SOPHOS

The State of Ransomware in Financial Services 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity, including 592 from the financial services 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 financial services organizations today and how the impact of ransomware has evolved over the last five 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 financial services 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 592 respondents from financial services 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.

5,000
respondents

592
from the financial services industry

14
countries

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

15
industry segments

Rate of Ransomware Attacks in Financial Services

65% of financial services organizations were hit by ransomware in 2024, in line with the 64% rate reported in 2023 but above the rate reported in the previous two years.

2020	2021	2022	2023	2024
48%	34%	55%	64%	65%

In the last year, has your organization been hit by ransomware?
Yes. n=592 (2024), n=336 (2023), 444 (2022), 550 (2021), 547 (2020)

This year's financial services 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. The ransomware attack rate reported by financial services organizations is higher than that reported by most other sectors in our study, with the central/federal government reporting the highest rate of 68%.

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

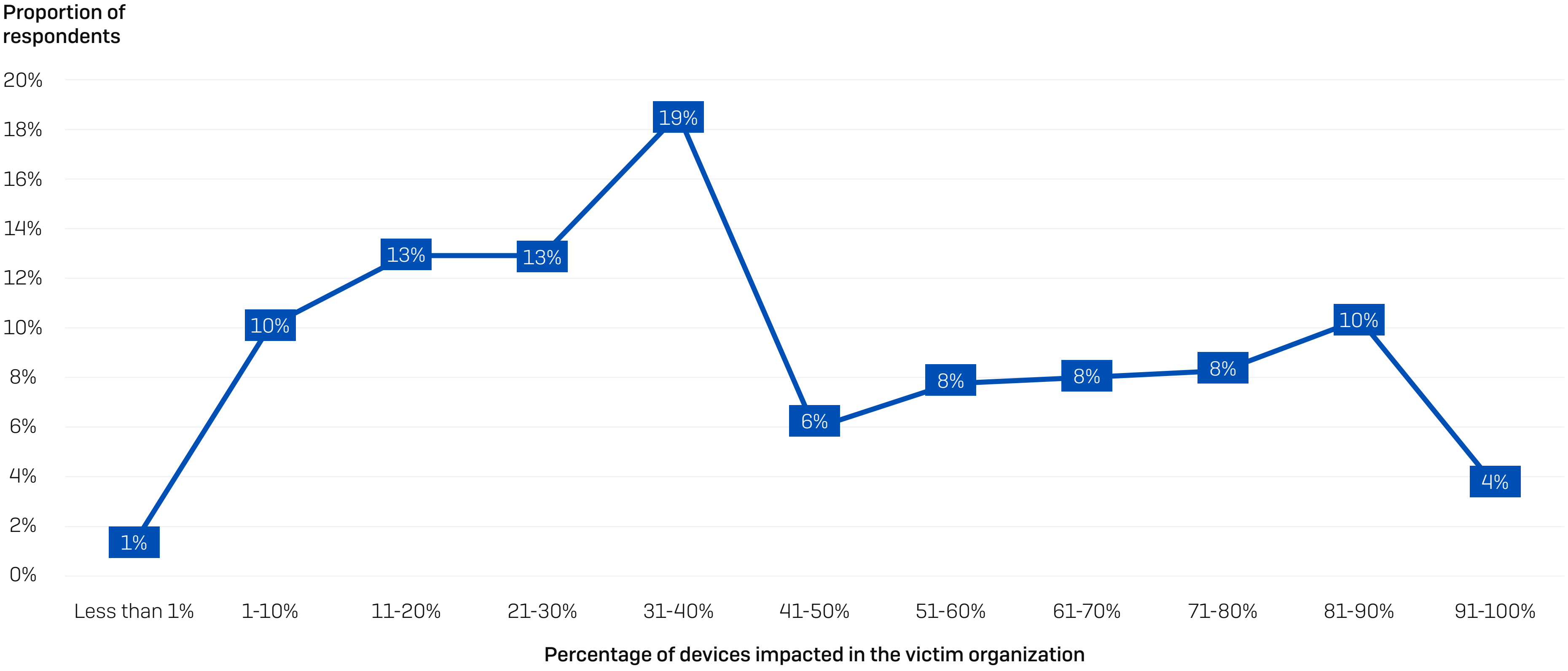
Percentage of Computers Impacted in Financial Services

On average, 43% of computers in financial services organizations are impacted by a ransomware attack, a little below the cross-sector average of 49%. It is extremely rare for financial services to have their full environment encrypted: only 4% 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 1% of financial services organizations saying that fewer than 1% of their devices were affected.

Financial services had the third-lowest percentage of devices impacted by ransomware across all sectors, globally. *IT, technology and telecoms* (33%) reported the lowest percentage, followed by *retail* at 40%.

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=387 financial services organizations hit by ransomware.

Root Causes of Ransomware Attacks in Financial Services

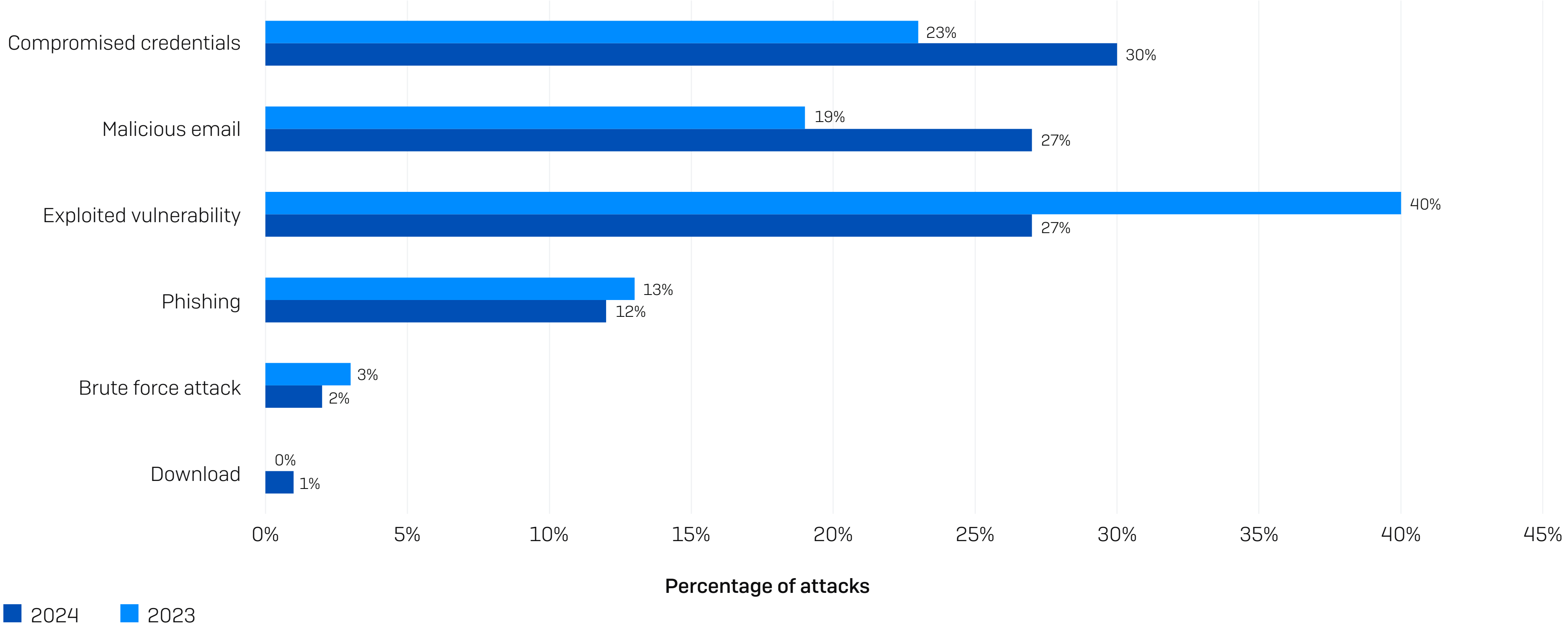
All except one organization in the financial services sector hit by ransomware were able to identify the root cause of the attack. In 2024, the most common entry method of ransomware attacks for this sector was compromised credentials, used in 30% of attacks. Malicious emails and exploited vulnerabilities both came in next at 27%.

