SOPHOS

The State of Ransomware in Healthcare 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity across 14 countries, including 402 from the healthcare sector, conducted in January-February 2024.

A Sophos Whitepaper. August 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 healthcare organizations 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 exploring ransom demands vs. ransom payments. Plus, for the first time, it shines a light on the role of law enforcement in ransomware remediation for healthcare organizations.

5,000
respondents

402
from the healthcare industry

14
countries

100-5,000
employee organizations
(50% 100-1,000, 50% 1,001-5,000)

15
industry segments

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 402 respondents from healthcare 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 Healthcare

67% of healthcare organizations were hit by ransomware in 2024, up from 60% reported in our 2023 study. Healthcare's ransomware attack rate this year is almost double that reported by the sector in 2021 (34%).

2021	2022	2023	2024
34%	66%	60%	67%

In the last year, has your organization been hit by ransomware?
Yes. n=402 (2024), 233 (2023), 381 (2022), 328 (2021)

The healthcare sector's experience contrasts with the global cross-sector average, which revealed a drop in attack rate: 59% of organizations reported being hit in our 2024 study, down from 66% in the previous two years. Across all sectors, healthcare reported the second-highest attack rate globally, joint with *energy, oil/gas and utilities. Central/federal government* organizations (68%) reported the highest attack rate.

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

Percentage of Computers Impacted in Healthcare

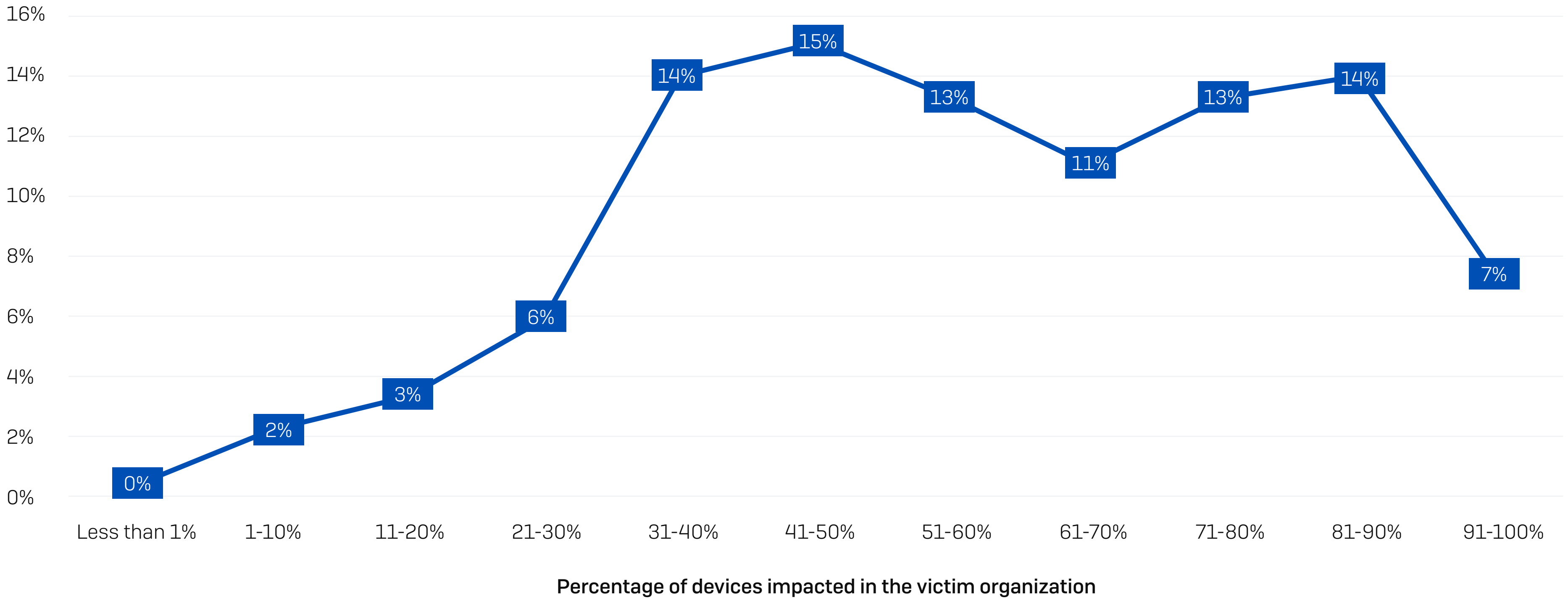
On average, 58% of computers in healthcare organizations are impacted by a ransomware attack.

It is extremely rare for healthcare organizations to have their full environment encrypted: only 7% 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. In the case of healthcare, only one respondent said that less than 1% of their devices were affected.

Healthcare and *energy, oil/gas and utilities* (62%) are the two sectors with the highest percentage of devices impacted in an attack. 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.

Proportion of respondents



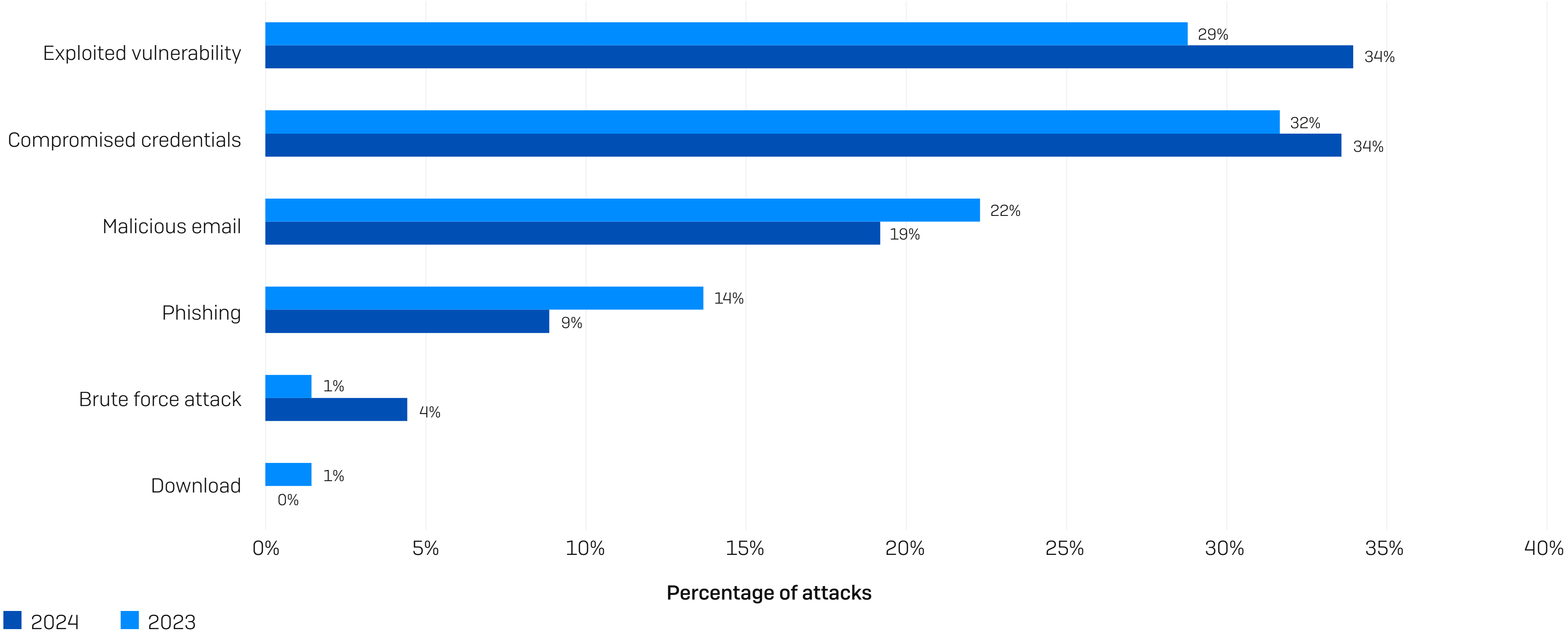
What percentage of your organization's computers were impacted by ransomware in the last year? n=271 healthcare organizations hit by ransomware

Root Causes of Ransomware Attacks in Healthcare

All organizations in the healthcare sector hit by ransomware were able to identify the root cause of the attack. In 2024, exploited vulnerabilities and compromised credentials (both at 34%) were the most common entry methods for ransomware attacks in this sector, followed by malicious emails, which were the root cause of 19% of attacks. Globally, for the second year in a row, across all sectors, exploited vulnerabilities topped the list as the most common root cause (32%) of ransomware attacks, with compromised credentials in second place (29%).

