

# The State of Ransomware in State and Local Government 2024

Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity across 14 countries, including 270 from the state and local government sector, conducted in January-February 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 state and local government 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 state and local government 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 270 respondents from state and local government 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 State and Local Government

State and local government reported the lowest rate of attacks of all sectors surveyed in 2024. 34% of state and local government organizations were hit by ransomware in 2024, a 51% reduction on the attack rate reported in 2023 and a welcome return to 2021 levels. In contrast, the *central/federal* government sector reported the highest rate of 68%.



In the last year, has your organization been hit by ransomware? Yes. n=270 (2024), n=225 (2023), 199 (2022), 131 (2021), 80 (2020) state and local government organizations.

Across all sectors, 59% of organizations reported being hit by ransomware in our 2024 study, down from 66% in the previous two years.

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

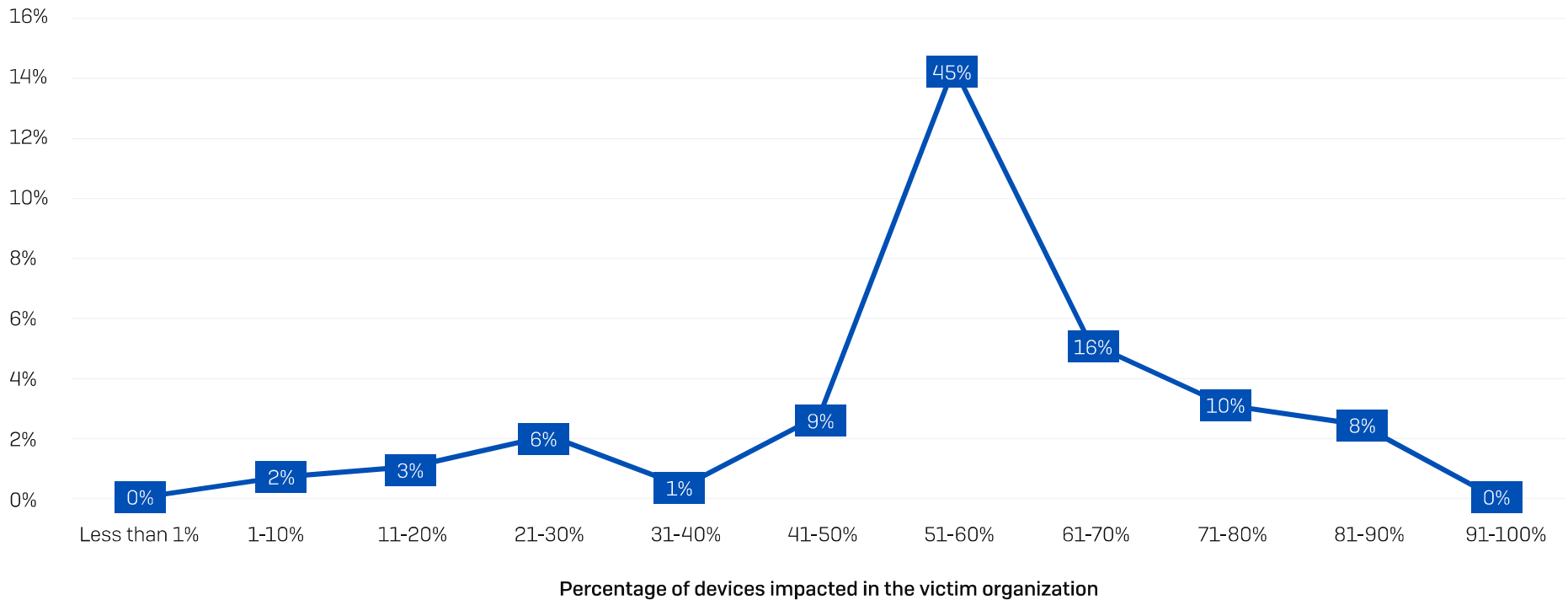
## Percentage of Computers Impacted in State and Local Government

On average, 56% of computers in state and local government organizations are impacted by a ransomware attack, above the cross-sector average of 49%. It is extremely rare for state and local government organizations to have their full environment encrypted: just 8% reported that 81% 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 state and local government organizations saying that 10% or fewer of their devices were affected.

State and local government is one of the sectors reporting the highest percentage of devices impacted in an attack. Only *energy, oil/gas and utilities* (62%) and *healthcare* (58%) reported a higher proportion of devices affected. Both these 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. *IT, technology and telecoms* reported the lowest percentage of devices impacted (33%), followed by *retail* (40%).