These findings contrast with our 2023 study, in which exploited vulnerabilities (40%) were the most common root cause of attacks in the sector, followed by compromised credentials (23%). The 2024 cross-sector trend revealed that exploited vulnerabilities were the most common root cause of attacks (32%), followed by compromised credentials at 29%.

Financial services organizations are more vulnerable to malicious email-based attacks than most other sectors. Only the *media, leisure and entertainment* and *manufacturing and production* sectors reported higher rates of malicious emails.

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 the exploitation of unpatched vulnerabilities, with almost half (49%) of attacks beginning in this way.

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=387 (2024)/216 (2023) financial services organizations hit by ransomware.

Backup Compromise in Financial Services

90% of financial services organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack, a little below the global average of 94%.

Of the compromise attempts, just under half (48%) were successful. This is one of the lowest rates of backup compromises, with only *IT, technology, and telecoms* (30%) and *retail* (47%) reporting lower rates. This indicates that financial services performs above average when it comes to stopping backup compromise activities. Backup compromise attempts on *energy, oil/gas and utilities* are most likely to be successful (79%).

Financial services organizations that had their 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 ($2.24M vs. $1M median initial ransom demand)
- Organizations whose backups were compromised were more likely to pay the ransom to recover encrypted data (63% vs. 38%)
- Median overall recovery costs were considerably more than that of those that did not have backups compromised ($3M vs. $375K)

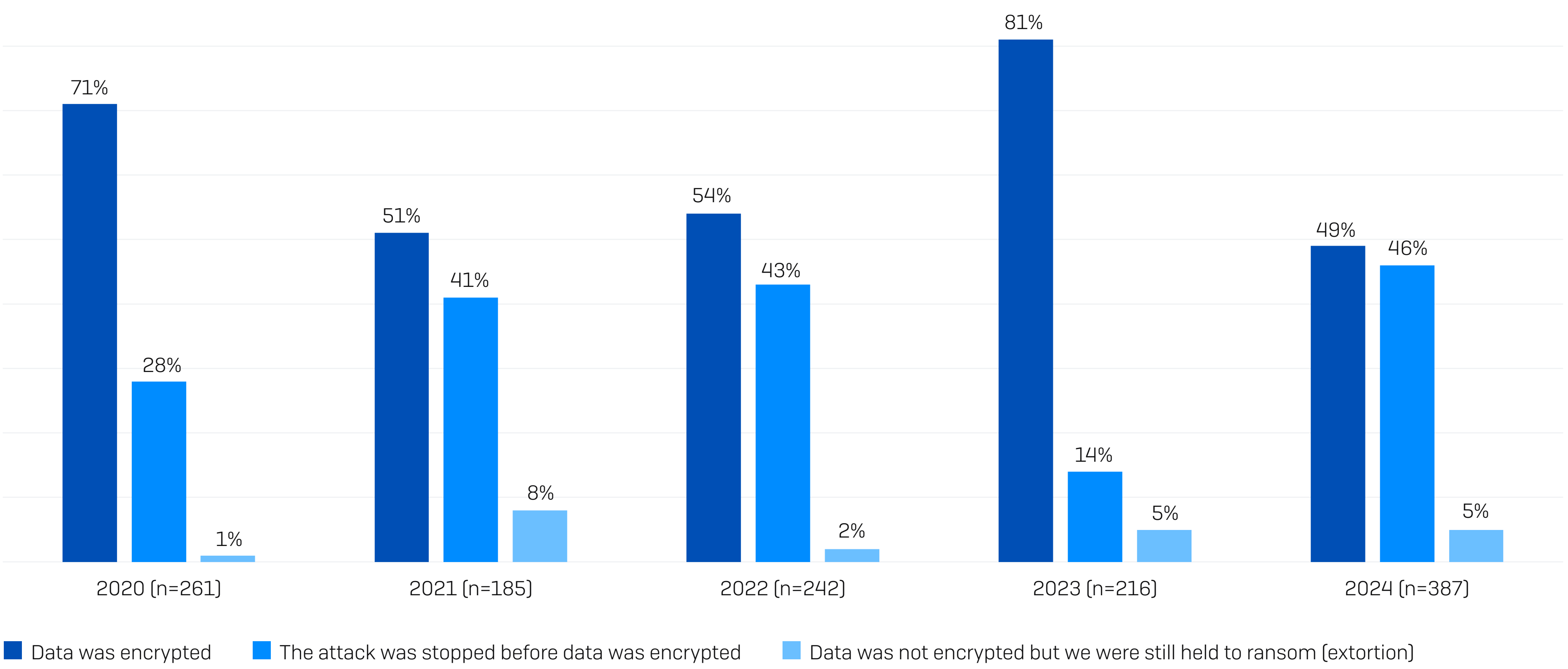
Rate of Data Encryption in Financial Services

49% of ransomware attacks on financial services organizations resulted in data encryption, a substantial and welcome drop from the 81% encryption rate reported in 2023.

46% were stopped before data was encrypted while 5% of financial services organizations experienced an extortion-only attack, where their data was not encrypted but they were held to ransom anyway. This is the second-highest extortion-only rate across all sectors globally, jointly with *retail*. *Distribution and transport* saw the highest rate of extortion-based attacks at 17%.

On a positive note, financial services reported the lowest data encryption rate across all sectors, considerably below the global cross-sector average of 70%. It also has the highest success rate in stopping attacks before data could be encrypted.

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 33% of incidents where data was encrypted, data was also stolen – a considerable increase from the 25% reported by financial services 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.

33%

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=387).

Data Recovery

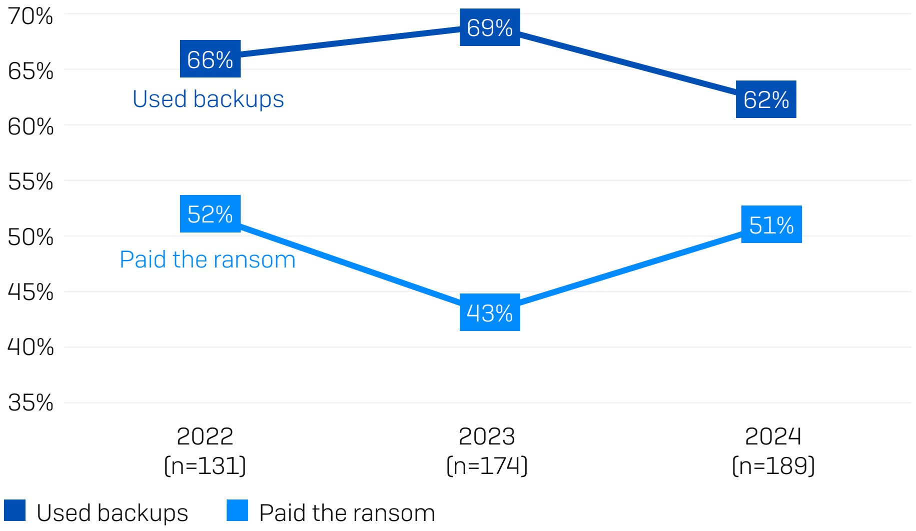
97% of financial services organizations that had data encrypted got their data back. While 62% of financial services organizations restored encrypted data using backups, 51% paid the ransom to get data back, and 23% used other means – while the survey did not explore this area further, this could include 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
62%	**51%**	**23%**

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=189)

The three-year view of financial services organizations reveals that the gap between the use of backups and ransom payment has narrowed over the last 12 months. In 2023, 69% of financial services organizations used backups, and 43% paid the ransom to restore encrypted data after the attack.