Government organizations are particularly susceptible 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. *Energy, oil/gas and utilities* is the sector most likely to fall victim to exploiting unpatched vulnerabilities, with almost half (49%) of attacks beginning in this way. The *media, leisure and entertainment* (30%), and *manufacturing and production* (29%) sectors reported the highest rates of malicious email-based attacks.

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=271 (2024)/139 (2023) healthcare organizations hit by ransomware.

Backup Compromise in Healthcare

95% of healthcare organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack, slightly above the global average of 94%.

Two-thirds (66%) of the healthcare compromise attempts were successful. This is one of the highest rates of backup compromises, with only the *energy, oil/gas and utilities* (79%) and *education* (71%) sectors reporting higher rates.

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

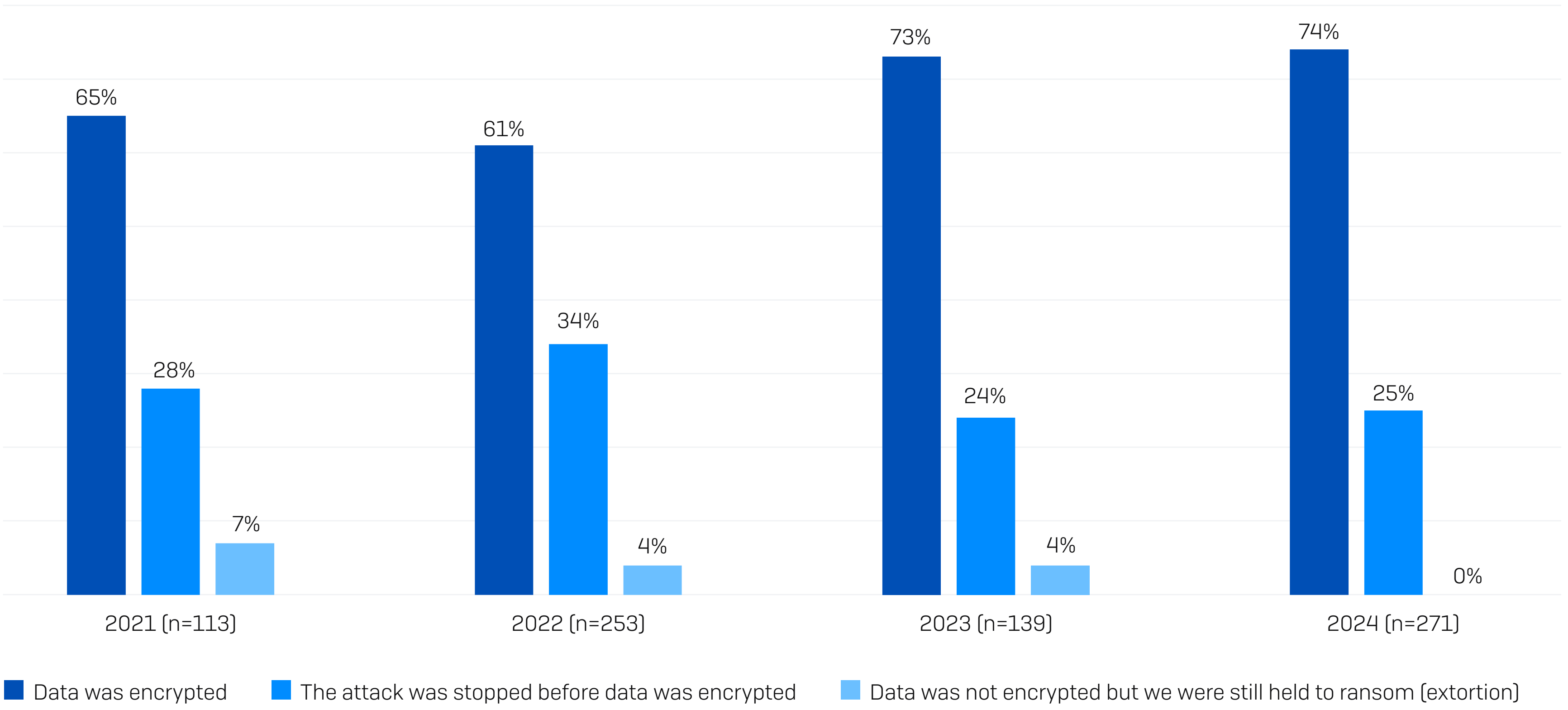
- Ransom demands were, on average, more than three times that of those whose backups weren't impacted ($4.4M vs. $1.3M median initial ransom demand)
- Organizations whose backups were compromised were more than twice as likely to pay the ransom to recover encrypted data (63% vs. 27%)
- Median overall recovery costs were double that of those that did not have backups compromised ($750K vs. $375K)

Rate of Data Encryption in Healthcare

74% of ransomware attacks on healthcare organizations resulted in data encryption, almost identical to the encryption rate reported in 2023 (73%) and higher than the global cross-sector average of 70%.

25% of attacks in healthcare were stopped before data was encrypted, in line with last year's 24%. The sector reported a drop in extortion-only attacks, with only a single respondent reporting such an attack, compared to 4% in our 2023 study.

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. Healthcare respondents reported that in 22% of incidents where data was encrypted, data was also stolen – a considerable (and welcome) decrease from the 37% reported by healthcare respondents 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.

22%

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=271)

The healthcare sector reported the second-lowest rate of encryption with data theft (joint with *lower education*); only *higher education* (18%) reported a lower rate.

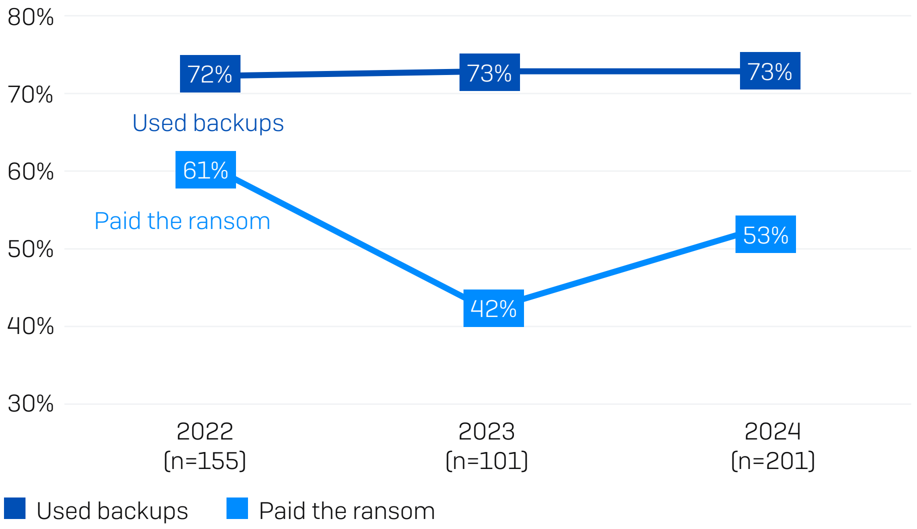
Data Recovery

98% of healthcare organizations that had data encrypted got their data back. While 73% of healthcare organizations restored encrypted data using backups, 53% paid the ransom to get data back, and 29% 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 and 56% paid the ransom.

Use backups to restore data	Paid the ransom and got data back	Use other means to get data back
73%	53%	29%

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=201)

Over the last three years, the healthcare sector's use of backups has remained steady (73% in 2023; 72% in 2022). However, the propensity of healthcare organizations to pay ransom has increased considerably in the last year (42% in 2023), although it remains lower than the 61% reported in 2022.



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, 52% of healthcare organizations that had data encrypted reported using more than one method, three times the rate reported in 2023 (17%).