*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=93 state and local government organizations hit by ransomware

## Root Causes of Ransomware Attacks in State and Local Government

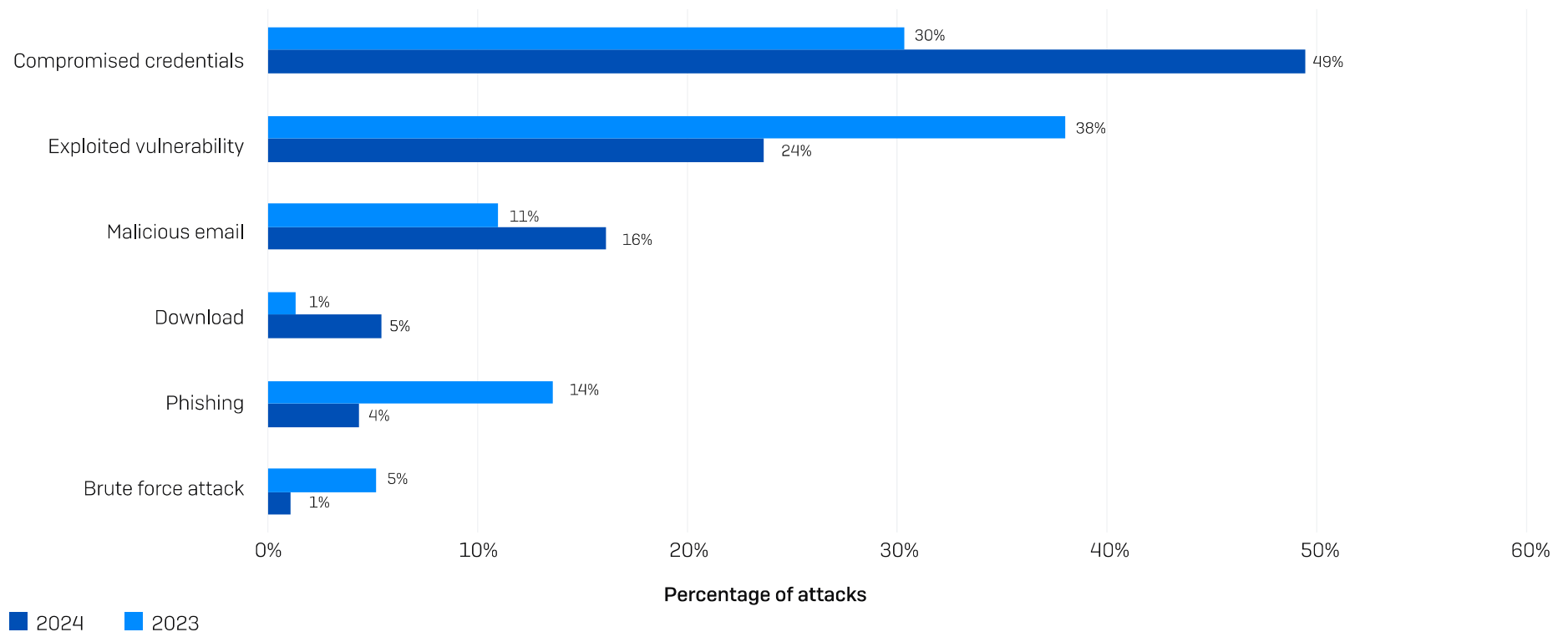
All state and local government respondents hit by ransomware were able to identify the root cause of the attack. Compromised credentials were the most common method of entry (49%), followed by exploited vulnerabilities (24%). For comparison, exploited vulnerabilities were the most common method of compromise in 2023.

The study reveals that the whole government sector is particularly susceptible to attacks that start with abuse of compromised credentials, with 47% of affected central/federal government organizations having experienced attacks starting in this way.

In contrast, across all sectors, exploited vulnerabilities were the most common root cause of attacks (32%), followed by compromised credentials (29%).

Energy, oil/gas and utilities is the sector most likely to fall victim to the exploitation of unpatched vulnerabilities (49%). 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 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=93 (2024)/155 (2023) state and local government organizations hit by ransomware.

## Backup Compromise in State and Local Government

Almost all [99%] state and local government organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack, higher than the global average of 94%.

Of the compromise attempts, just over half [51%] were successful. This is one of the lowest rates of successful backup compromises across all industries, with only *IT, technology, and telecoms* [30%], *retail* [47%], and *financial services* [48%] reporting lower rates. Backup compromise attempts on *energy, oil/gas and utilities* are most likely to be successful [79%].

State and local government organizations that had their backups compromised reported considerably worse outcomes than those whose backups were not breached:

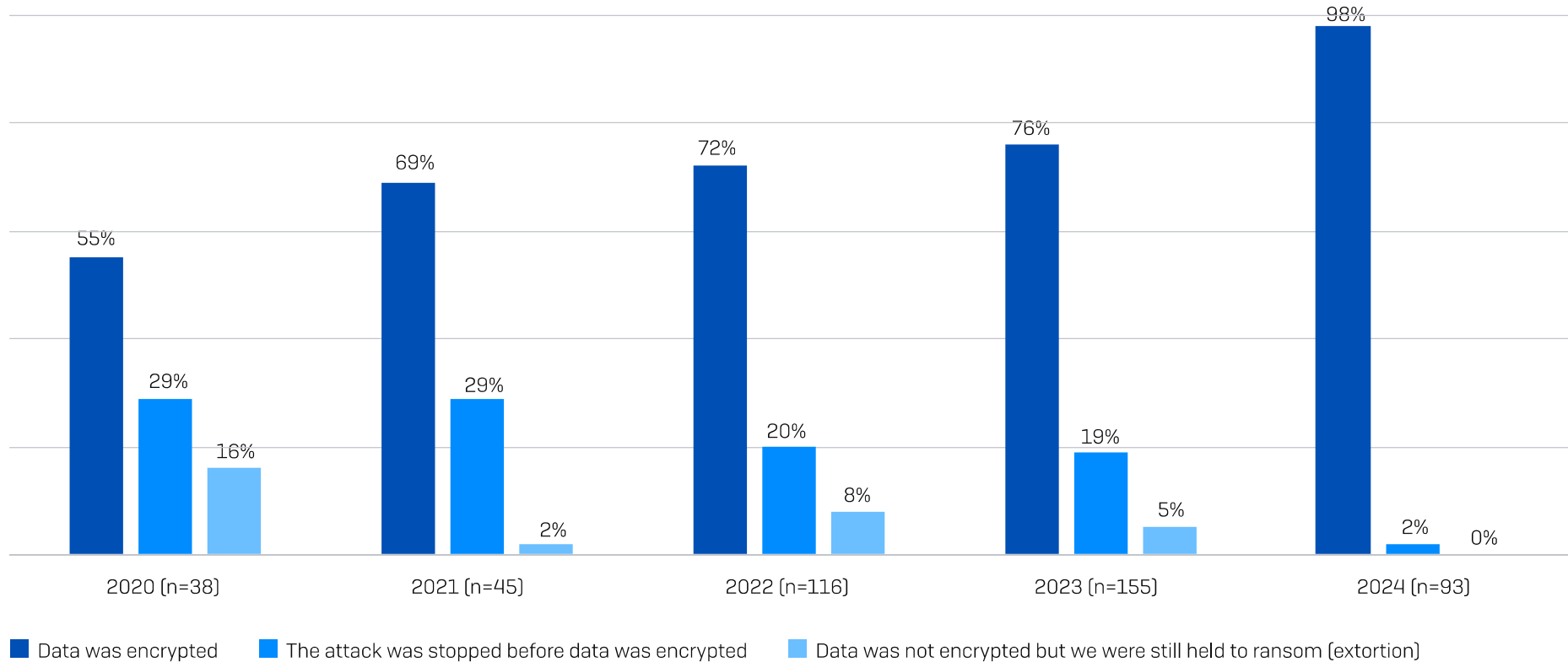
- Organizations whose backups were compromised were more likely to pay the ransom to recover encrypted data [83% vs. 23%]
- Median overall recovery costs were four times greater than when backups were not compromised [\$3M vs. \$750K]

## Rate of Data Encryption in State and Local Government

98% of ransomware attacks on state and local government organizations resulted in data encryption, a considerable increase from the 76% encryption rate reported in 2023. The 2024 cross-sector average is 70%. This is the highest rate of data encryption of all sectors studied.

Only 2% of attacks were stopped before data was encrypted, compared to 19% in our 2023 study. No respondent reported an extortion-only attack, where the data is not encrypted but organizations are held to ransom anyway.

*See the appendix for a detailed breakdown of the percentage of computers impacted 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. 42% of state and local government organizations reported that where data was encrypted, data was also stolen – a slight decrease from the 48% reported by the sector last year, but still a significant number. 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.

**42%**

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, and the data was also stolen [n=91]



## Data Recovery

All state and local government organizations that had data encrypted got their data back. 78% restored encrypted data using backups, the second highest rate of backup use reported (tied with *higher education*).

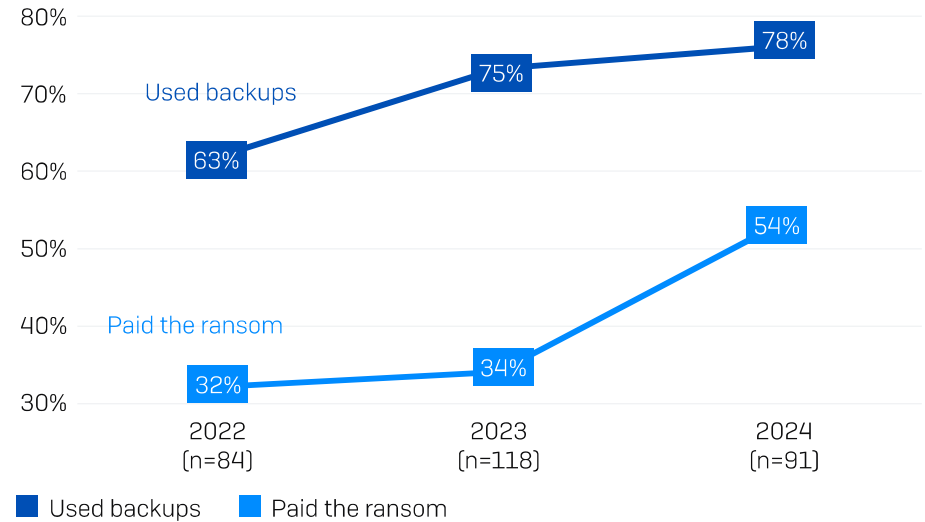
54% paid the ransom to get data back, and 18% used other means – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.

In comparison, globally, 68% of those that had data encrypted used backups to recover their files while 56% paid 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 (n=91)

The three-year view of state and local government organizations reveals a steady rise in both the use of backups and the sector's propensity to pay the ransom



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, 44% of state and local government organizations that had data encrypted reported using more than one method, four times the rate reported in 2023 (11%).