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, 37% of financial services organizations 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

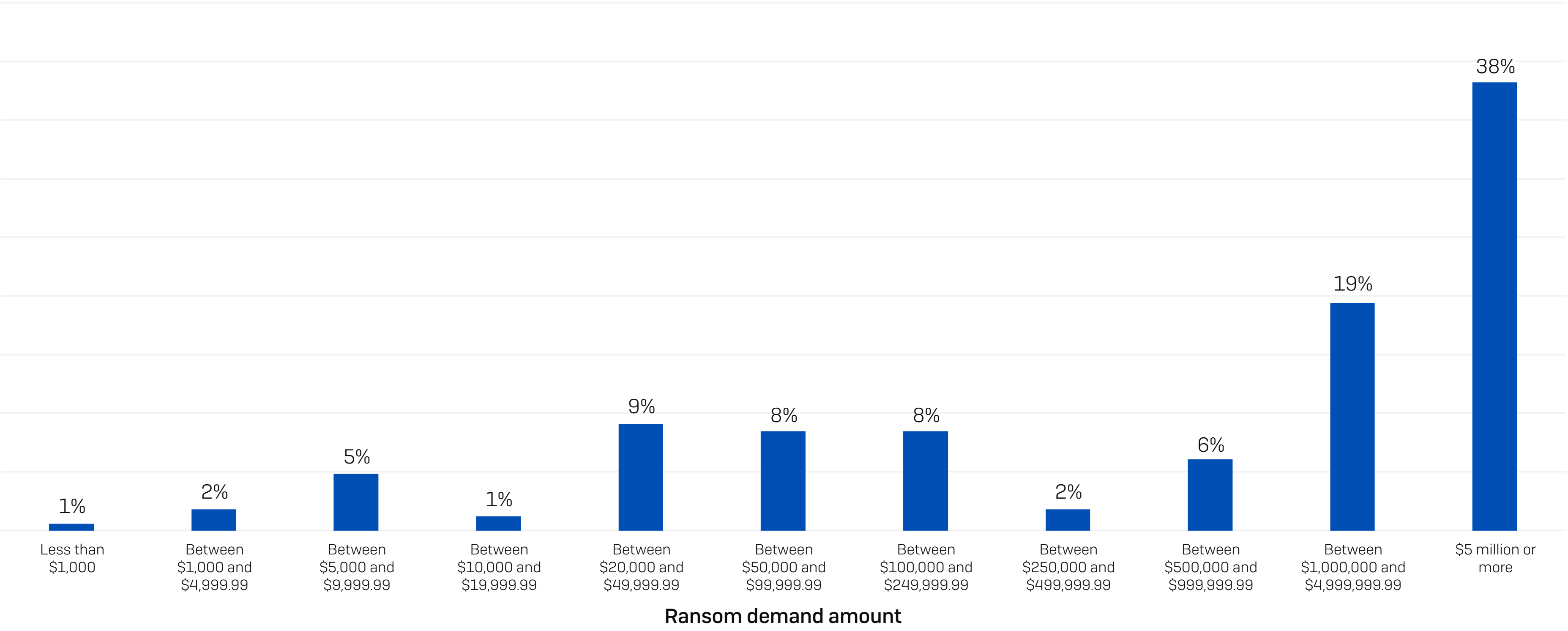
This year, for the first time, we included both ransom demands and payments in this report. Across the 165 financial services organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was $2M (median) and $5.09M (mean).

One of the most notable findings in this year's study is that more than half (58%) of ransom demands in financial services organizations are for $1M or more, with 38% 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=165

Ransom Payments

90 financial services respondents whose organizations paid the ransom shared the actual sum paid. Looking at both median and mean averages, we see that ransom payment amounts have increased considerably in financial services in the last year:

- Median payment: $2M
  (an 18X increase on the $109,000 reported in 2023)
- Mean payment: $3.3M
  (a 2X increase on the $1.7M 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.

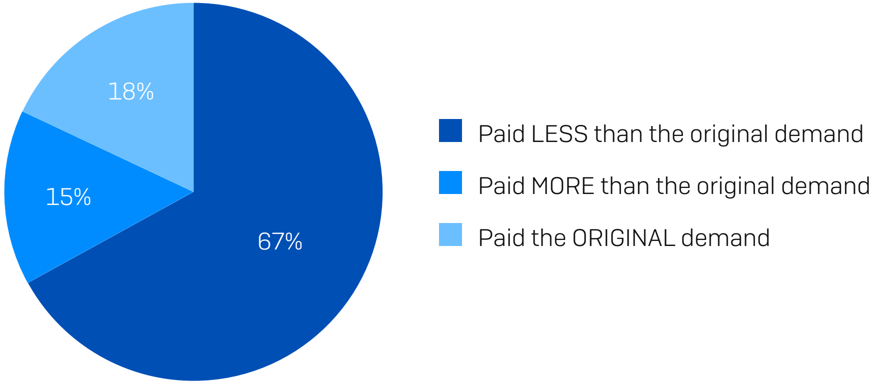
See the appendix for a detailed breakdown of average ransom payment by industry.

Propensity to Negotiate Ransom Amounts in Financial Services

Financial services victims rarely pay the initial sum demanded by the attackers. The study revealed that only 18% paid the initial ransom demand. 67% paid less than the original demand, while 15% paid more.

On average, across all financial services respondents, organizations paid 75% 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=90.

Financial services is the sector most likely to negotiate down the ransom payment, jointly with *business and professional services*. 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.

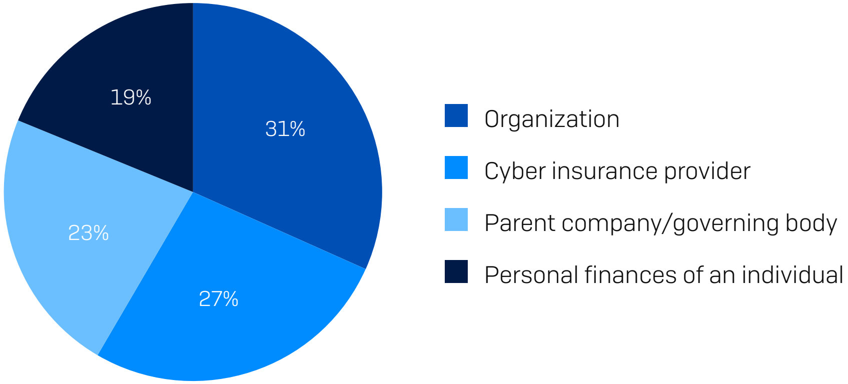
See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

Source of Ransom Funding in Financial Services

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 financial services respondents reporting multiple sources of payment in 97% of cases
- The primary source of ransom funding in financial services organizations is the organization itself, covering almost one-third (32%) of the payment on average; the organization's parent company and/or governing body typically provides 23%.
- Insurance providers are heavily involved in ransom payments, contributing in 96% 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=99.

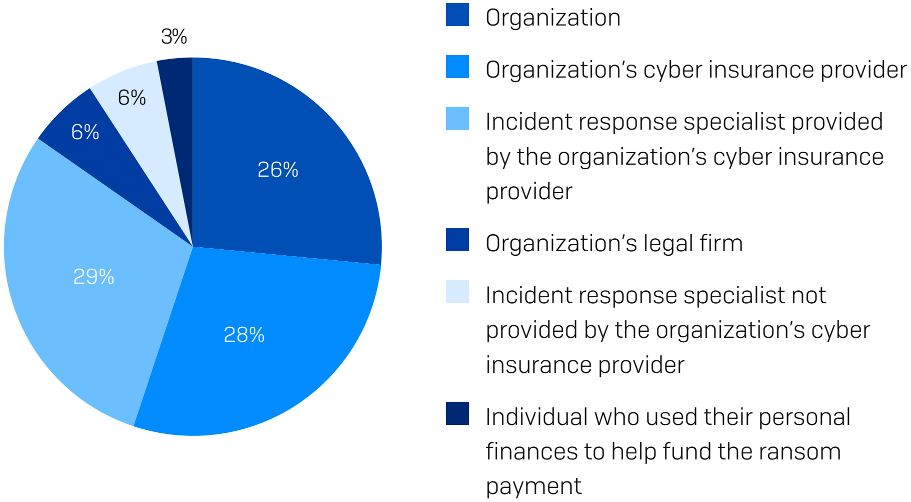
Ransom Transaction Execution

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

In the financial services sector, insurance providers transferred the funds for over half of ransom transactions, either directly (28%) or through their appointed incident response specialist (29%). The victim organization made over one-quarter (26%) of payments, while 6% were executed by the victim's legal firm.