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

Ransom Demands

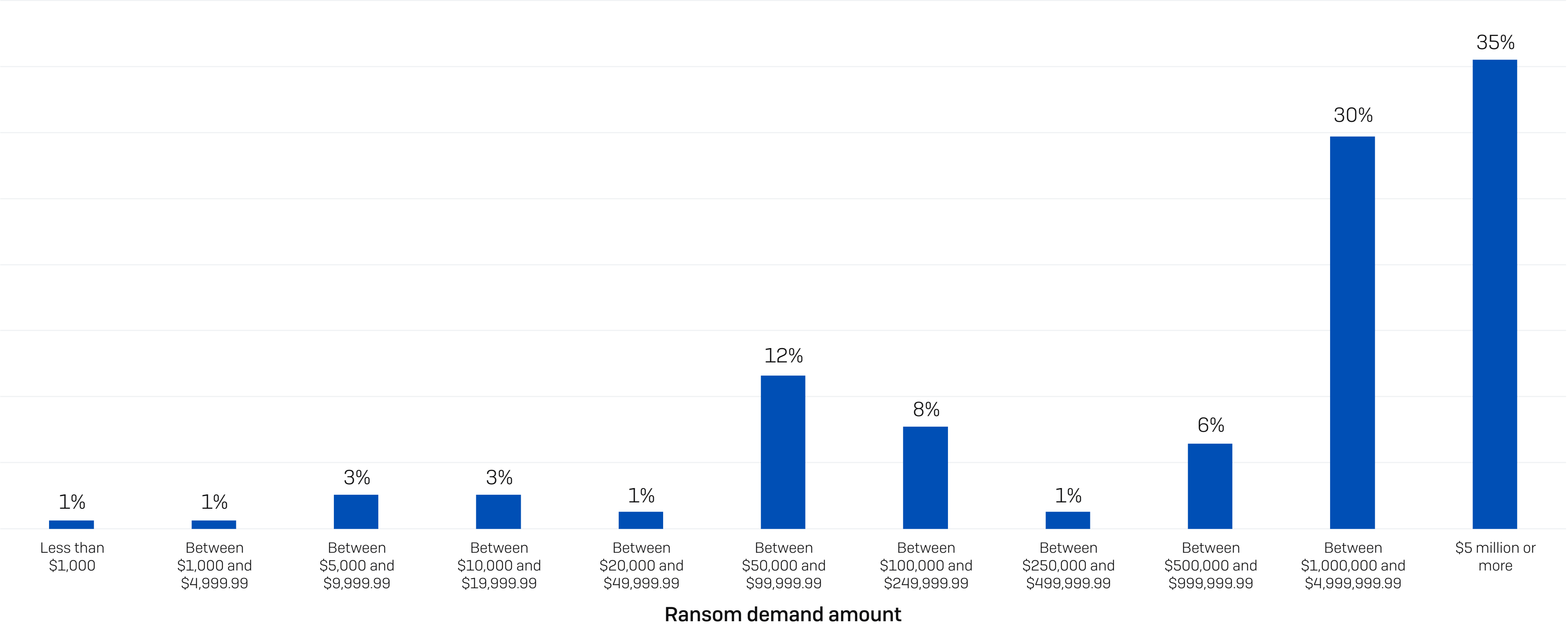
This year, for the first time, we included both ransom demands and payments in this report. Across the 155 healthcare organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was $4M (median), the second highest across sectors after *central/federal government* organizations, and the average mean was $4.9M.

One of the most notable findings in this year's study is that 65% of ransom demands in healthcare organizations are for $1M or more, with 35% of demands for $5M or more.

High ransom demands were common across all industries 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 of $1M, while *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=155

Ransom Payments

99 healthcare respondents whose organizations paid the ransom shared the actual sum paid.

- Median payment: $1.5M
- Mean payment: $4.4M

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.

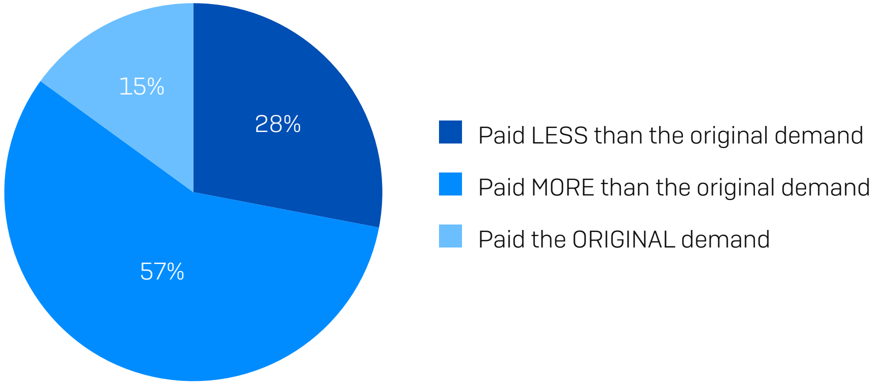
See the appendix for a detailed breakdown of average ransom payment by industry.

Propensity to Negotiate Ransom Amounts in Healthcare

Healthcare victims rarely pay the initial sum demanded by the attackers. The study revealed that only 15% paid the initial ransom demand. 28% paid less than the original demand, while 57% paid more.

On average, across all healthcare respondents, organizations paid 111% 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=99.

Healthcare was second most likely to pay more than the original ransom demand; *higher education* had the highest propensity to pay more (67%). The sectors most likely to pay more than the original demand are also those with a high proportion of public sector organizations. 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.

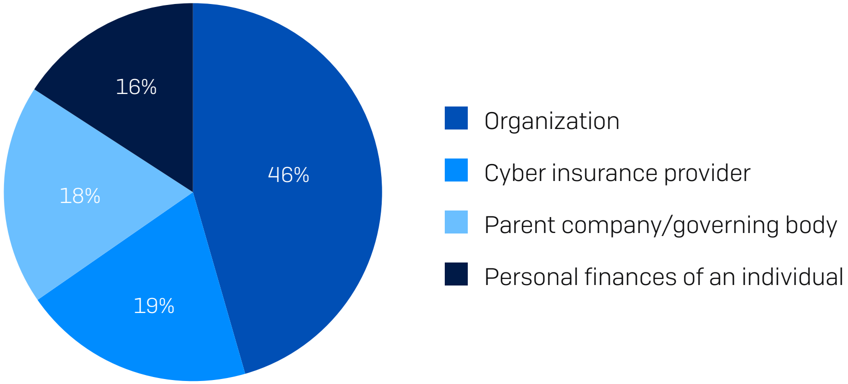
See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

Source of Ransom Funding in Healthcare

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 healthcare respondents reporting multiple sources of payment in 76% of cases
- The primary source of ransom funding in healthcare organizations is the organization itself, covering almost half (46%) of the payment on average; the organization's parent company and/or governing body typically provides 18%
- Insurance providers are heavily involved in ransom payments, contributing in 77% of cases. 19% 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=107

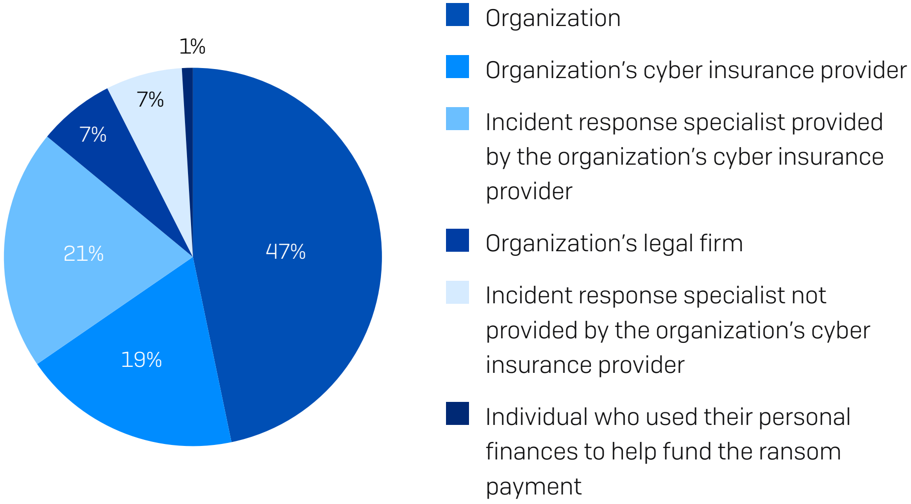
Ransom Transaction Execution

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

In the healthcare sector, insurance providers transferred the funds for 39% of ransom transactions, either directly (19%) or through their appointed incident response specialist (21%). The victim organization made almost half (47%) of payments, while 7% were executed by the victim's legal firm.

