SOPHOS

The State of Ransomware in Retail 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity, including 577 from the retail sector, across 14 countries, conducted in January-February 2024.

A Sophos Whitepaper. June 2024

Introduction

The fifth annual Sophos 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 retail today and how the impact of ransomware has evolved over the last four years.

This year's report also incorporates brand new areas of study, including exploration of ransom demands vs. ransom payments. Plus, for the first time, it shines a light on the role of law enforcement in ransomware remediation for retail organizations.

A note on reporting dates

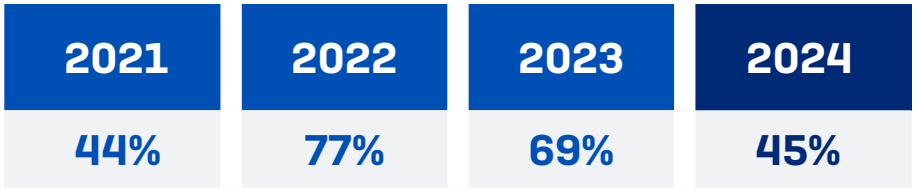
To enable easy comparison of data across our annual surveys, we name the report for the year in which the survey was conducted: in this case, 2024. We are mindful that respondents are sharing their experiences over the previous year, so many of the attacks referenced occurred in 2023.

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, including 577 respondents from retail organizations. 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.

Rate of Ransomware Attacks in Retail

A little less than half of retail organizations (45%) reported being hit by ransomware last year. This is a notable and welcome drop from the 69% and 77% ransomware rates reported in 2023 and 2022, respectively.



In the last year, has your organization been hit by ransomware?
Yes. n=577 (2024), n=355 (2023), 422 (2022), 435 (2021)

The retail experience echoes the wider cross-sector trend of a fall in attack rates. Globally, 59% of organizations reported being hit in our 2024 study, down from 66% in the previous two years. Across sectors, retail reported one of the lowest ransomware rates, second only to *state/local government* (34%).

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

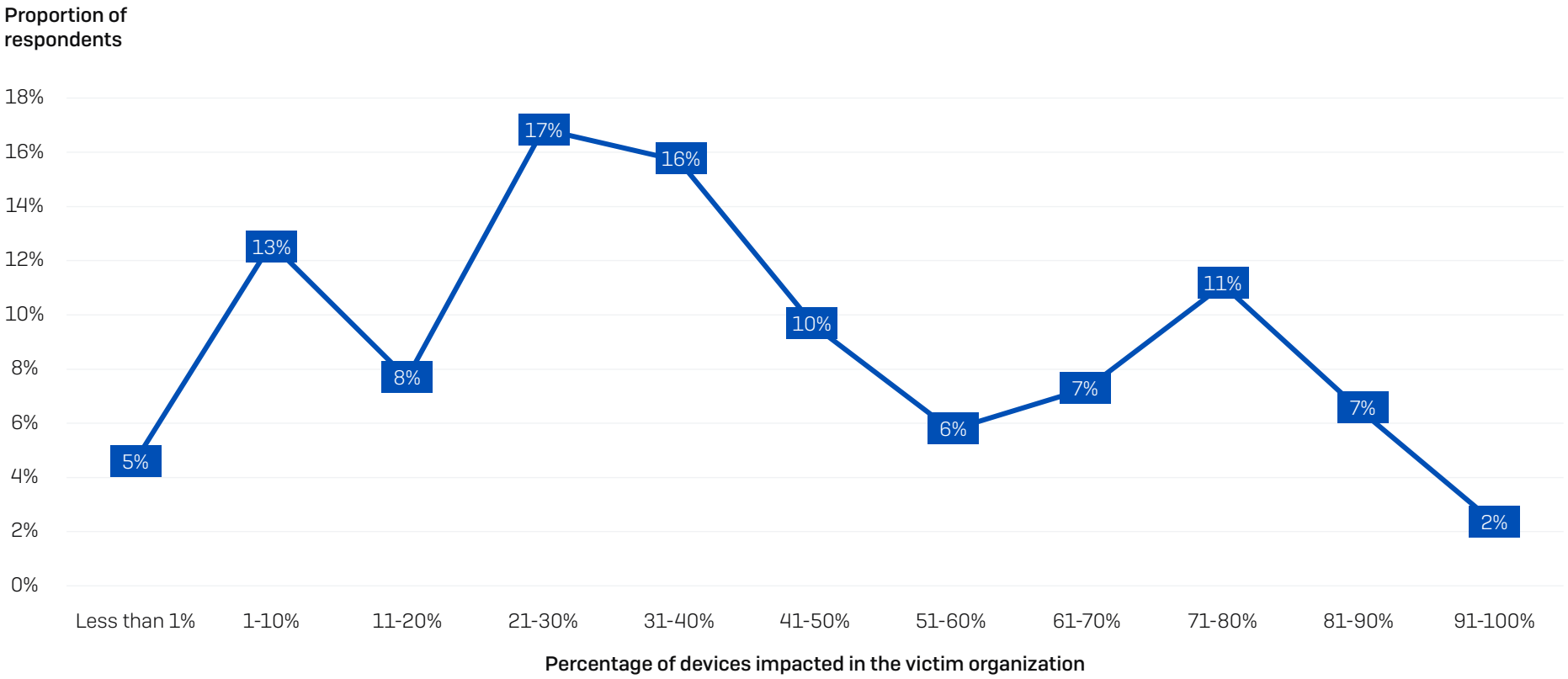
Percentage of Computers Impacted in Retail

On average, in retail, 40% of computers are impacted by a ransomware attack. It is extremely rare to have a full environment encrypted: only 2% of organizations reported 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 5% of retail organizations saying that fewer than 1% of their devices were affected.

Retail had the second lowest percentage of devices impacted by ransomware across all sectors globally, with only *IT, technology and telecoms* (33%) reporting a lower number.

The *Energy, oil/gas and utilities* sector experiences the effects of an attack most broadly, 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 the percentage of computers impacted by industry.



What percentage of your organization's computers were impacted by ransomware in the last year? n=261 retail organizations hit by ransomware

Root Causes of Ransomware Attacks in Retail

All retail organizations hit by ransomware were able to identify the root cause of the attack. Exploited vulnerabilities were the most common root cause of attacks (32%), followed by malicious emails (25%).

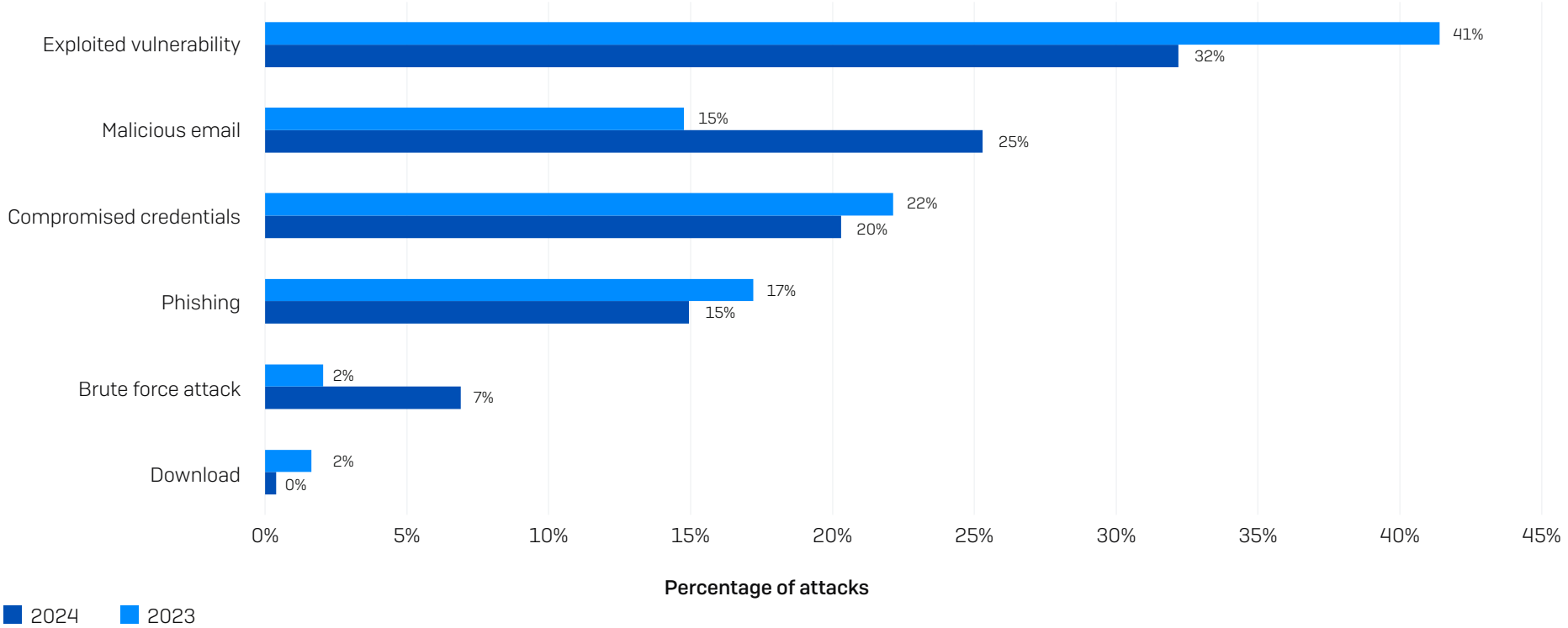
40% of retail respondents reported that email-based approaches (malicious emails or phishing) were the starting point of attacks in 2024.