35% of transfers were made by incident response specialists, whether appointed by the insurance provider (29%) 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=99.

Recovery Costs in Financial Services

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, financial services organizations reported a mean cost of $2.58M to recover from a ransomware attack, an increase from the $2.23M reported in 2023. The global cross-sector average recovery costs were $2.73M in 2024 and $1.82M in 2023

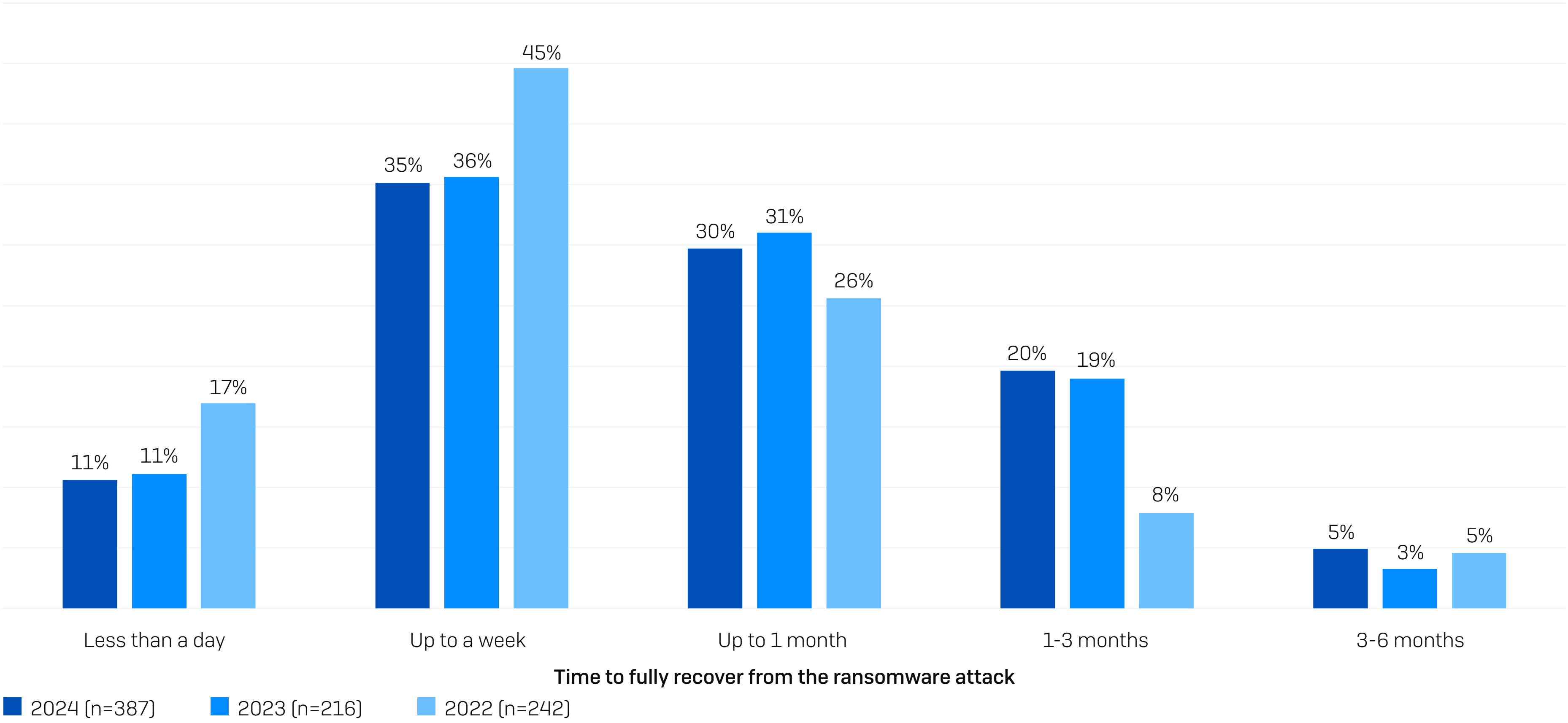
2021	2022	2023	2024
$2.10M	$1.59M	$2.23M	$2.58M

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=387 (2024)/216 (2023)/242 (2022)/185 (2021). N.B. 2022 and 2021 question wording also included "ransom payment"..

Recovery Time in Financial Services

The time taken to recover from a ransomware attack has largely remained steady in financial services. Our 2024 research revealed:

- 46% of ransomware victims were fully recovered in a week or less, in line with the 47% reported in 2023 (although a considerable drop from 62% reported in 2022)
- 25% took more than a month to recover, up slightly from 22% in 2023

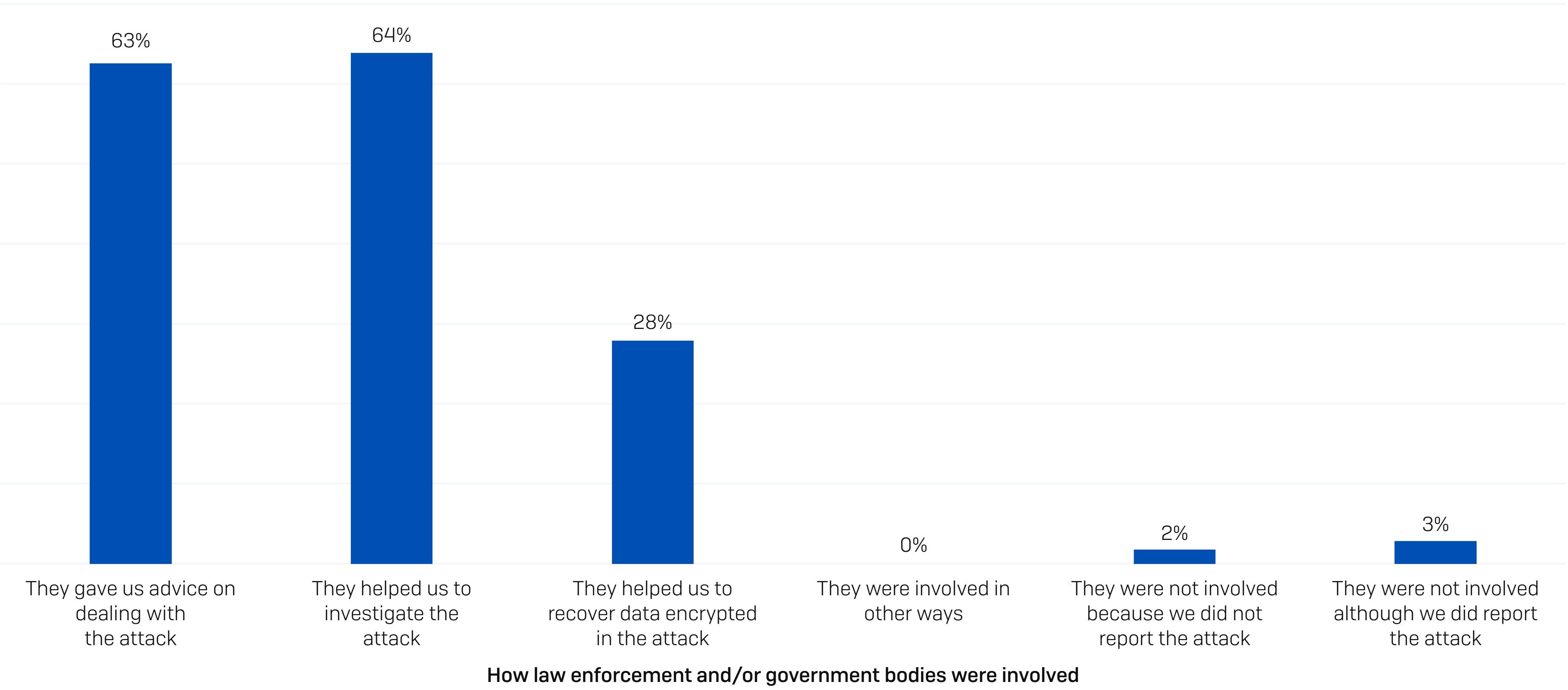


How long did it take your organization to fully recover from the ransomware attack? Base number in chart.

Involvement of Law and Order in Financial Services

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.