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

## Ransom Demands

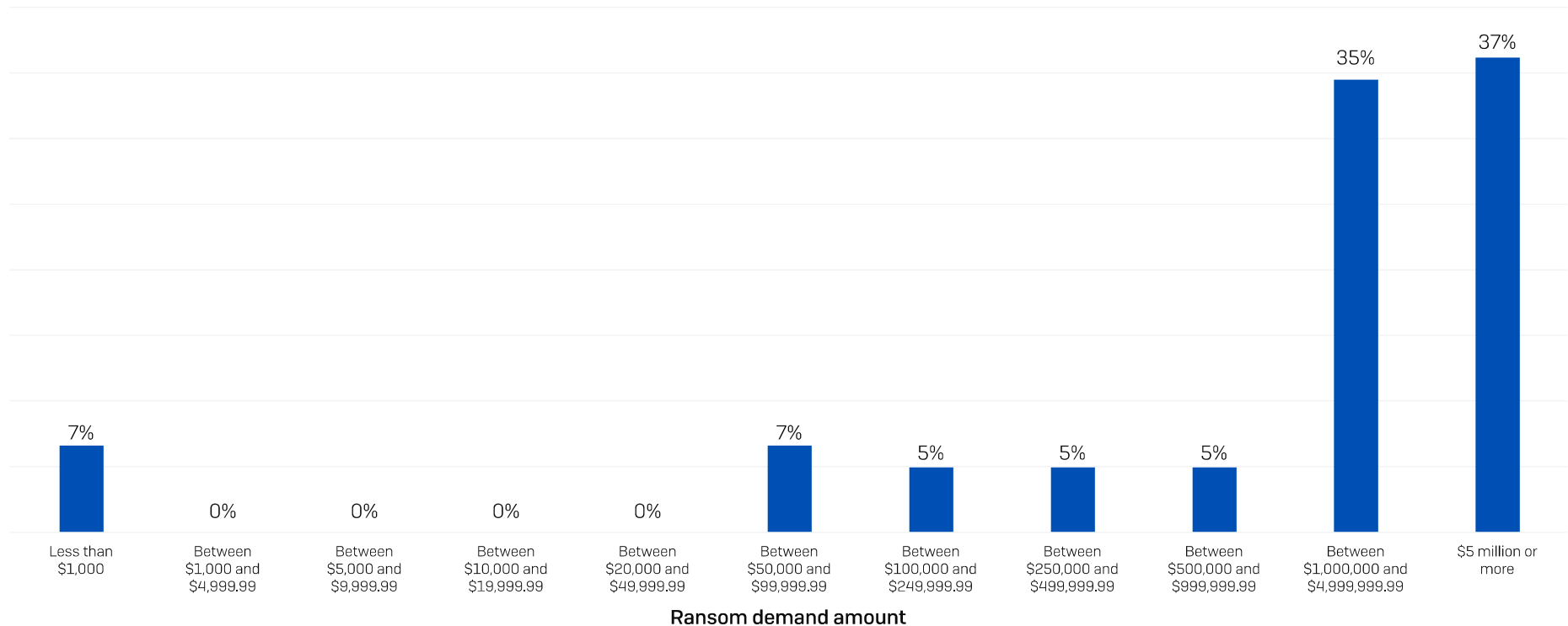
For the first time this year, we included both ransom demands and payments in this report. Across the 60 state and local government organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was \$3.3M (median) and \$4.6M (mean).

One of the most notable findings in this year's study is that close to three-quarters (72%) of ransom demands made to state and local government organizations are for \$1M or more, with 37% of demands for \$5M or more.

High ransom demands were common across all industries with all named sectors (excluding "other") reporting median 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 [\$9.9M] 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=60

## Ransom Payments

49 state and local government respondents whose organizations paid the ransom shared the actual sum paid:

- Median payment: \$2.2M
- Mean payment: \$5.3M

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.

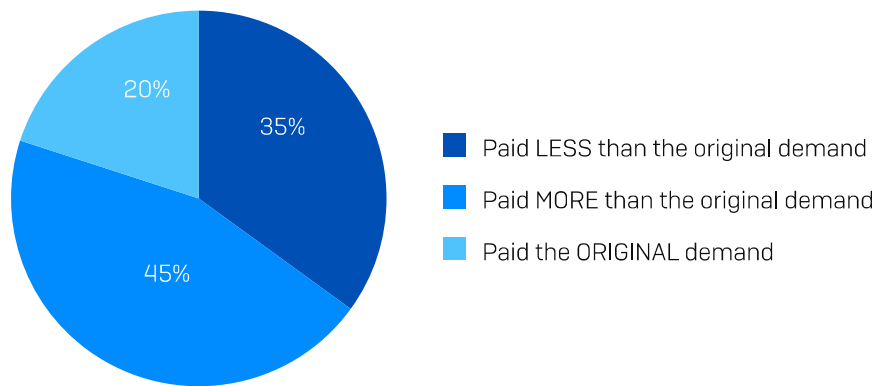
*See the appendix for a detailed breakdown of average ransom payment by industry.*

## Propensity to Negotiate Ransom Amounts in State and Local Government

State and local government victims rarely pay the initial sum demanded by the attackers. The study revealed that only 20% paid the initial ransom demand, 35% paid less than the original demand, while 45% paid more.