Exploited vulnerabilities were also the most common root cause of attacks at a cross-sector level (32%), with compromised credentials in the second position (29%).

Globally, retail is the sector least likely to report compromised credentials (20%) as the root cause of attacks, together with *lower education* (20%).

Both retail and *IT, technology, and telecoms* reported that 7% of ransomware incidents began with a brute force attack. Their reduced exposure to unpatched vulnerabilities and compromised credentials may be forcing adversaries to focus, in part, on other approaches.

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



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=261 retail organizations hit by ransomware.

Backup Compromise in Retail

92% of retail organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. Of the attempts, 47% were successful.

Retail's attempted backup compromise rate and compromise success rate are lower than the cross-sector average of 94% and 57% respectively. In fact, across sectors, retail reported the second lowest rate of successful backup compromise with only *IT, technology, and telecoms* having a lower success rate (30%). Compromise attempts on *Energy, oil/gas and utilities* are most likely to be successful (79%).

Retail organizations that had their backups compromised reported considerably worse outcomes than those whose backups were not breached:

- Ransom demands were, on average, considerably more than that of those whose backups weren't impacted ($2.2M vs. $165K median initial ransom demand)
- Organizations whose backups were compromised were twice as likely to pay the ransom to recover encrypted data (75% vs. 35%)
- Median overall recovery costs were considerably more than that of those that did not have backups compromised ($3M vs. $375K)

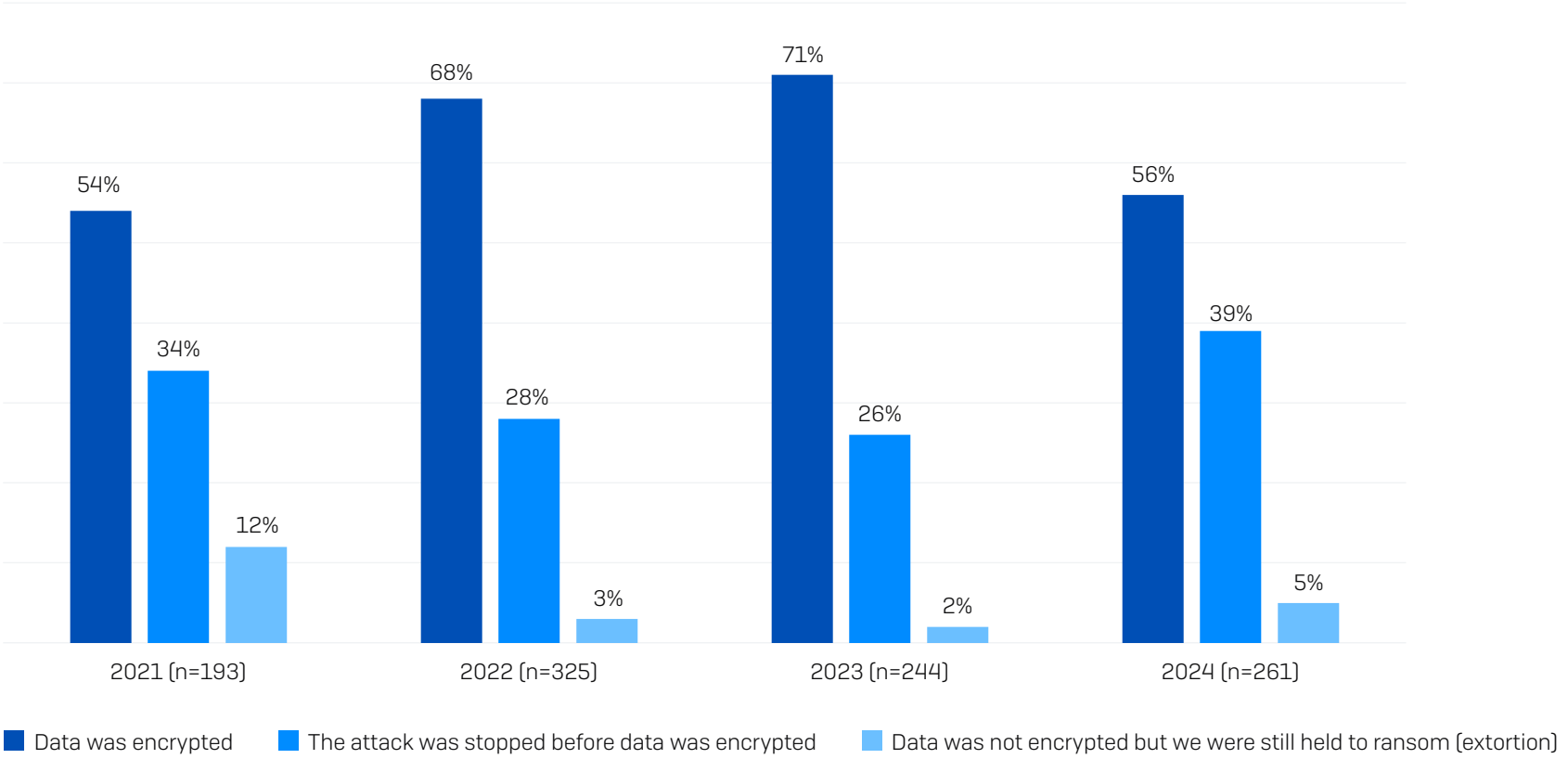
Rate of Data Encryption in Retail

56% of ransomware attacks on retail organizations resulted in data encryption, an encouraging drop from the 71% reported in 2023 and 68% in 2022.

5% of retail organizations experienced an extortion-only attack, where the data was not encrypted but they were held to ransom anyway. This is more than double the rate reported last year (2%) and the second-highest extortion rate across all sectors globally, jointly with *financial services*.

The data encryption rate in retail was notably lower than the global cross-sector average of 70%, and the lowest across all sectors other than *financial services* (49%). Retail also had one of the highest rates of stopping the attack before data could be encrypted (39%), with only *financial services* (46%), and *IT, technology and telecoms* (41%) better able to stop the encryption.

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 the chart.

Data Theft

Adversaries don't just encrypt data; they also steal it. In 32% of incidents in retail organizations where data was encrypted, data was also stolen – a considerable increase (52%) from the 21% reported last year. 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.

32%
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=261)

Data Recovery

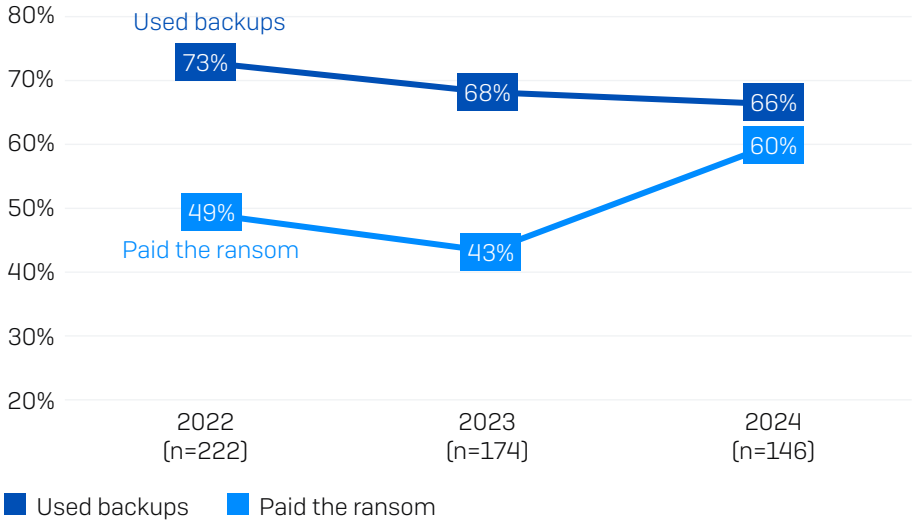
Almost all retail organizations (99%) that had data encrypted got their data back. 66% of retail organizations restored encrypted data using backups, 60% paid the ransom to get data back, and 20% used other means – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.