27% of transfers were made by incident response specialists, whether appointed by the insurance provider (21%) or another party, typically the victim (7%).

Executor of ransom payment transfer



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=107

Recovery Costs in Healthcare

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, healthcare organizations reported a mean cost of $2.57M to recover from a ransomware attack, an increase from the $2.2M reported in 2023. Recovery costs in the sector have doubled since 2021, when the average bill came in at $1.27M.

In comparison, the average cross-sector recovery costs were $2.73M in 2024 and $1.82M in 2023.

2021	2022	2023	2024
$1.27M	$1.85M	$2.20M	$2.57M

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=271 (2024)/139 (2023)/ 253 (2022)/ 113 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

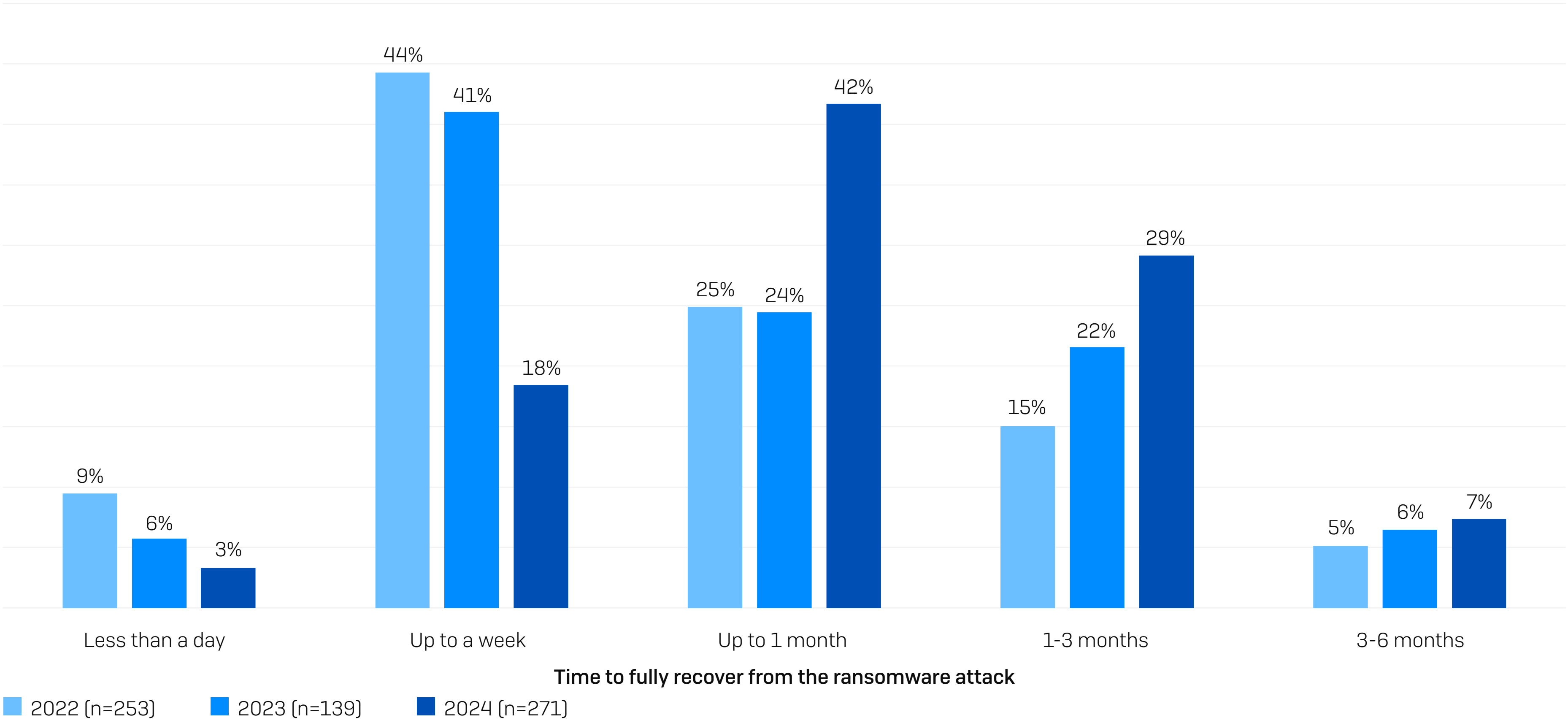
The median recovery cost data for healthcare organizations remained steady in the last two years at $750,000. The cross-sector average revealed that the median recovery costs doubled from $375,000 to $750,000 over the last year.

Recovery Time in Healthcare

The time taken to recover from a ransomware attack has steadily increased in healthcare. Our 2024 research revealed:

- 22% of ransomware victims were fully recovered in a week or less, a considerable drop from 47% reported in 2023 and 54% in 2022
- 37% took more than a month to recover, up from 28% in 2023

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.

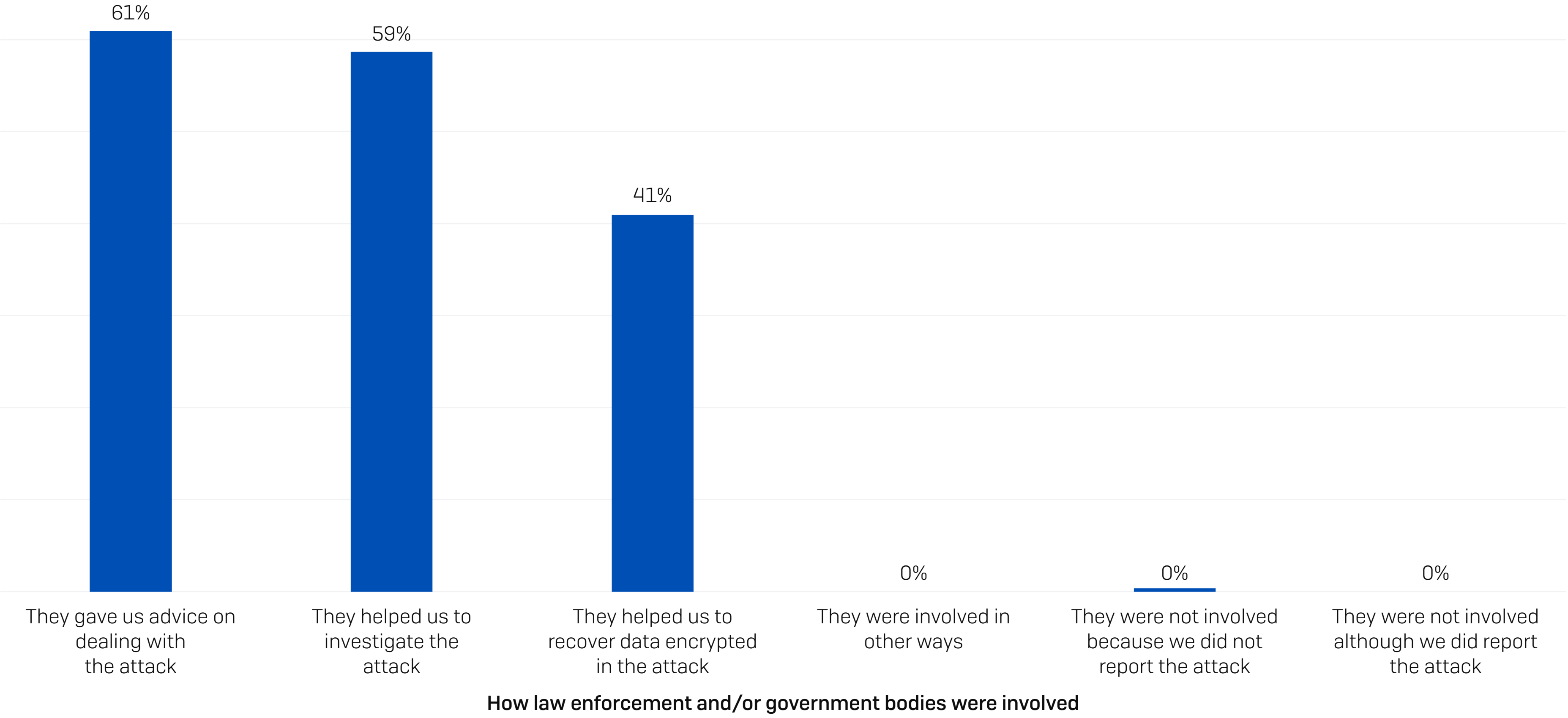


How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

Involvement of Law and Order in Healthcare

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.