On average, across all state and local government respondents, organizations paid 104% 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=49

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 the original demand and the eventual payment don't always line up.

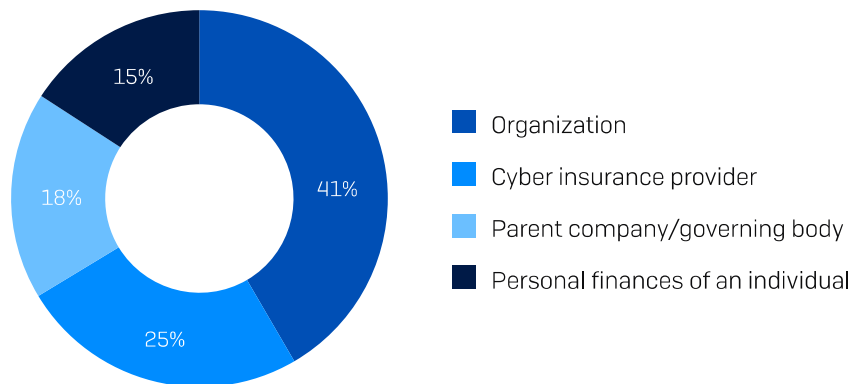
*See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.*

## Source of Ransom Funding in State and Local Government

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 state and local government respondents reporting multiple sources of payment in 82% of cases.
- ▶ The primary source of ransom funding in state and local government organizations is the organization itself, covering 41% 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 84% of cases. 25% 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=49

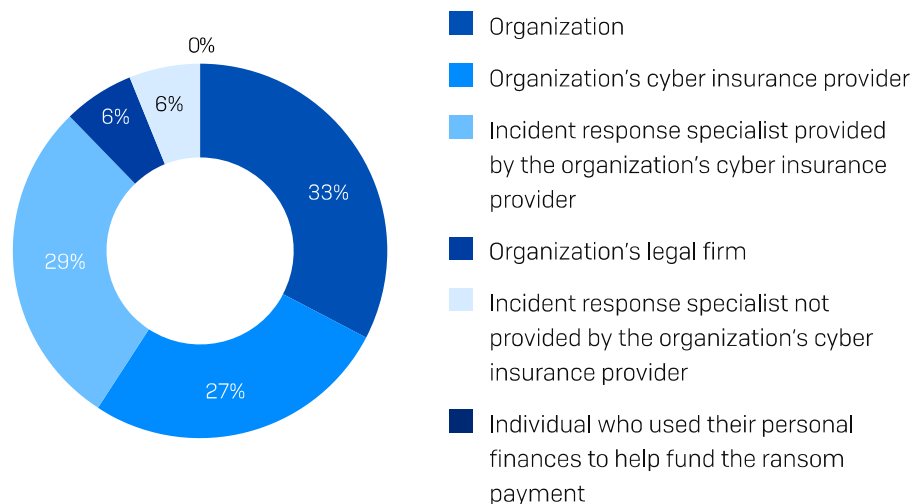
## Ransom Transaction Execution

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

In the state and local government sector, insurance providers transferred the funds for over half of ransom transactions, either directly [27%] or through their appointed incident response specialist [29%]. The victim organization made around one-third [33%] 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=49.

## Recovery Costs in State and Local Government

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, state and local government organizations reported a mean cost of \$2.83M to recover from a ransomware attack, more than double the \$1.21M reported in 2023. The global cross-sector average recovery costs came in at \$2.73M in 2024 and \$1.82M in 2023.