In comparison, globally, 68% used backups while 56% paid the ransom.

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
66%	60%	20%

Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data (n=146)

The three-year retail view reveals that the gap between the use of backups and ransom payment has shrunk considerably over the last 12 months. Backup use has fallen, albeit slightly, for the second consecutive year. However, a cause for concern is the sector's propensity to pay the ransom, which has increased considerably over the last year.



Did your organization get any data back? Yes, we paid the ransom and got the data back; Yes, we used backups to restore the data. Base numbers in chart.

A notable change over the last year is the increase in the propensity for victims to use multiple approaches to recover encrypted data (e.g., paying the ransom and using backups). In this year's study, over one-third of retail organizations (39%) that had data encrypted reported using more than one method, more than double the rate reported in 2023 (16%).

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

Ransom Demands

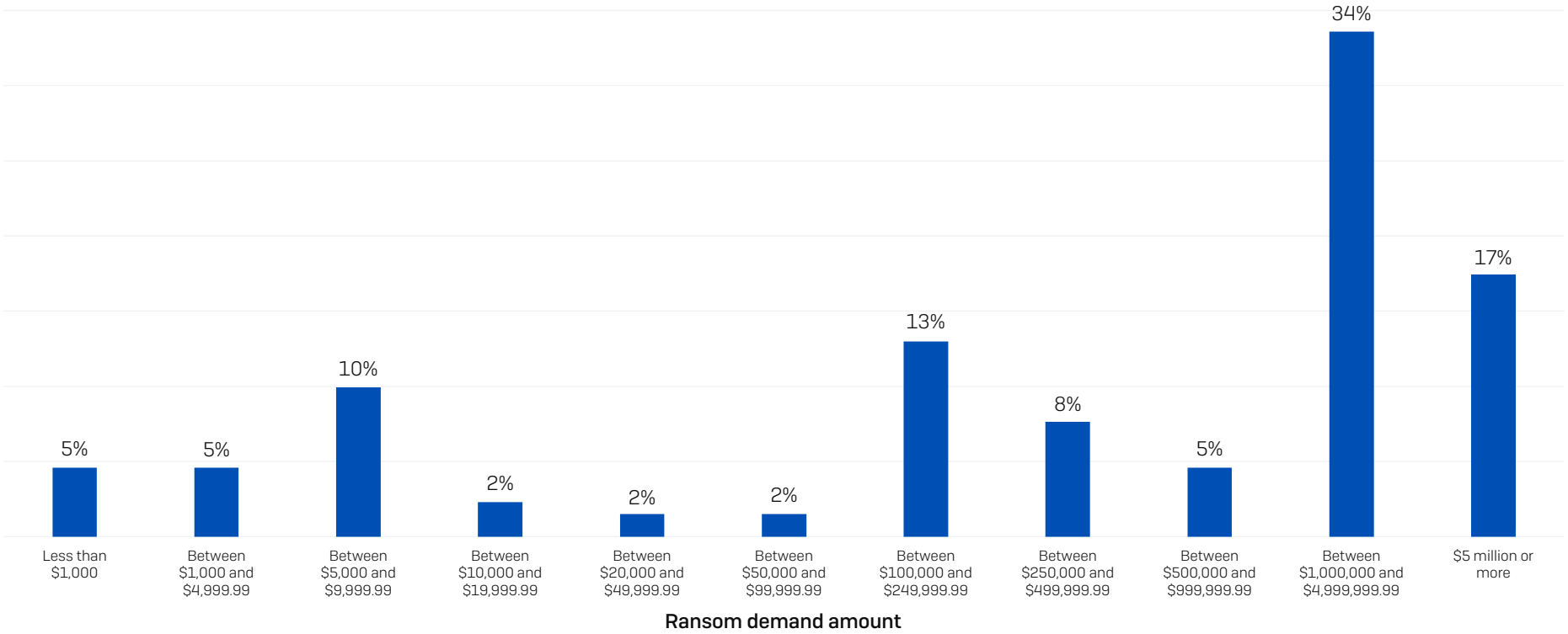
This year, for the first time, we included both ransom demands and payments in this report. Across the 131 retail organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was $1,000,000 (median) and $2.98M (mean).

One of the most notable findings in this year's study is that more than half (51%) of ransom demands in retail organizations are for $1M or more, with 17% of demands for $5M or more. Only 5% of respondents reported less than four-figure ransom demands, indicating that adversaries commonly seek huge ransom payments.

All named sectors (excluding "*other*") reported median ransom demands of $1M or higher. Retail, and *IT, technology and telecoms* received the lowest median demands of $1M. *Central/federal government* reported the highest median ($7.7M) and mean ($9.8M) demands.

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

Percentage of demands for the ransom amount



How much was the ransom demand from the attacker(s)? n=131

Ransom Payments

78 retail respondents whose organizations paid the ransom shared the actual sum paid. Looking at both median and mean averages, we see that ransom payments have decreased in the last year:

- Median payment: $950,000
  (a 68% decrease on the $3,000,000 reported in 2023)
- Mean payment: $2,229,116
  (a 9% decrease on the $2,458,481 reported in 2023)

Ransom payments vary considerably by industry. *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.

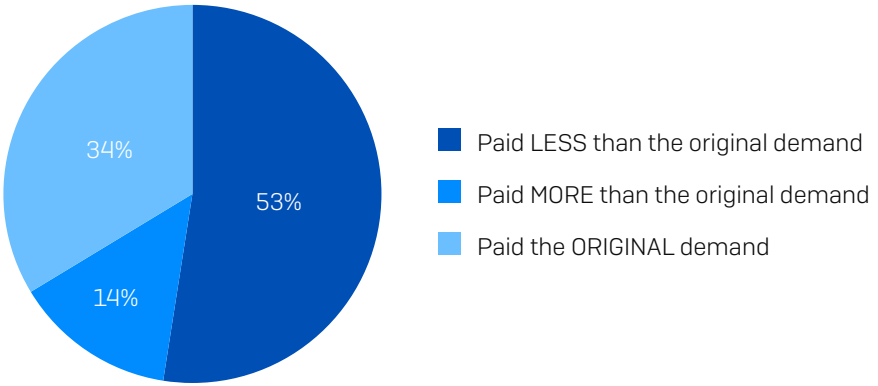
See the appendix for a detailed breakdown of average ransom payment by industry.

Propensity to Negotiate Ransom Amounts in Retail

The study has revealed that retail victims rarely pay the initial sum demanded by the attackers. Only one-third (34%) of respondents said that their payment matched the original request. 53% paid less than the original demand, while only 14% paid more.

The result is that, on average, retail organizations paid 84% of the initial ransom demanded by adversaries.

Propensity to negotiate ransom amount



How much was the ransom demand from the attacker(s)? How much was the ransom payment that was paid to the attackers? n=74.

Retail has one of the lowest propensities to pay more than the original demand, together with *manufacturing* (8%) and *IT, technology, and telecom* (13%). 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)

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

Source of Ransom Funding in Retail

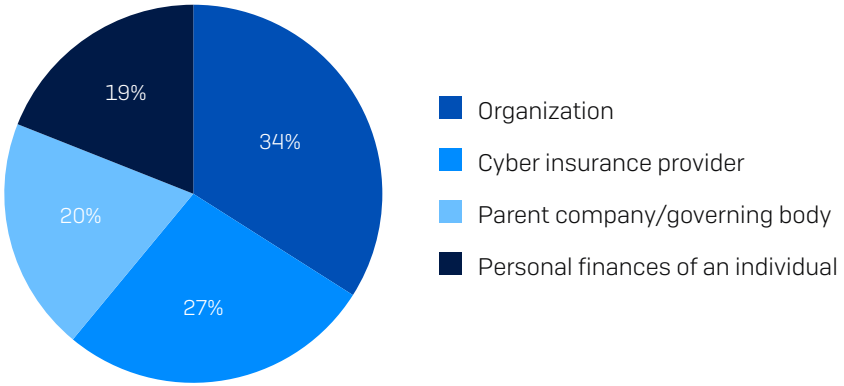
Who provides the money for the ransom is an area of considerable interest, and the study has revealed a number of insights in this area:

Funding the ransom is a collaborative effort, with retail respondents reporting multiple sources of payment in 89% of cases

The primary source of ransom funding in retail organizations is the organization itself, covering over one-third (34%) of the payment on average; the organization's parent company and/or governing body typically provides 20%

Insurance providers are heavily involved in ransom payments, contributing in 89% of cases. 27% of total ransom payment funding comes from insurance providers.