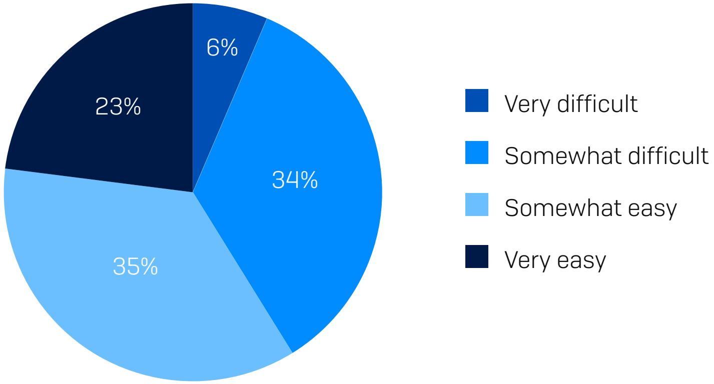
Reflecting the normalization of ransomware, 95% of financial services organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 63% reported that they received advice on dealing with the attack, 64% got help investigating the attack, and 28% 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=387.

Ease of Engagement in Financial Services

58% of those who engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (23% very easy, 35% somewhat easy). 6% said the process was very difficult, while 34% 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=380 (not showing "don't know" responses).

Conclusion

Ransomware remains a major threat to financial services organizations of all sizes around the globe. While the attack rate in financial services is in line with the 2023 figure, the impact of an attack on those who 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. Over a quarter of attacks (27%) start with the exploitation of unpatched vulnerabilities in financial services, 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

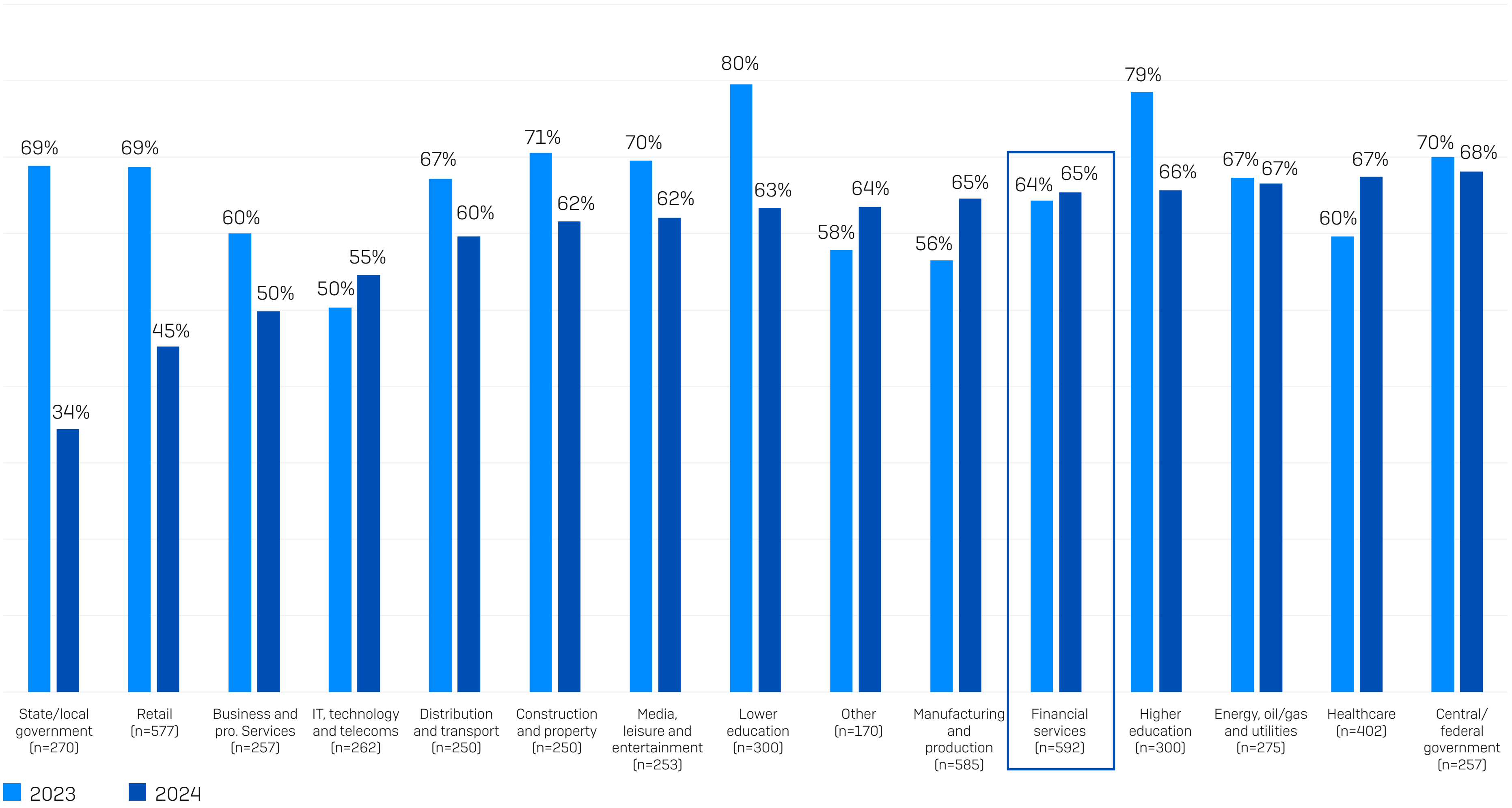
About Vanson Bourne

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

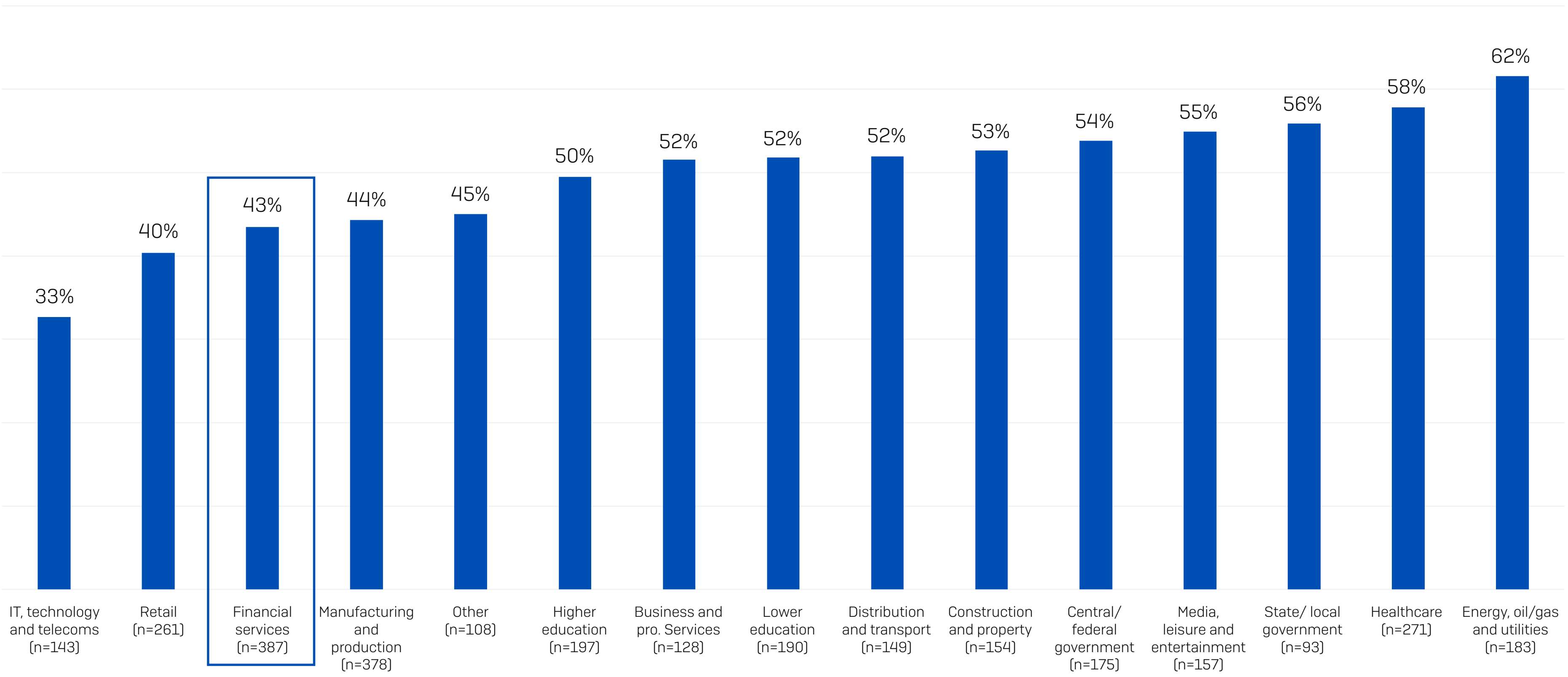
Percentage of organizations hit by ransomware in the last year