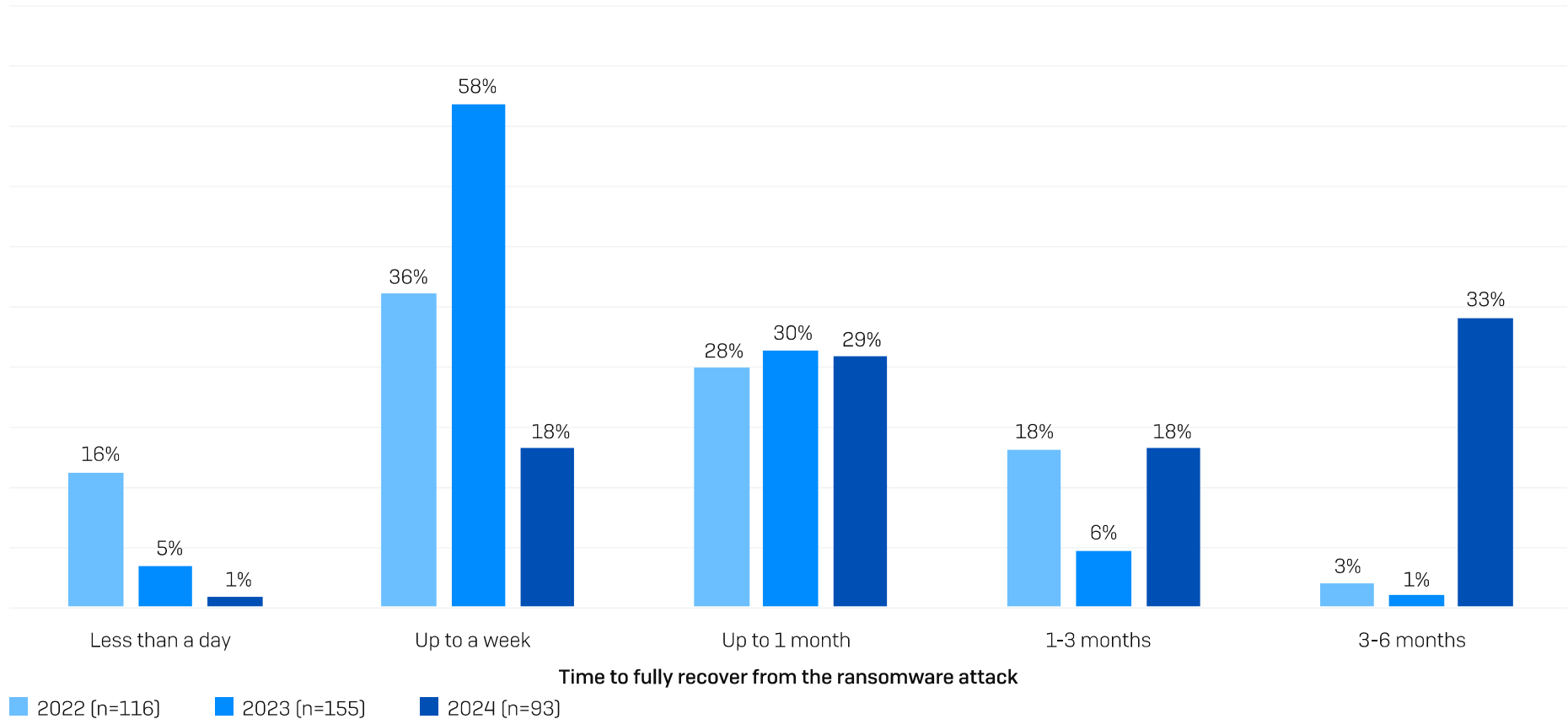


What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=93 (2024)/155 (2023)/ 116 (2022)/ 45 (2021)/ 38 (2020). N.B. 2022, 2021, and 2020 question wording also included "ransom payment".

## Recovery Time in State and Local Government

Over the last year, the time taken to recover from a ransomware attack has sharply increased in state and local government. Our 2024 research revealed:

- 19% of ransomware victims were fully recovered in a week or less, a considerable decrease from the 63% reported in 2023
- More than half (51%) of the victims took more than a month to recover, considerably higher than the 7% reported in 2023