Source of ransom payment funding



From which of the following source(s) was the money to fund the ransom payment obtained? n=87

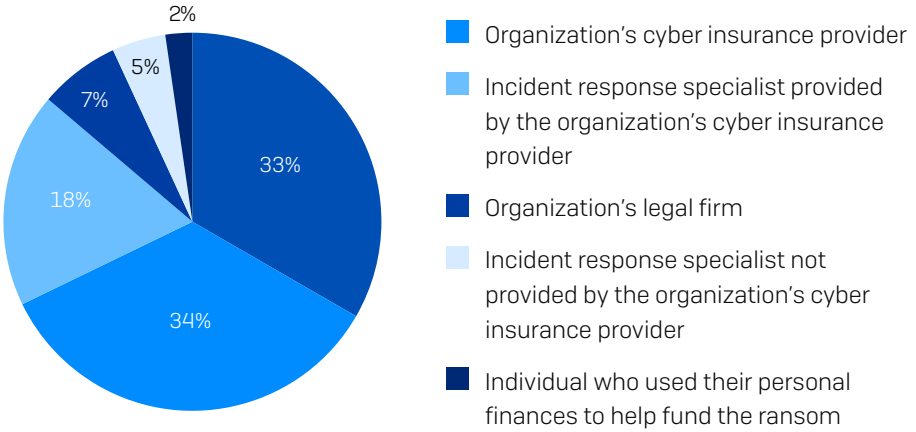
Ransom Transaction Execution

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

In the retail sector, insurance providers transferred the funds for over half of ransom payments, either directly (34%) or through their appointed incident response specialist (18%). The victim organization made one-third (33%) of payments, while 7% were executed by the victim's legal firm.

23% of transfers were made by incident response specialists, whether appointed by the insurance provider (18%) or another party, typically the victim (5%).

Executor of ransom payment transfer



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=87.

Recovery Costs in Retail

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, retail organizations reported a mean cost of $2.73M to recover from a ransomware attack, an increase from the $1.85M reported in 2023. The retail recovery costs very closely match the global cross-sector numbers ($2.73M in 2024; $1.82M in 2023).

2021	2022	2023	2024
$1.97M	$1.27M	$1.85M	$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=261 (2024)/244 (2023)/325 (2022)/193 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

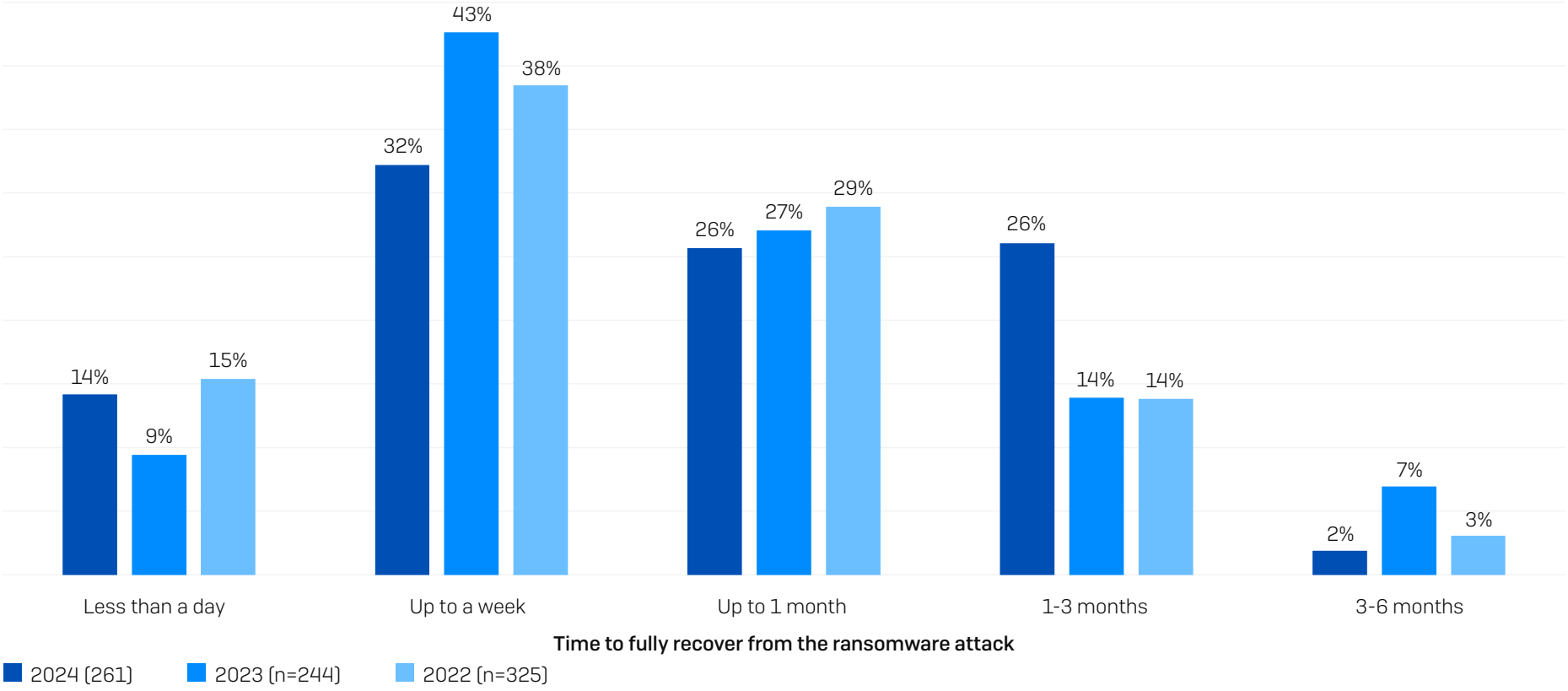
The median recovery cost for retail organizations has remained flat at $750,000. However, across all sectors surveyed, the median recovery costs doubled from $375,000 to $750,000 over the last year.

Recovery Time in Retail

The time taken to recover from a ransomware attack is steadily increasing in retail organizations. Our 2024 research revealed:

- 46% of ransomware victims in retail are fully recovered in a week or less, down from 52% in 2023 and 53% in 2022
- 28% in retail now take more than a month to recover, up from 21% in 2023 and 17% 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.