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

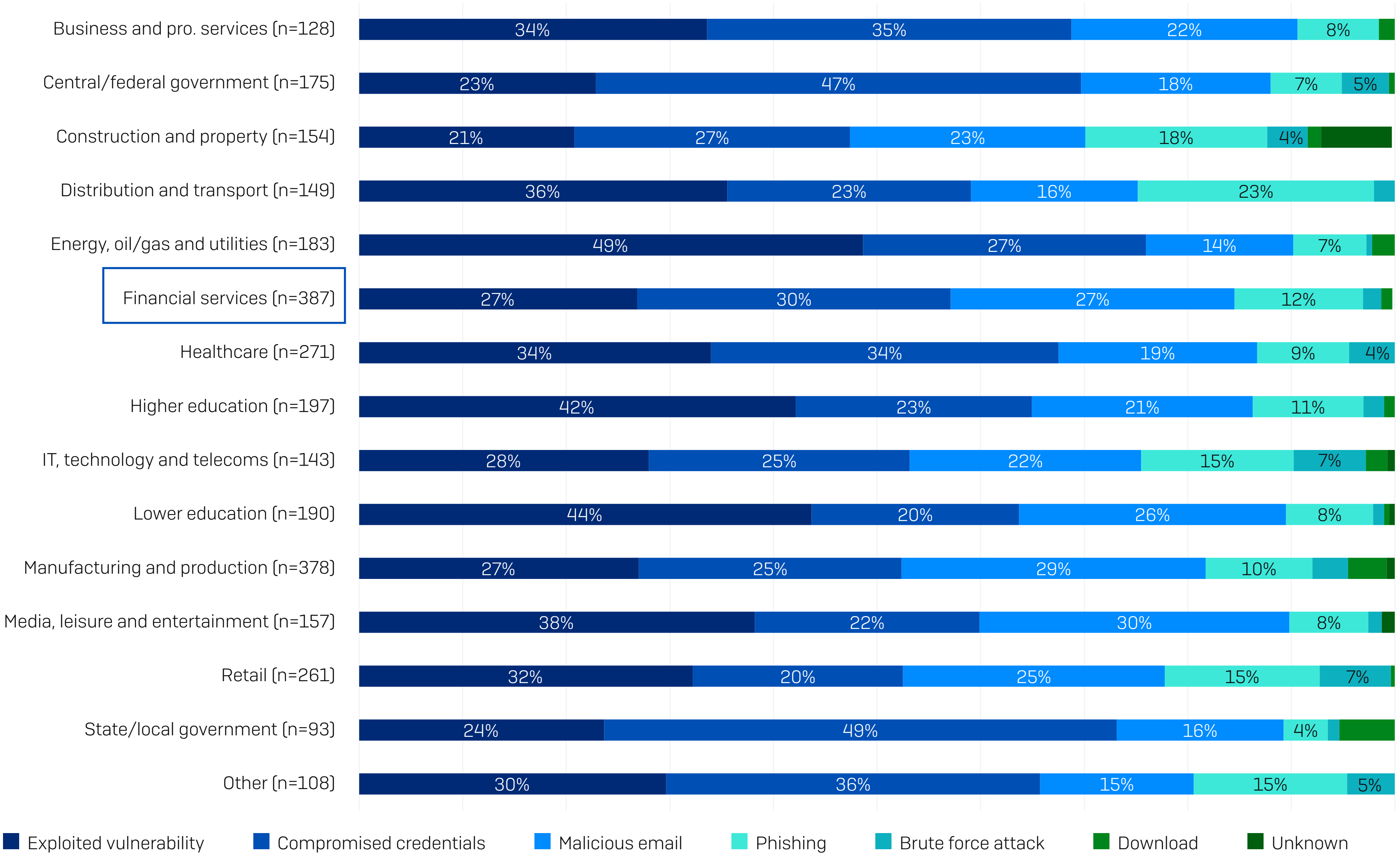
Percentage of Computers Impacted by Industry

Percentage of devices impacted



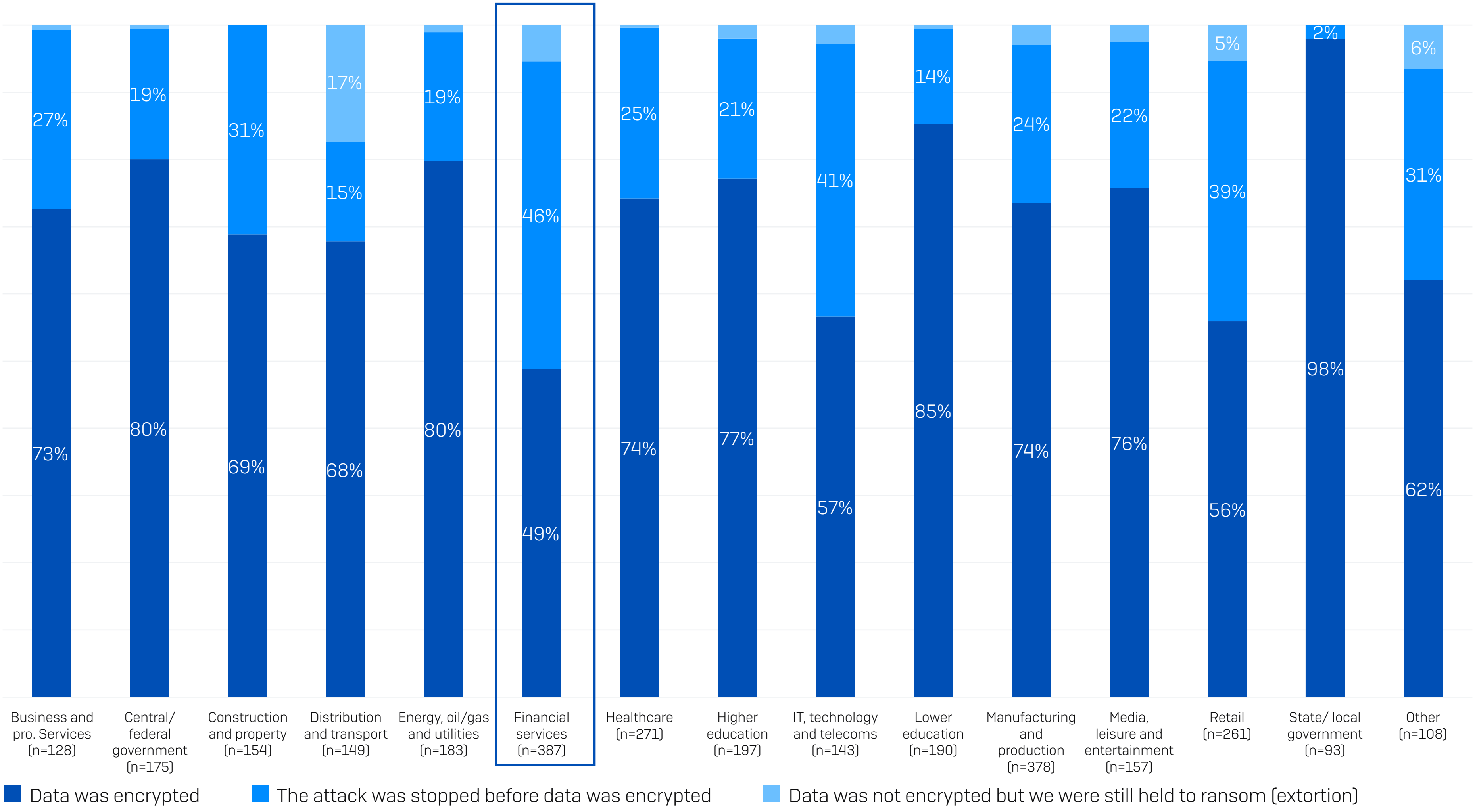
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

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.