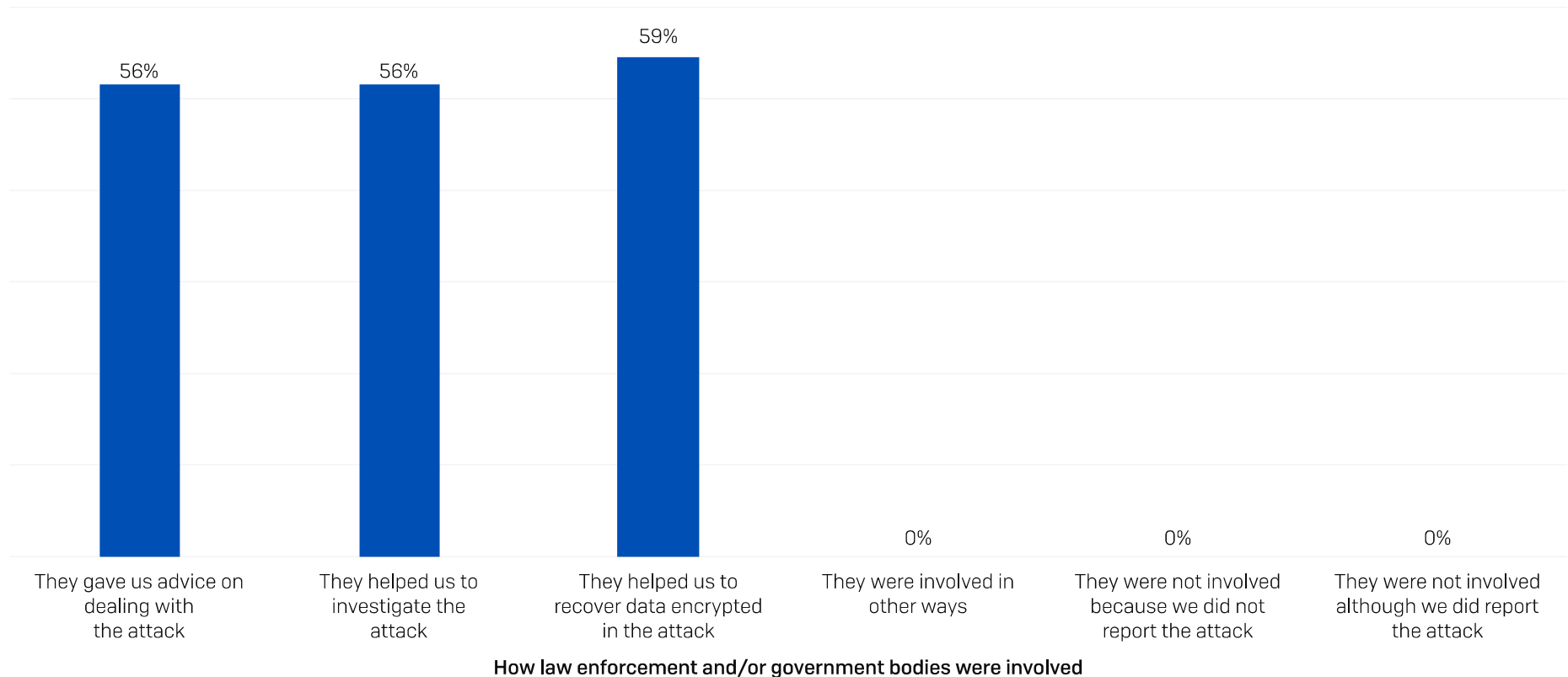


How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

## Involvement of Law and Order in State and Local Government

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 and likely high levels of mandatory reporting, all state and local government organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 56% reported that they received advice on dealing with the attack, 56% got help investigating the attack, and 59% said they received help recovering data encrypted in the attack – the highest rate across all sectors.

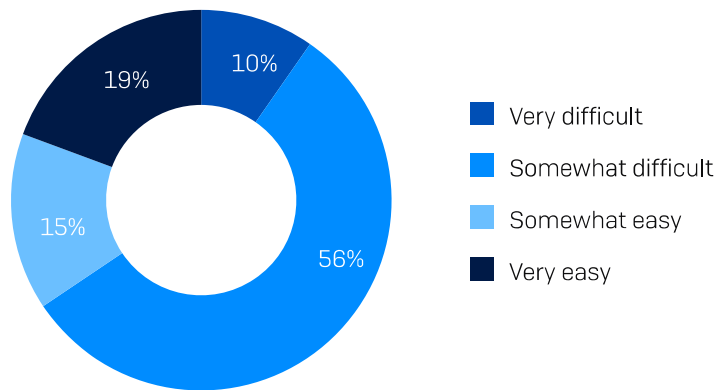


If your organization reported the attack to law enforcement and/or an official government body, how did they get involved? n=93.



## Ease of Engagement in State and Local Government

Almost two-thirds [66%] found it difficult to engage with law enforcement and/or official bodies in relation to the attack, with 56% finding it somewhat difficult and 10% saying it was very difficult. In contrast, 34% said the process was easy (19% very easy, 15% somewhat easy). With reporting mandatory for the sector in many jurisdictions, these findings are concerning.



How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=93 (not showing "don't know" responses).

## Conclusion

Ransomware remains a major threat to state and local government organizations of all sizes around the globe. While the percentage of organizations hit by ransomware has dropped significantly over the last year, the sector reported the highest data encryption rates across all sectors. 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. Almost a quarter (24%) of respondents say that attacks start with the exploitation of unpatched vulnerabilities in state and local government, 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](http://www.sophos.com).