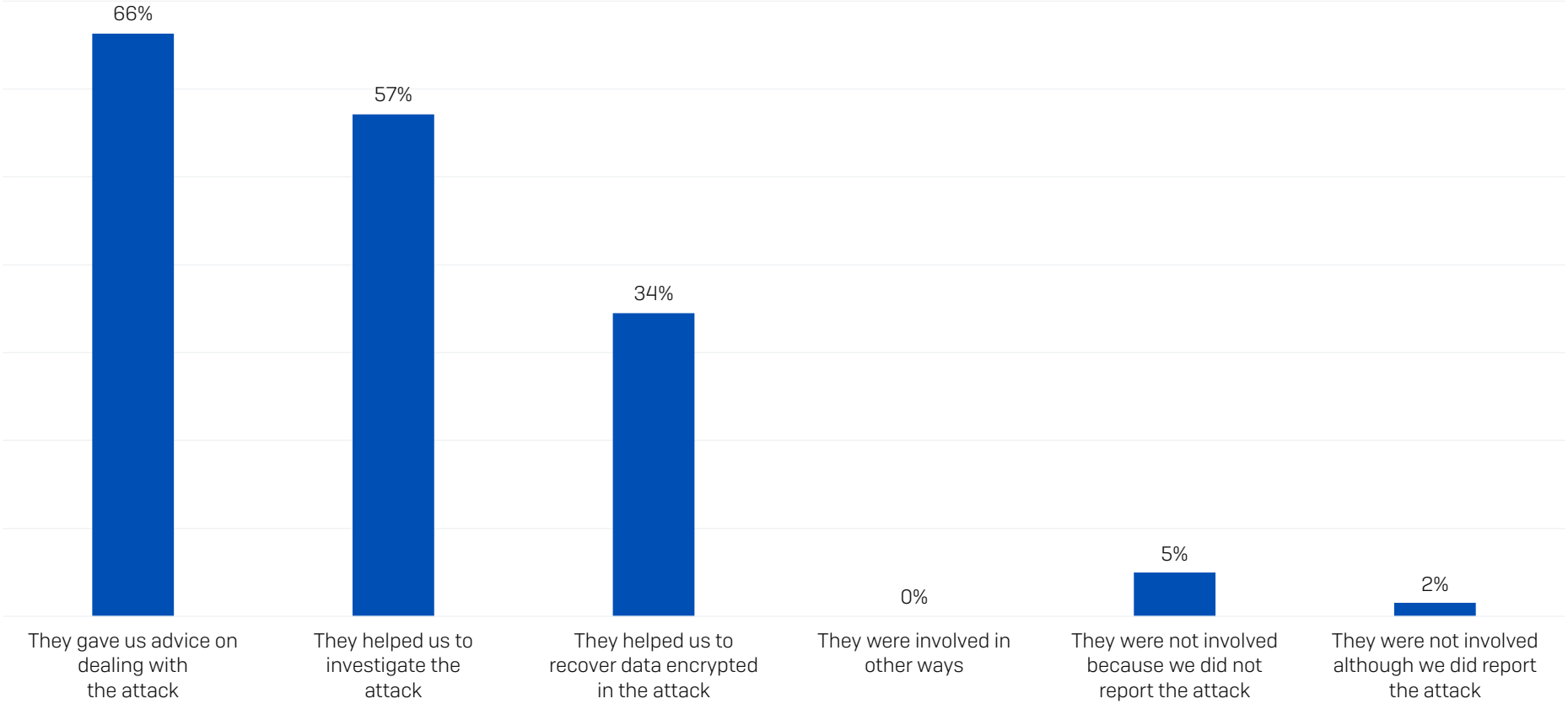


How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

Involvement of Law and Order in Retail

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.

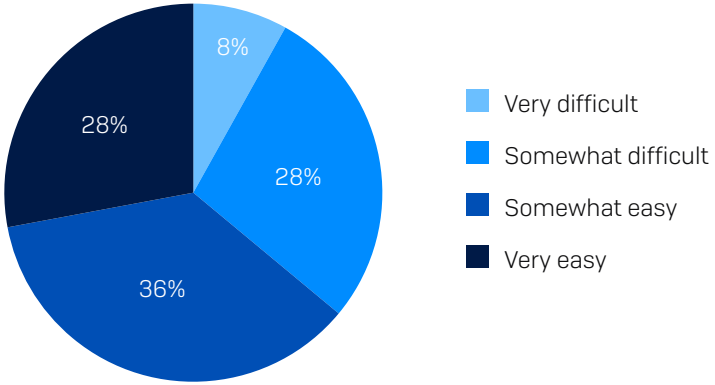
Reflecting the normalization of ransomware, 93% of retail organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 66% reported that they received advice on dealing with the attack, 57% got help investigating the attack, and 34% said 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=261

Ease of Engagement in Retail

Almost two-thirds (64%) of those who engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (28% very easy, 36% somewhat easy). 8% said the process was very difficult, while 28% 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=247 (excluding "don't know" responses).

Conclusion

Ransomware remains a major threat to retail organizations of all sizes around the globe. While the attack rate in retail 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 the exploitation of unpatched vulnerabilities in retail, 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 roll back 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