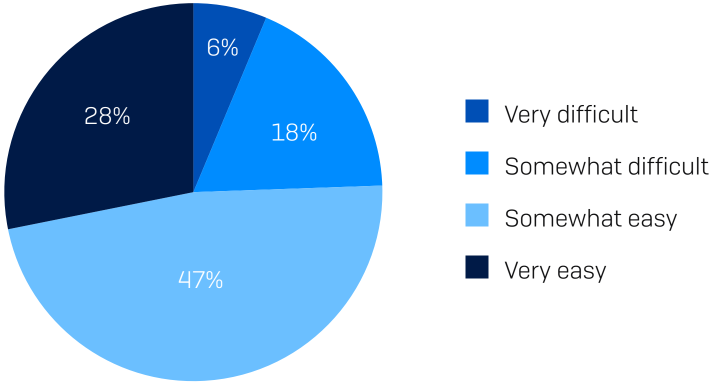
Reflecting the normalization of ransomware, almost all healthcare organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 61% reported that they received advice on dealing with the attack, 59% got help investigating the attack, and 41% said they received help to recover data encrypted in the attack.



If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? n=271

Ease of Engagement in Healthcare

76% of those who engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (28% very easy, 47% somewhat easy). 6% said the process was very difficult, while 18% 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=270 (not showing "don't know" responses).

Conclusion

Ransomware remains a major threat to healthcare organizations of all sizes around the globe. While the attack rate has dropped globally, the healthcare sector experienced increased attacks last year. 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. Over one-third (34%) of attacks start with the exploitation of unpatched vulnerabilities in healthcare, so 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 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.

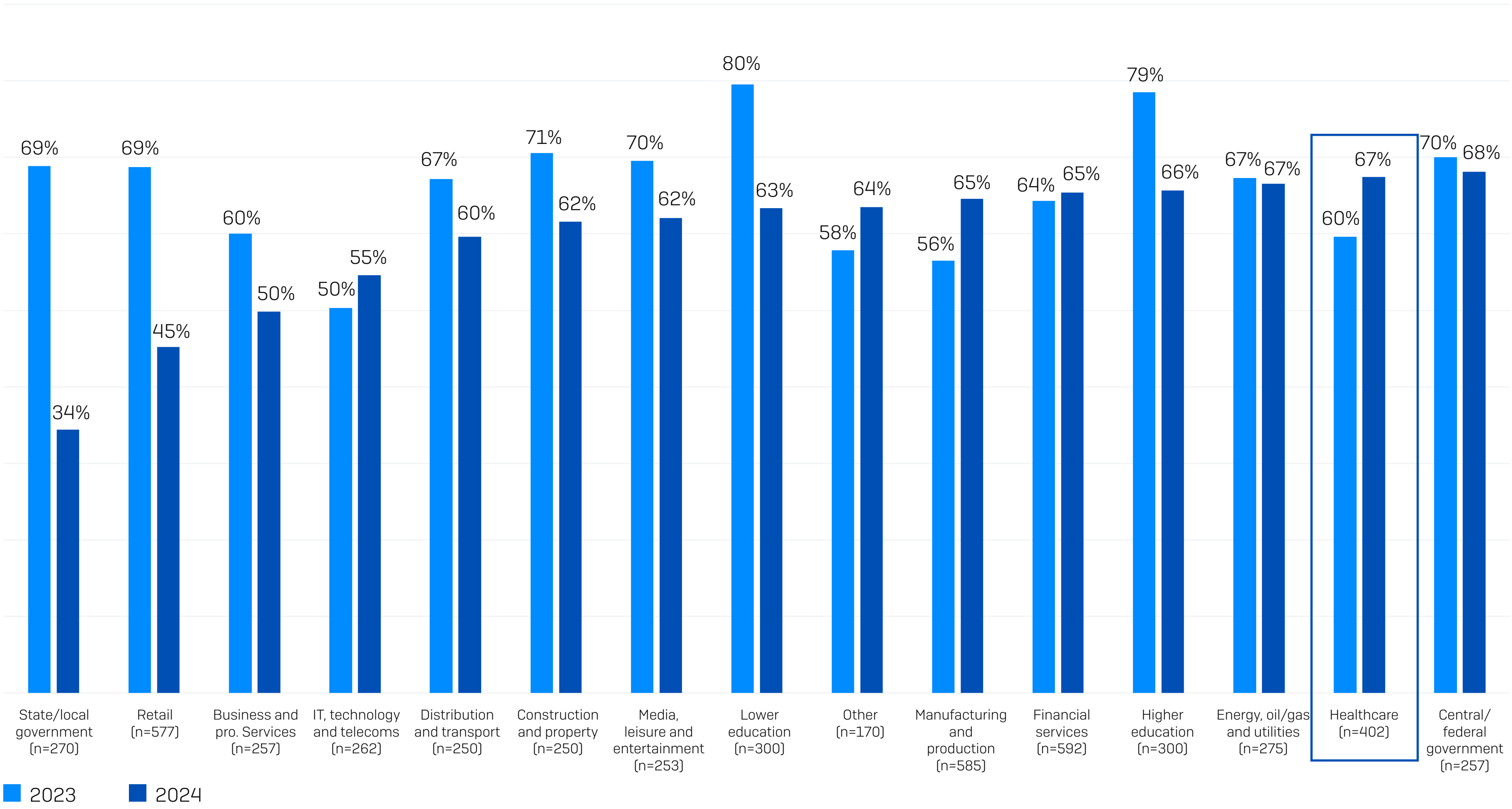
About Vanson Bourne

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

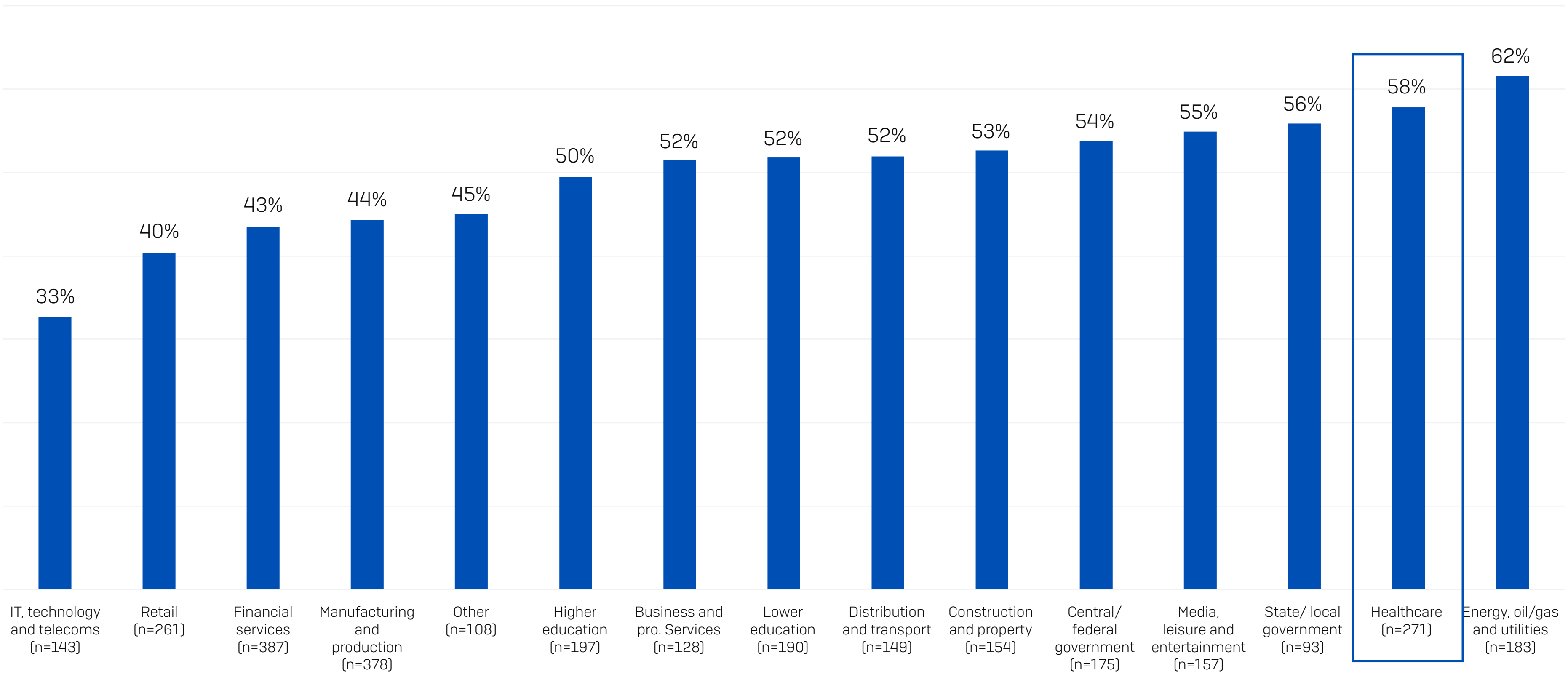
Percentage of organizations hit by ransomware in the last year



