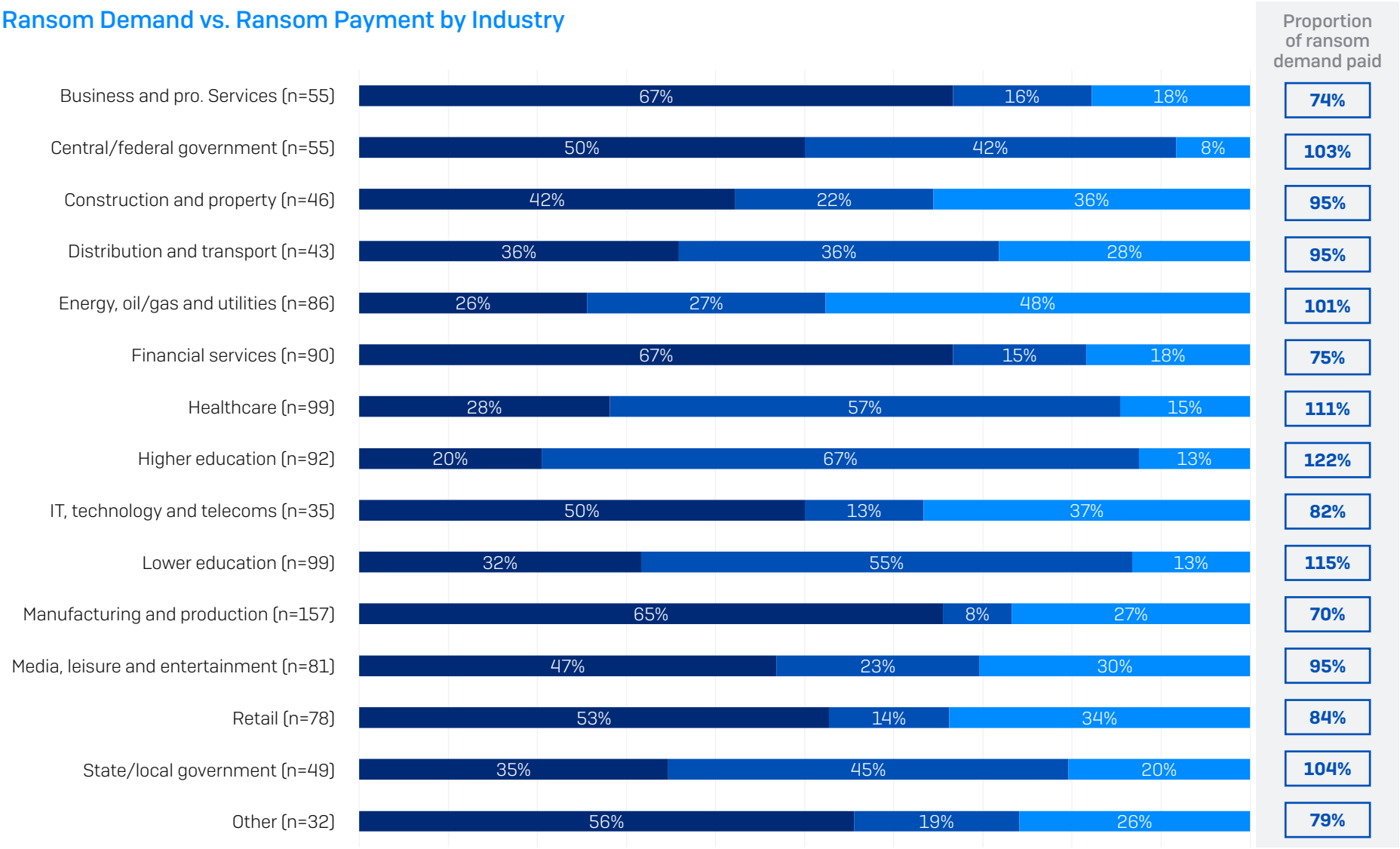
Ransom Payment by Industry

Ransom payment



How much was the ransom payment that was paid to the attackers? Base numbers in chart. Data ordered by median payment.

Ransom Demand vs. Ransom Payment by Industry



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? Base numbers in chart.

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.

© Copyright 2024. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2024-04-22 WP-EN (PC)

SOPHOS