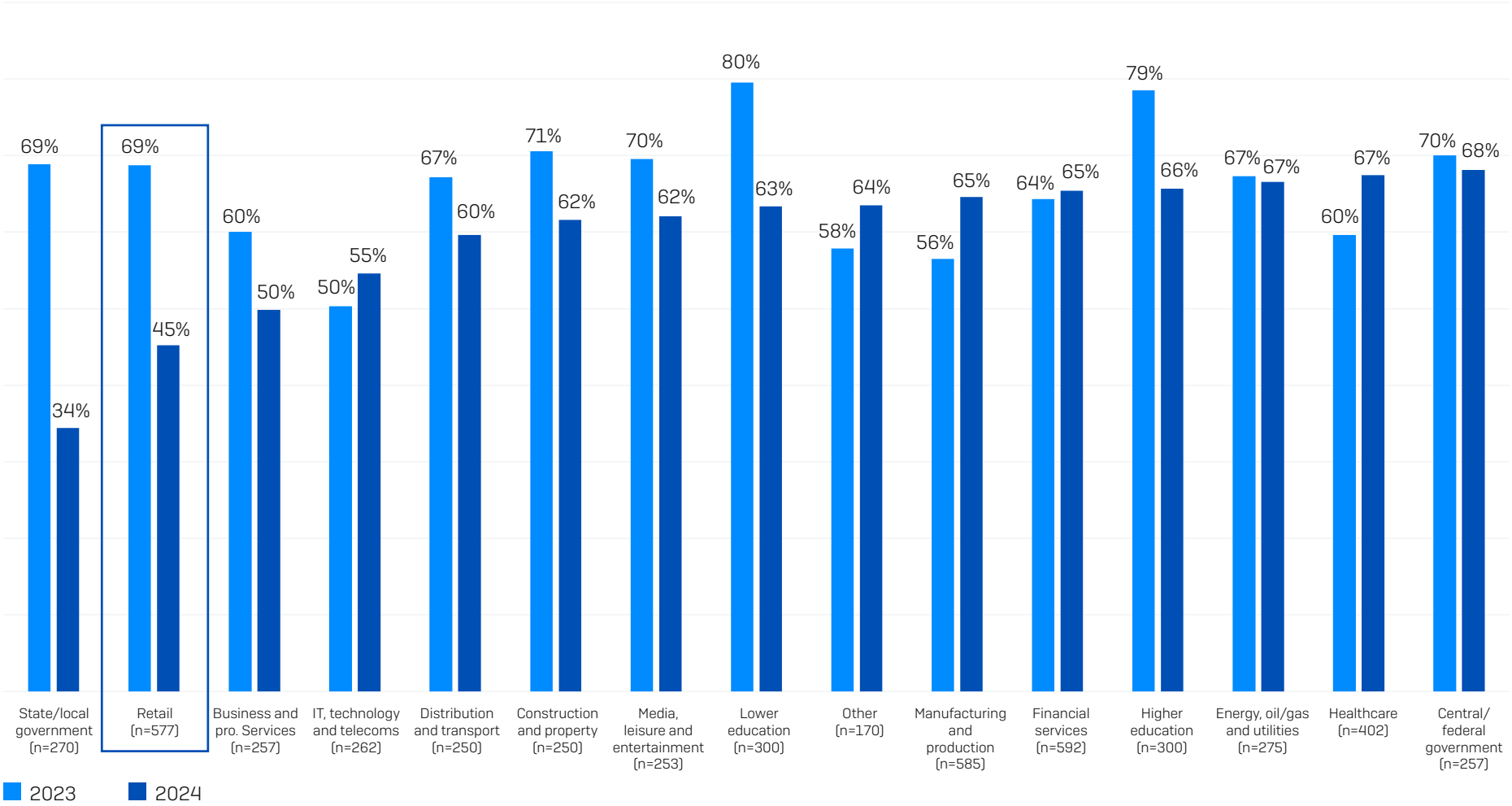
About Vanson Bourne

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

Rate of Ransomware Attacks by Industry

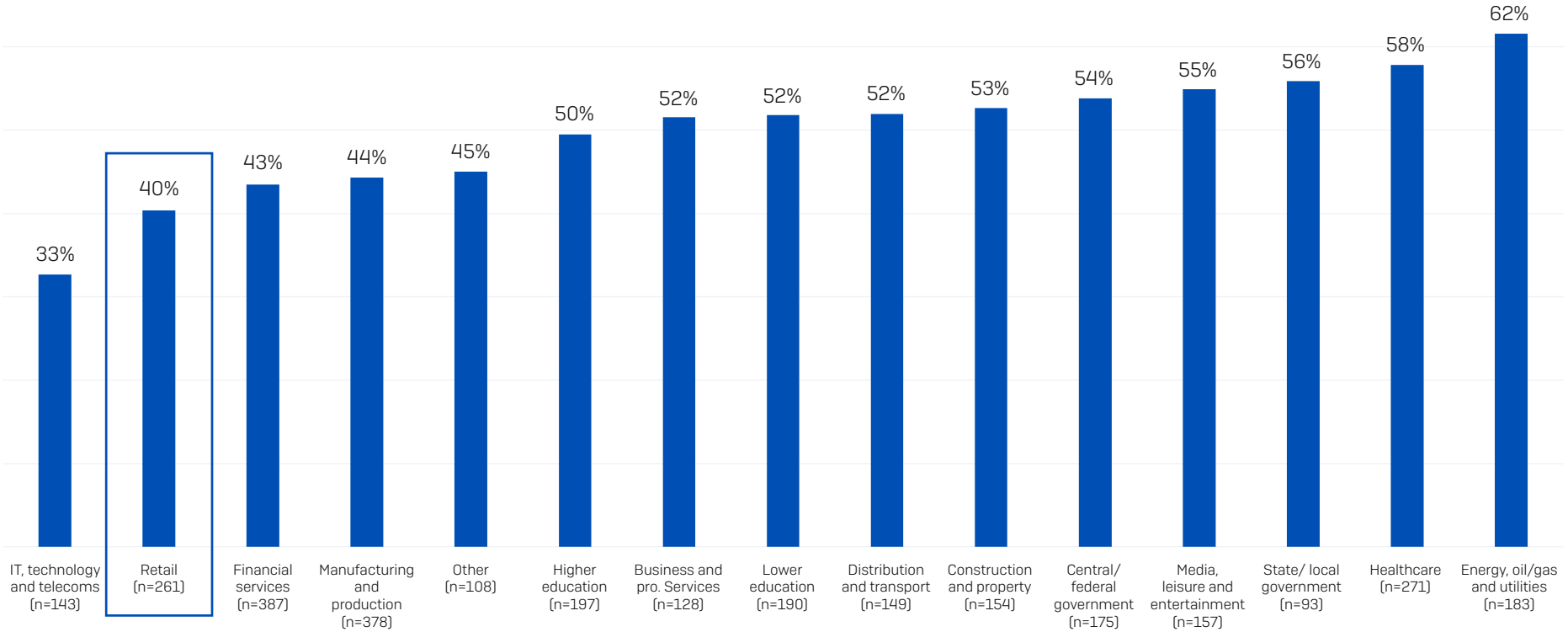
Percentage of organizations hit by ransomware in the last year



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

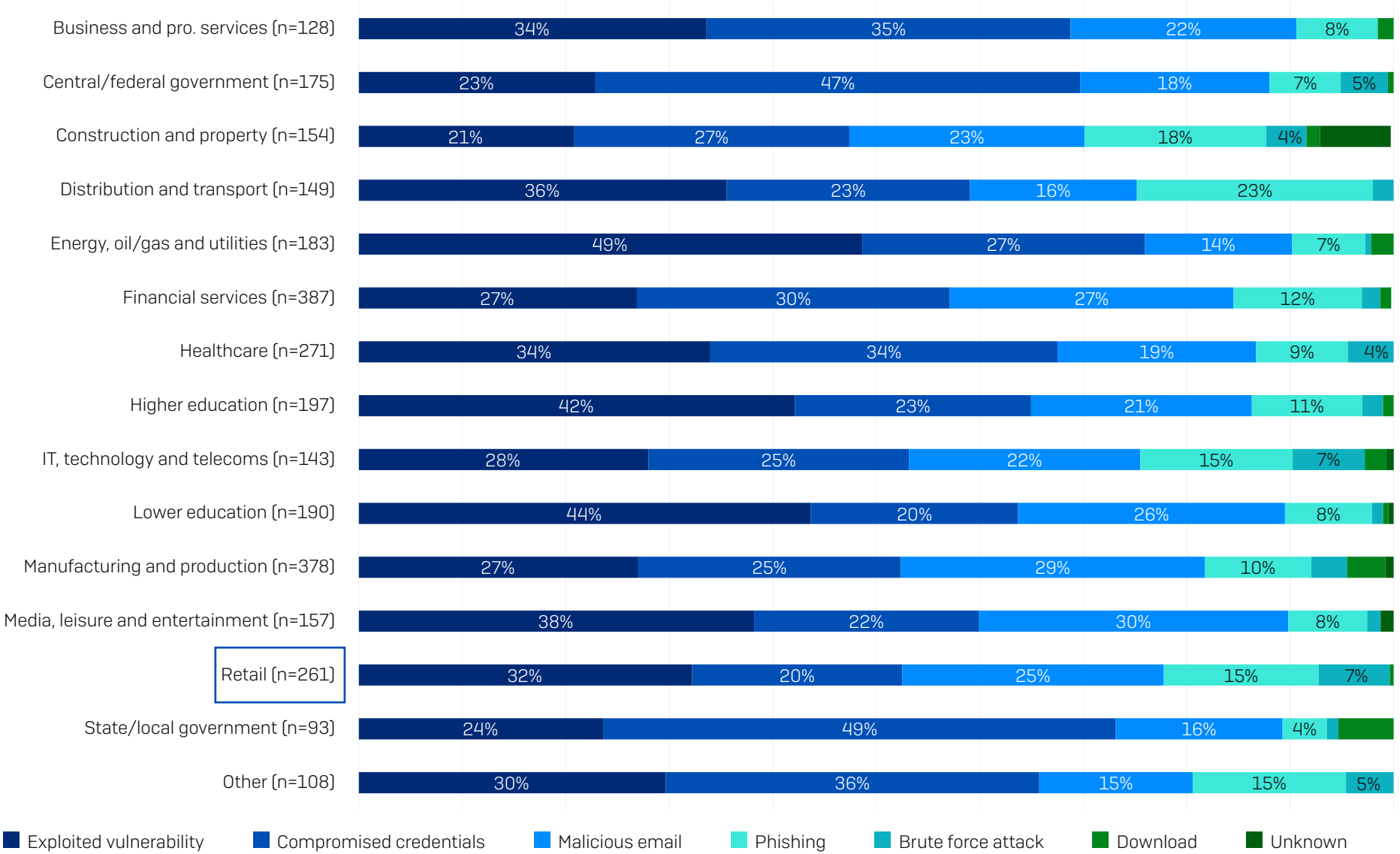
Percentage of Computers Impacted by Industry

Percentage of devices impacted



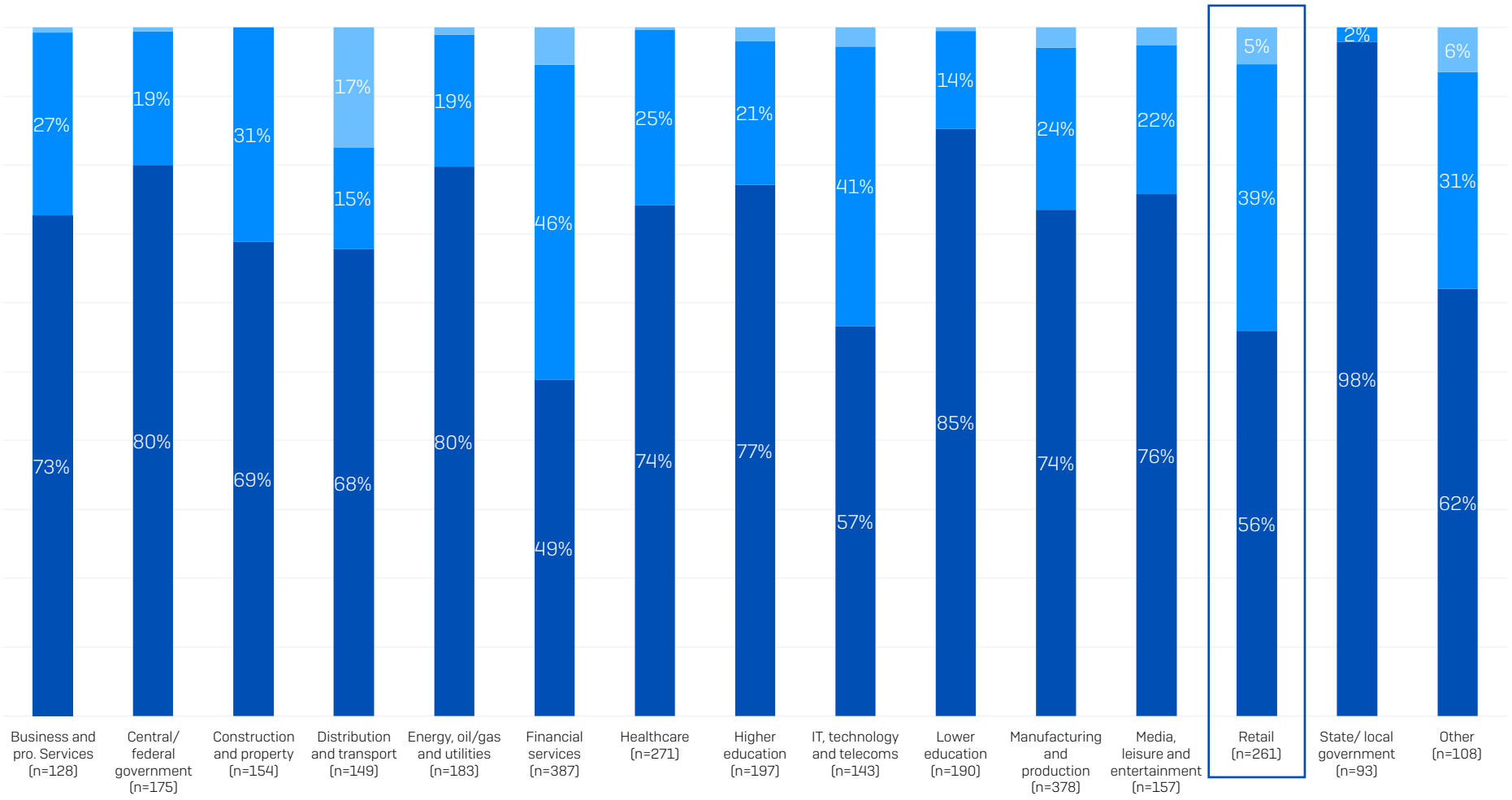
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

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.