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.

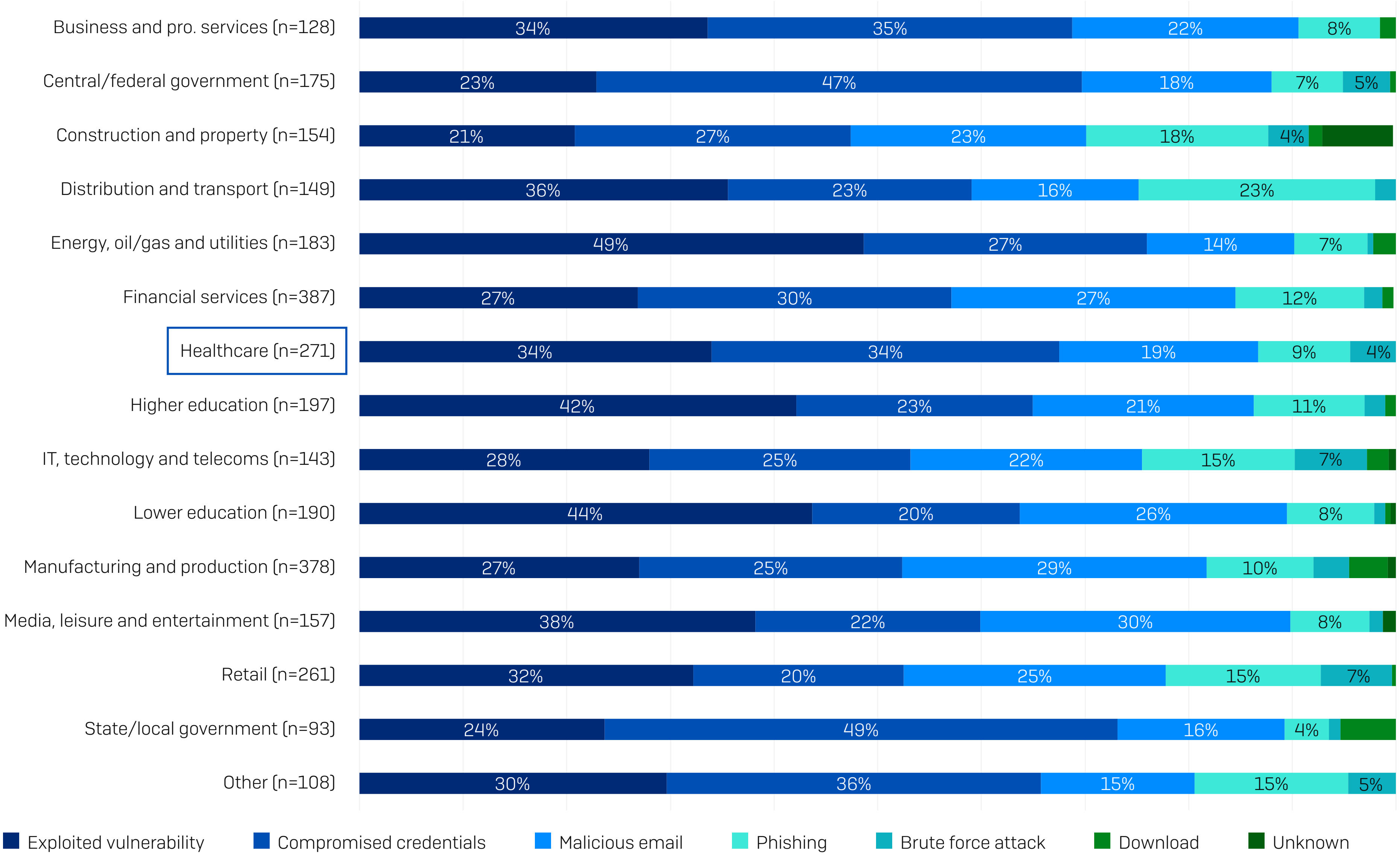
Percentage of Computers Impacted by Industry

Percentage of devices impacted



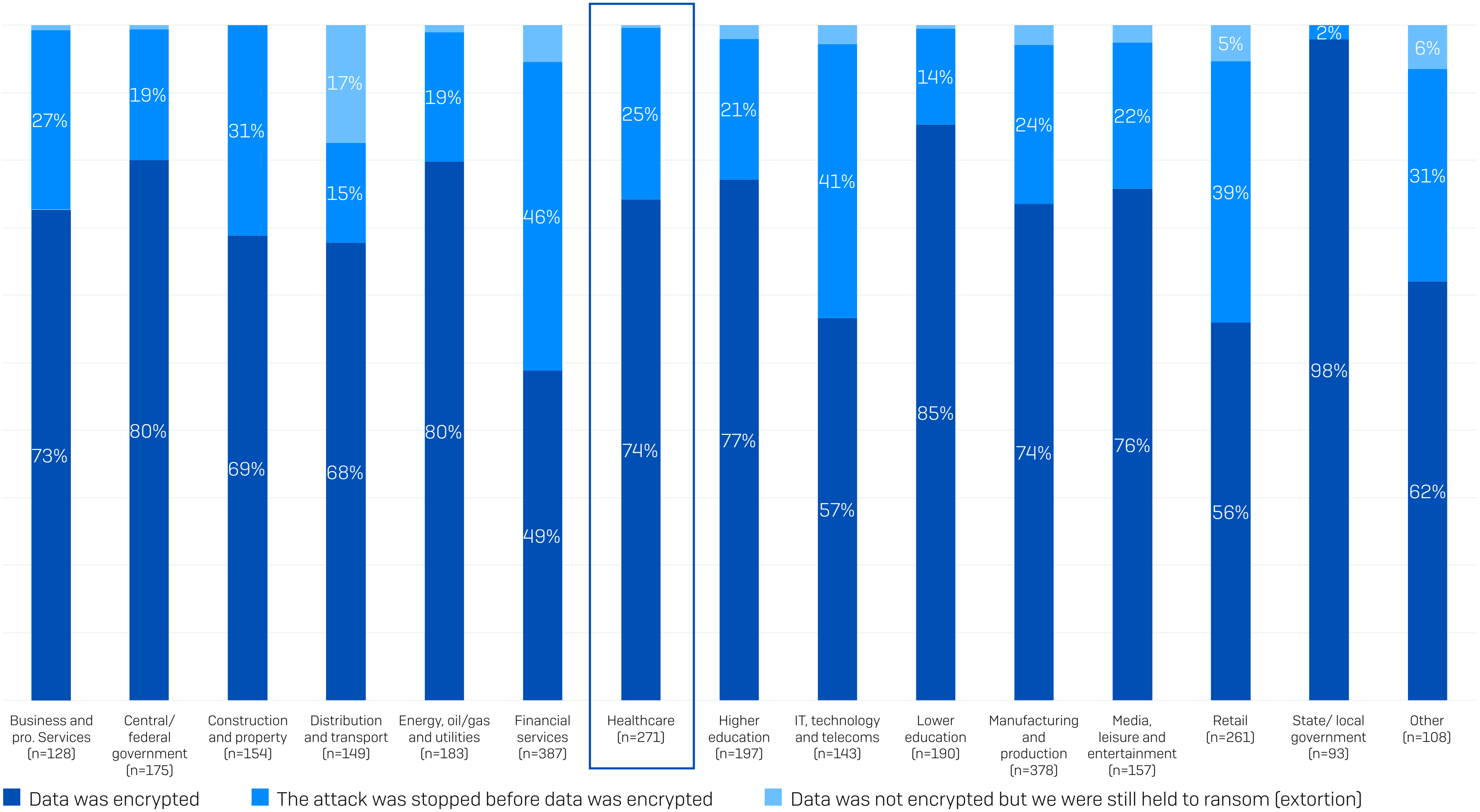
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

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.