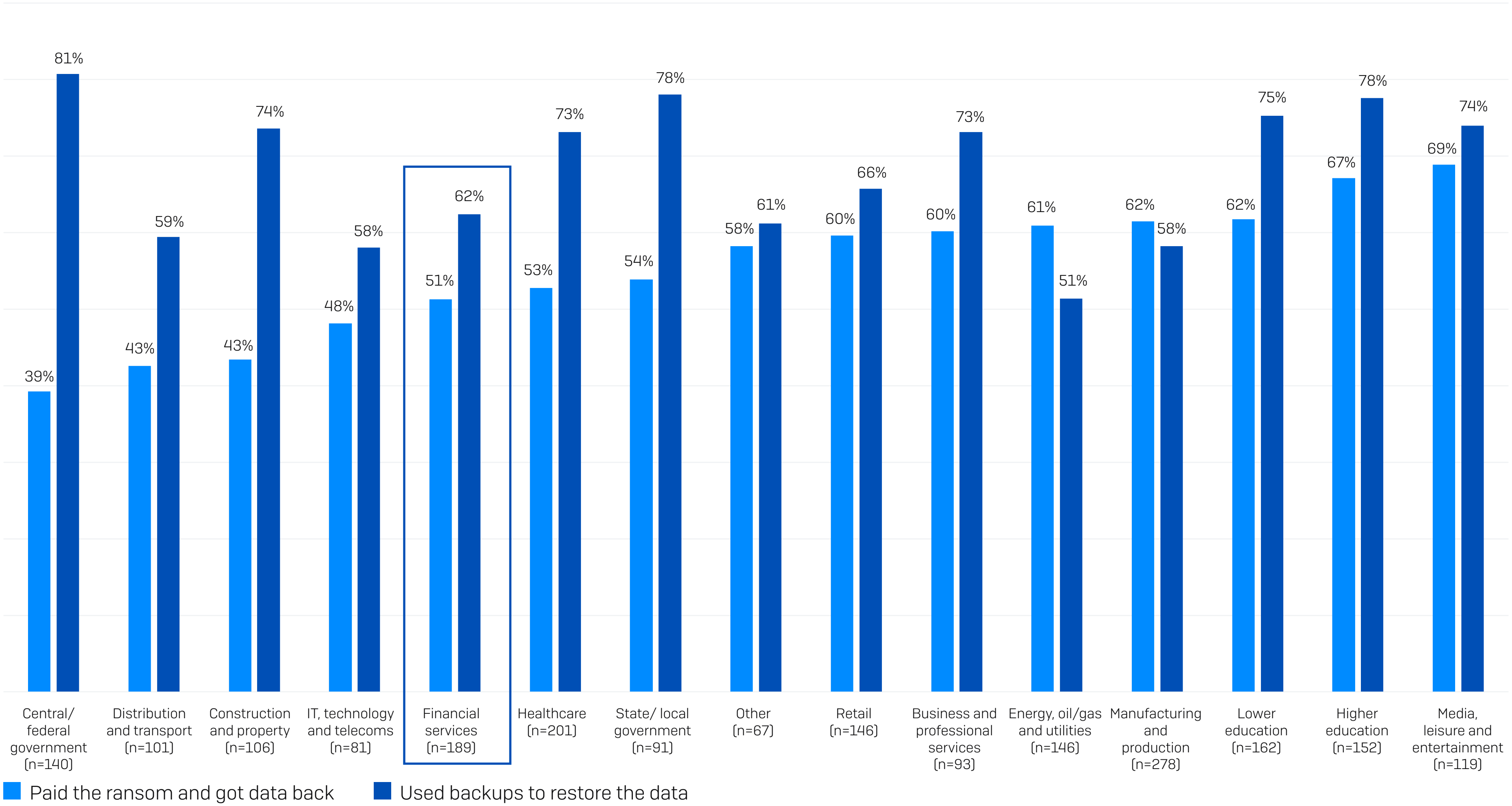
Data Encryption Rate by Industry



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

Data Recovery Method by Industry

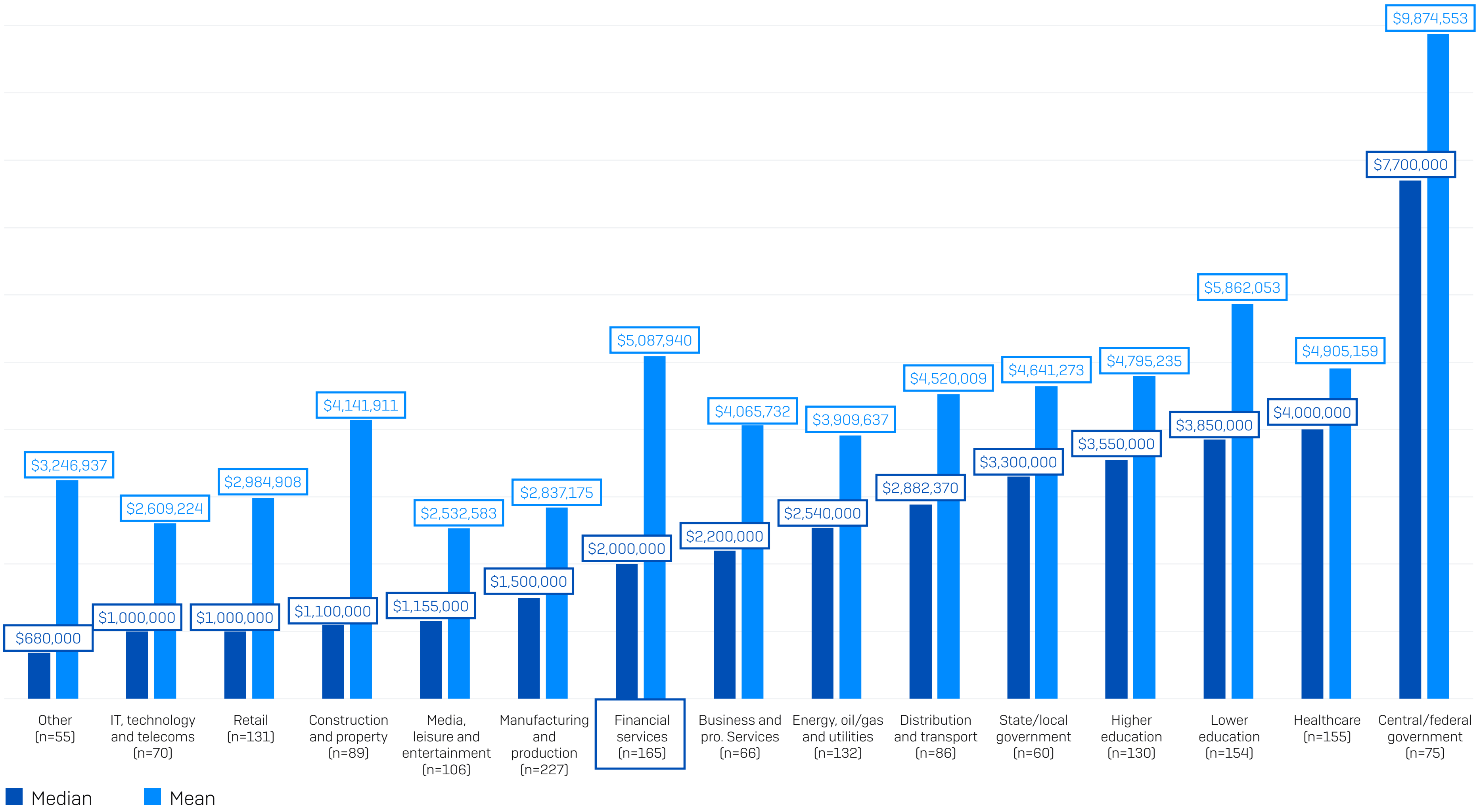
Percentage that got encrypted data back that used the recovery method