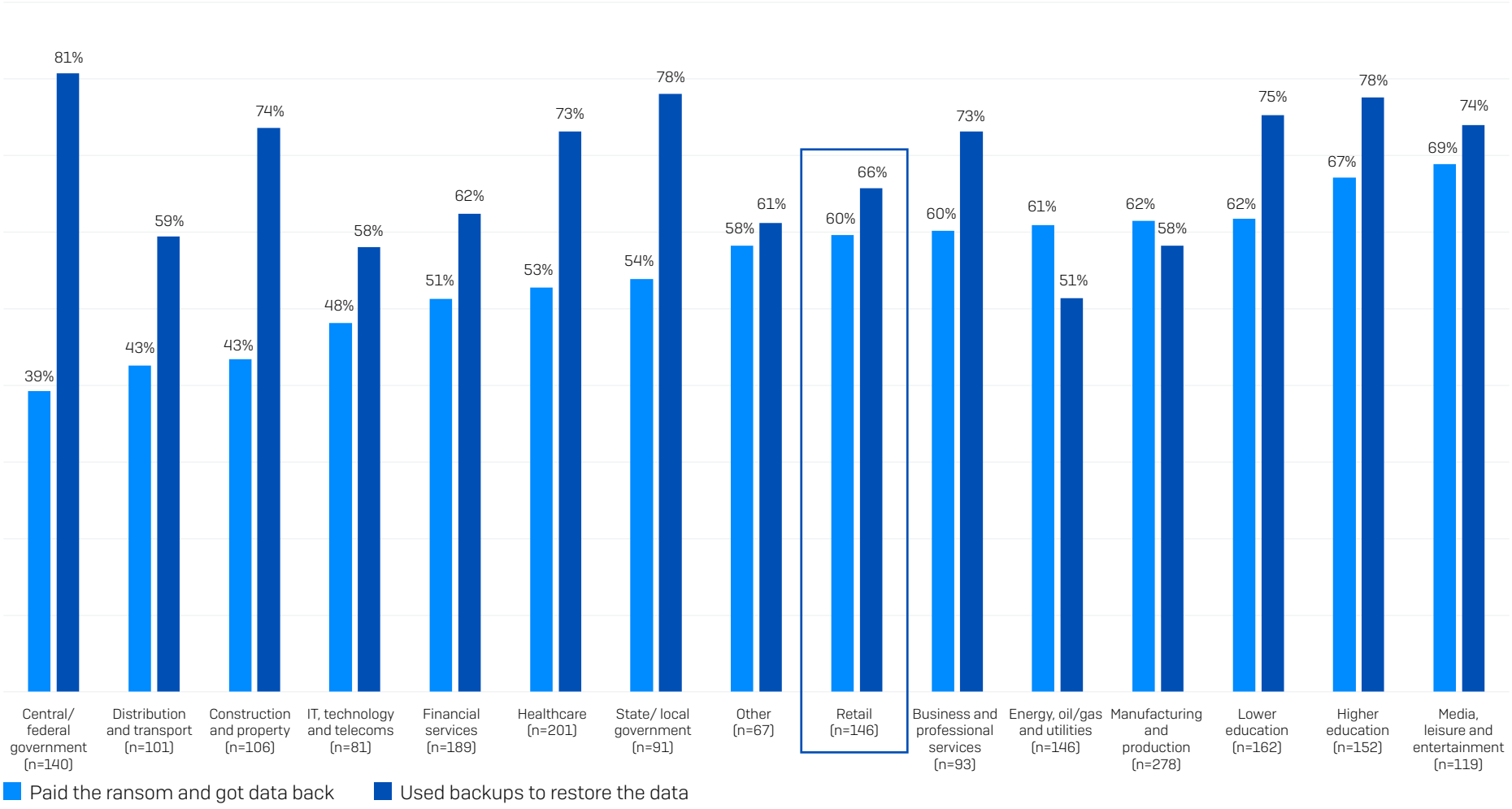
Data Encryption Rate by Industry



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

Data Recovery Method by Industry

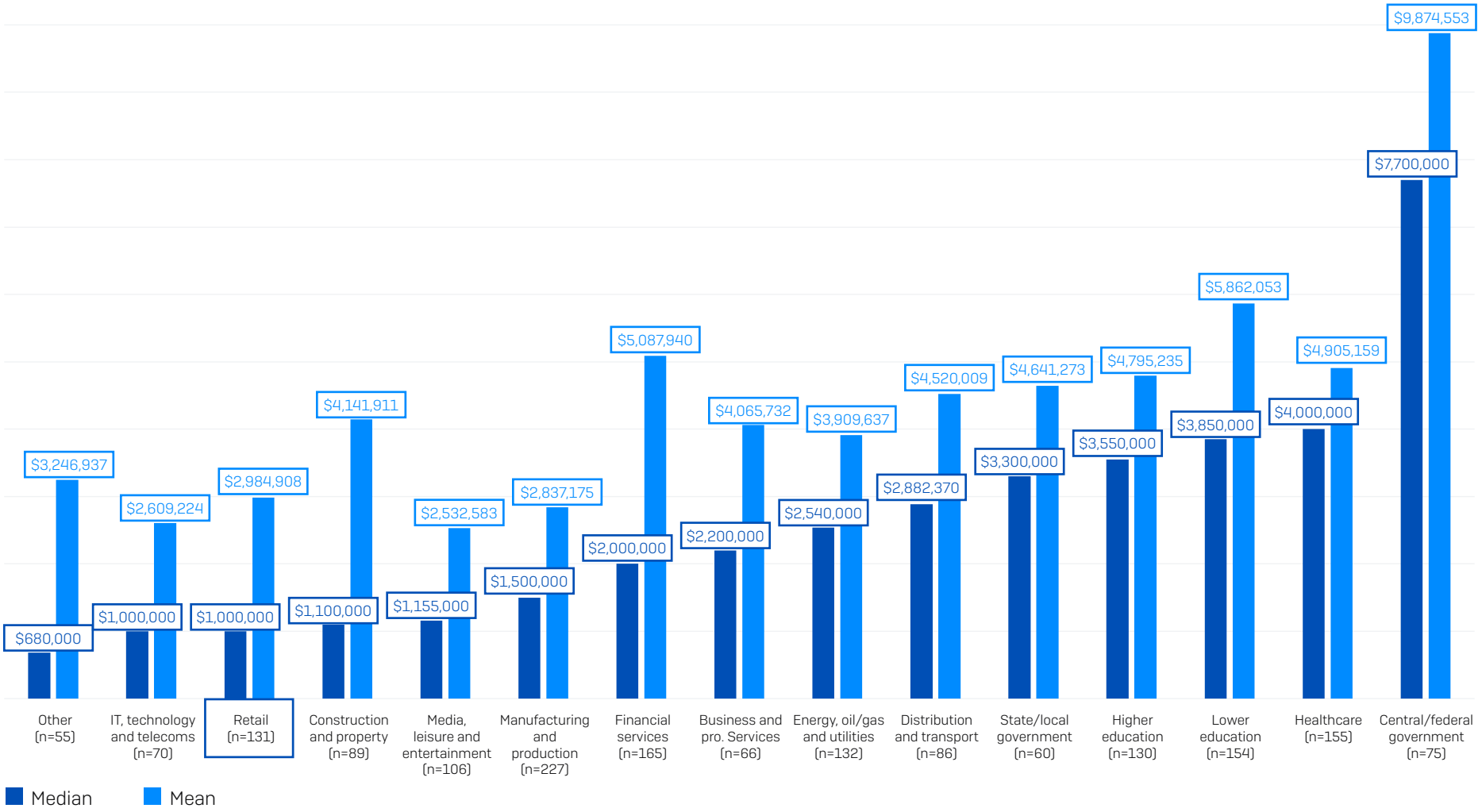
Percentage that got encrypted data back that used the recovery method