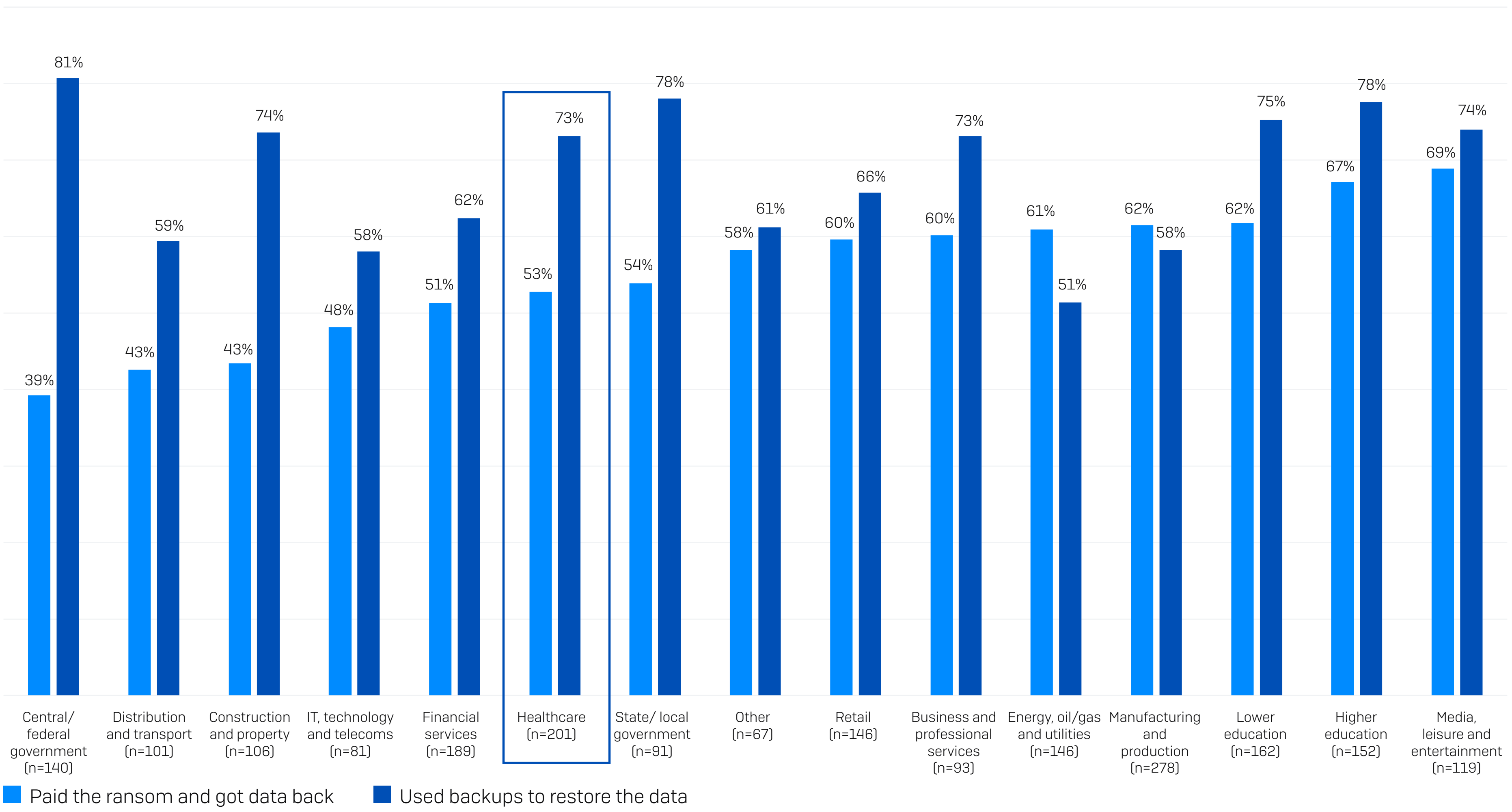
Data Encryption Rate by Industry



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

Data Recovery Method by Industry

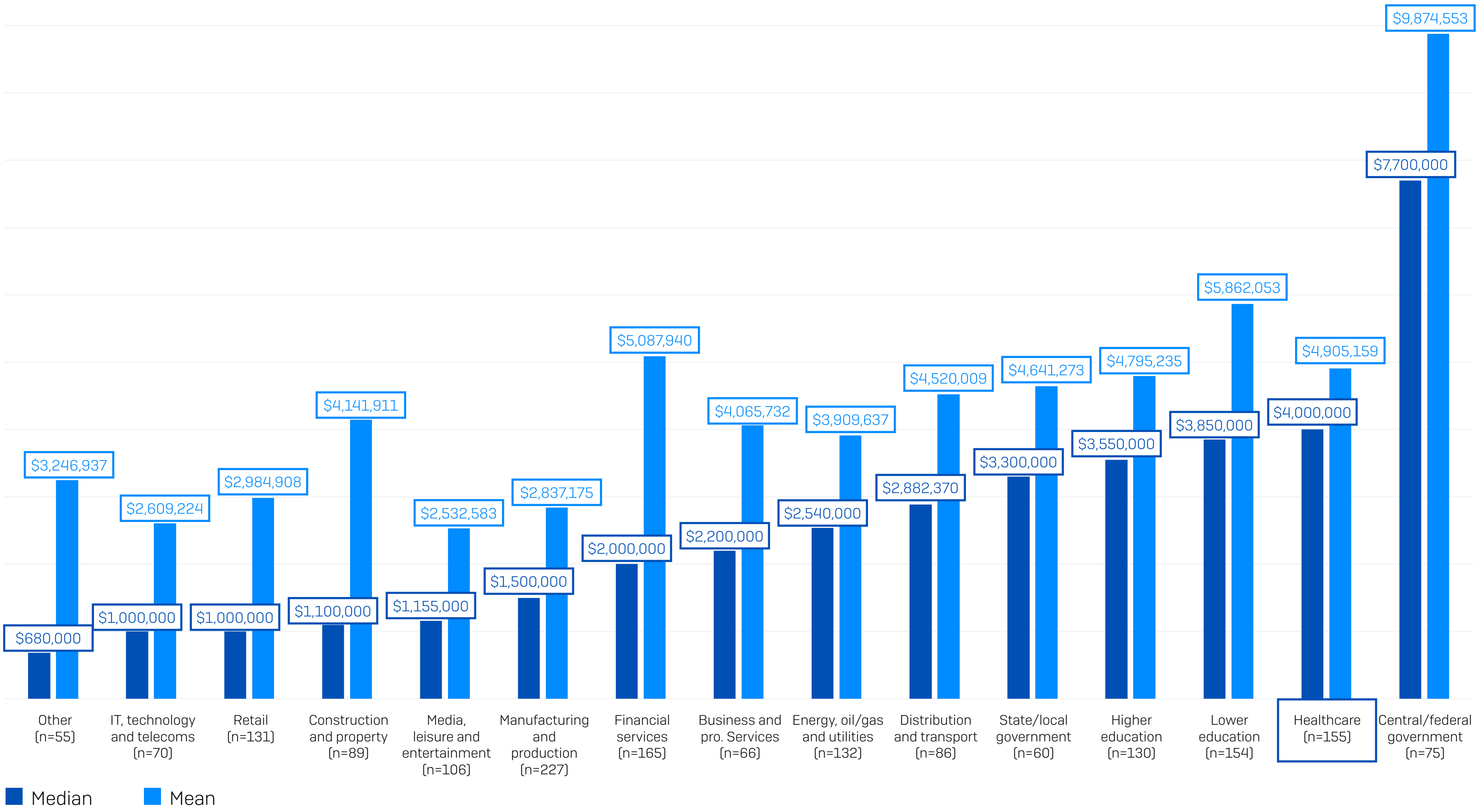
Percentage that got encrypted data back that used the recovery method