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

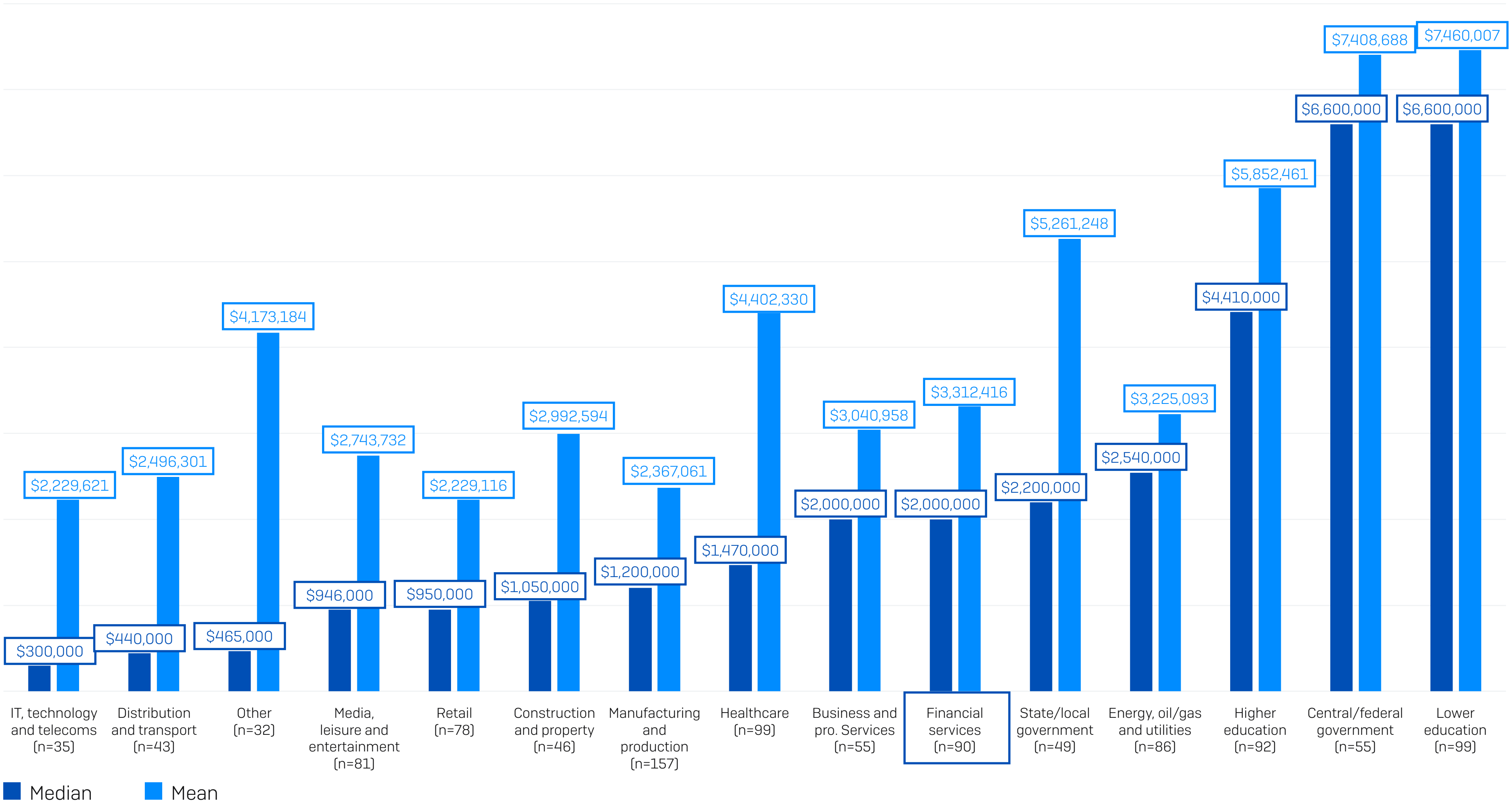
Ransom demand



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

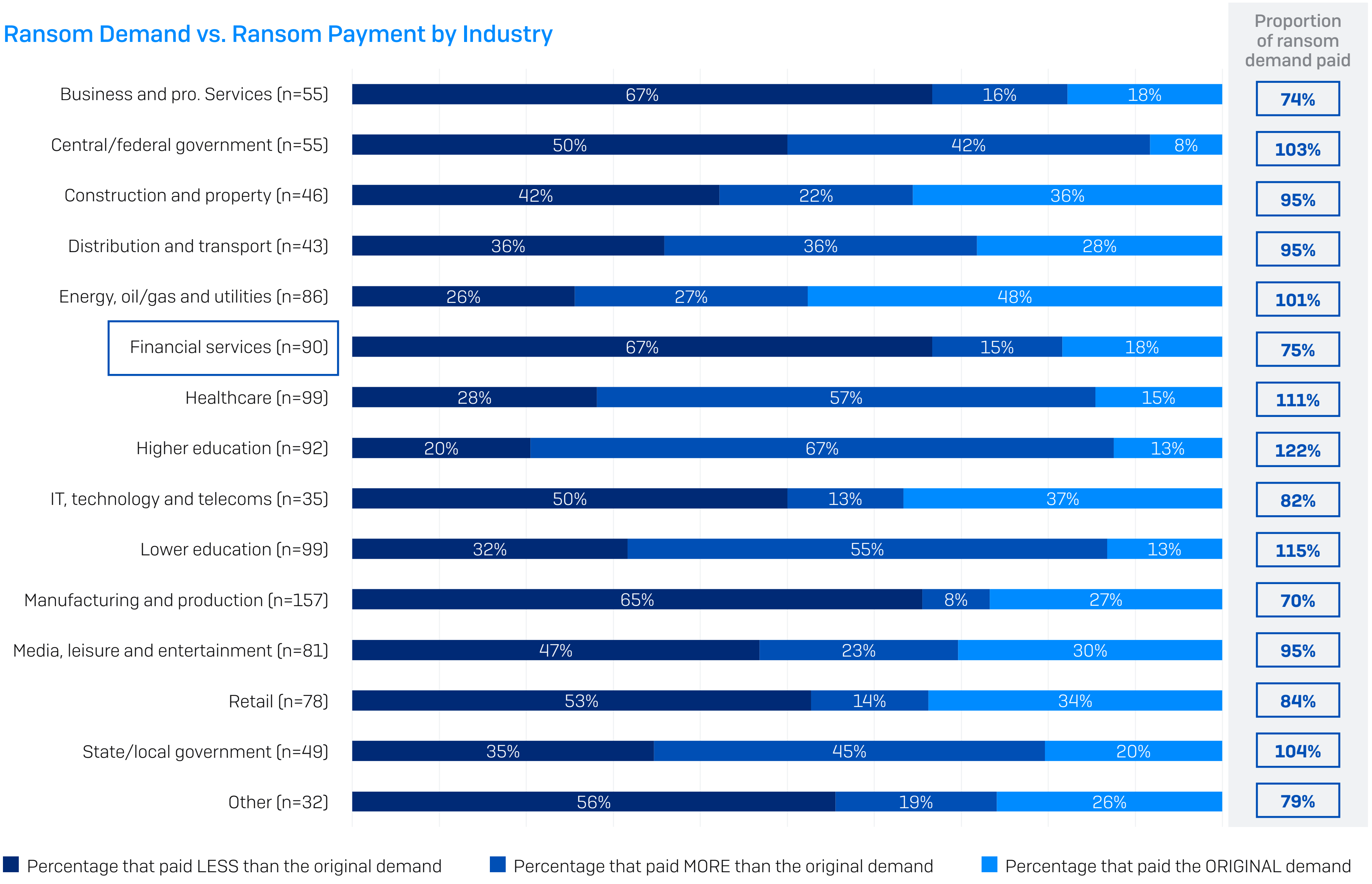
Ransom Payment by Industry

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.

2024-06-21 WP-EN (PC)