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

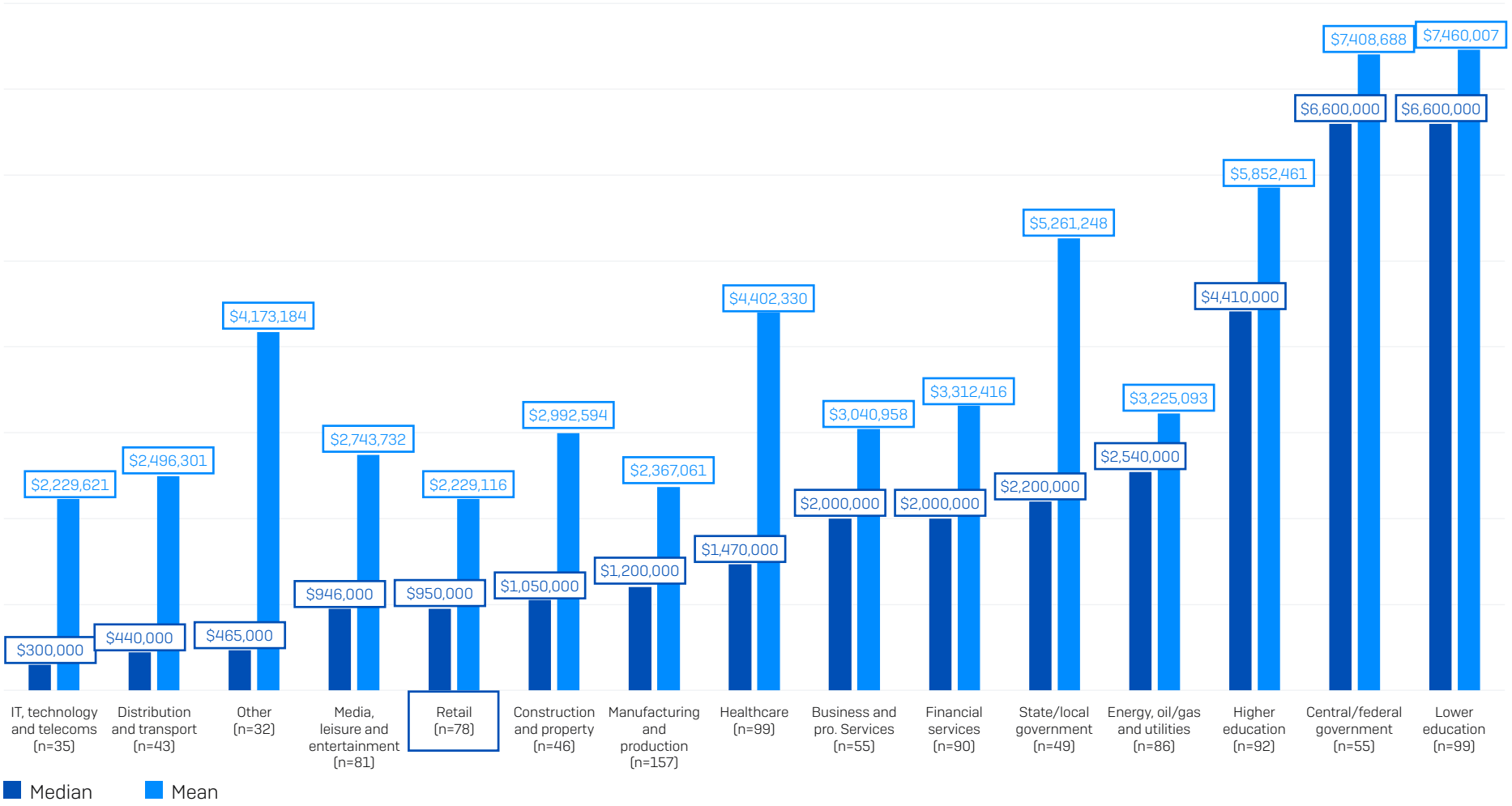
Ransom demand



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

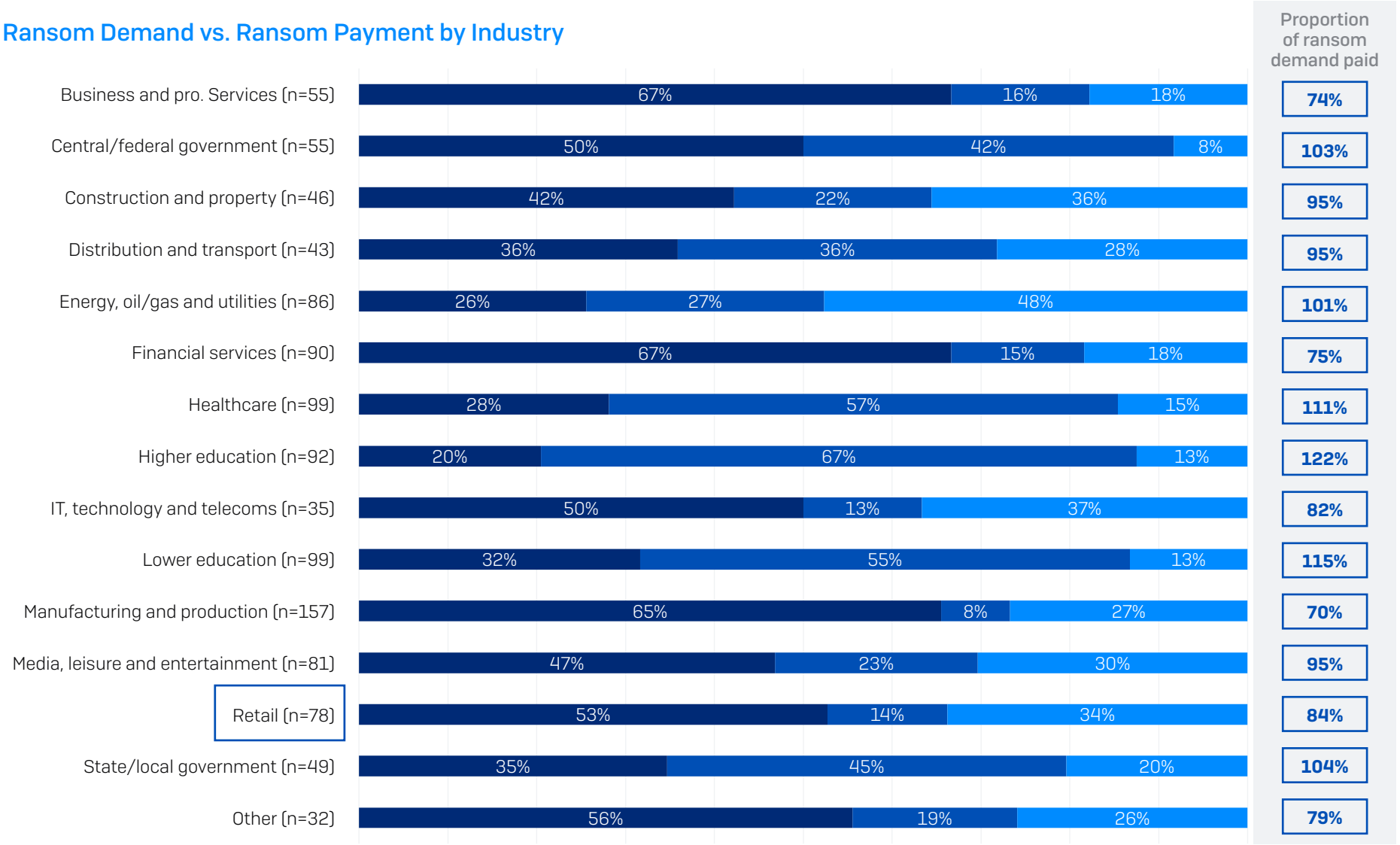
Ransom Payment by Industry

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



Percentage that paid LESS than the original demand

Percentage that paid MORE than the original demand

Percentage that paid the ORIGINAL demand

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.

2024-06-04 WP-EN (PC)

SOPHOS