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

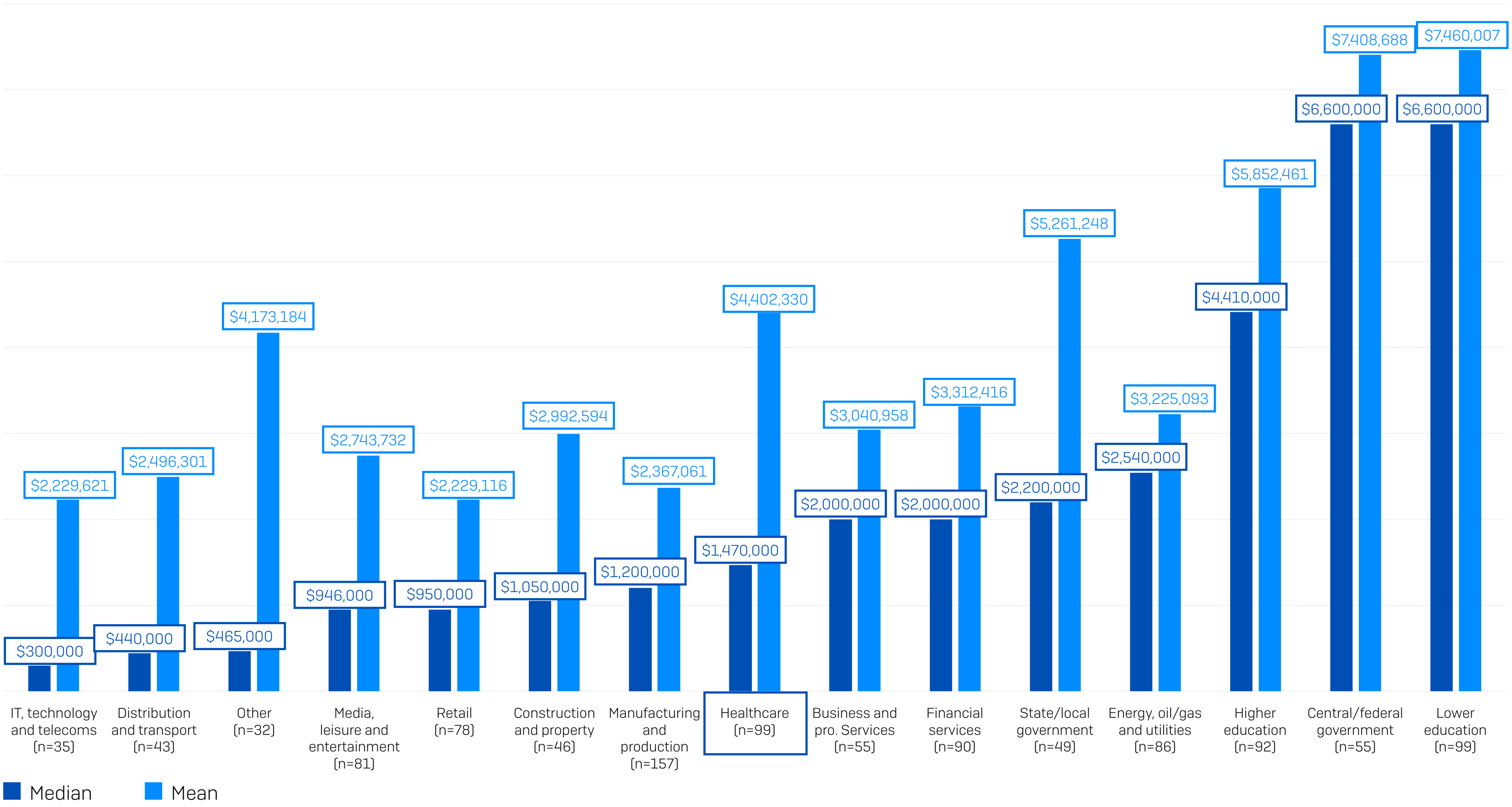
Ransom demand



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

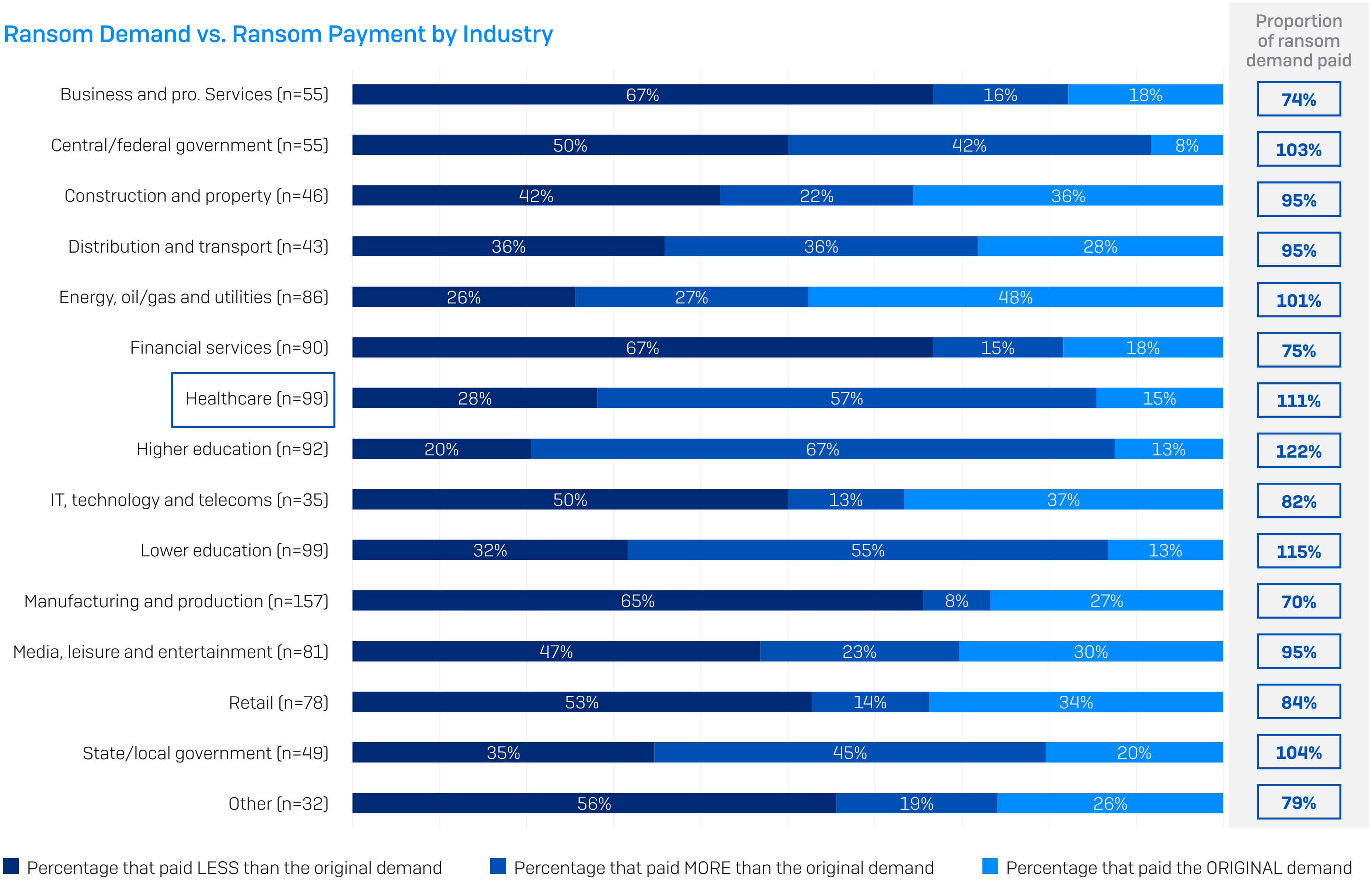
Ransom Payment by Industry

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



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.