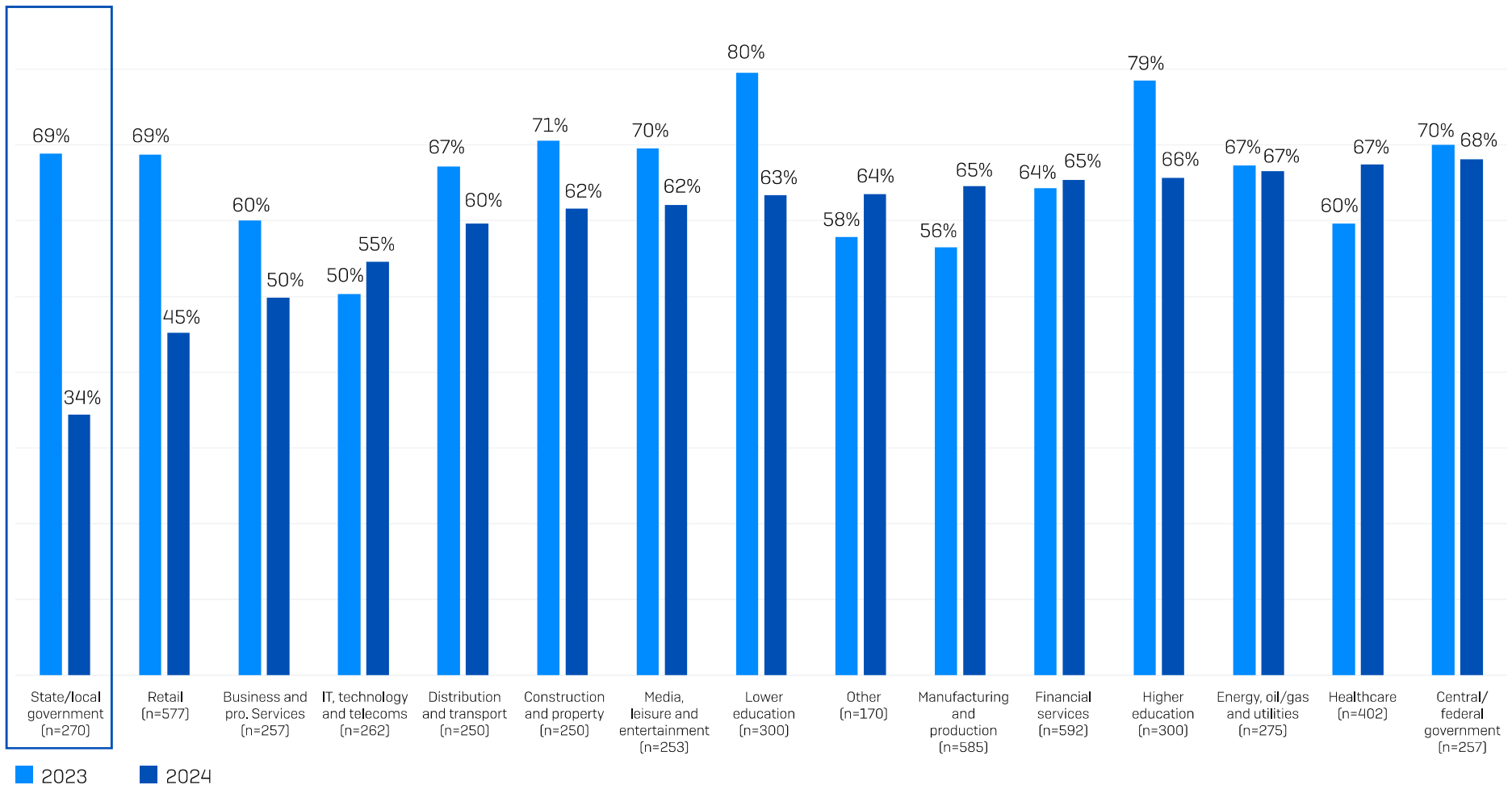
## About Vanson Bourne

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](http://www.vansonbourne.com)

# Appendix

## Rate of Ransomware Attacks by Industry

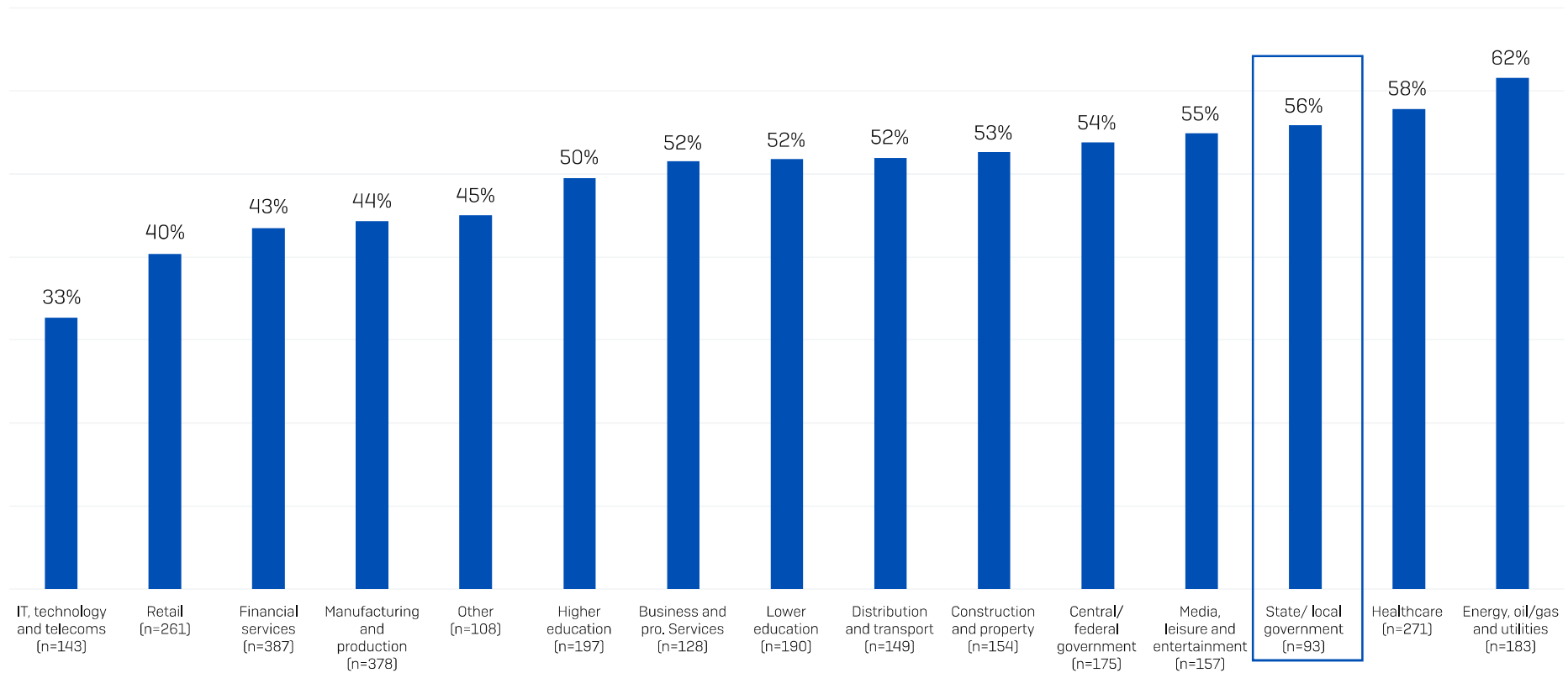
Percentage of organizations hit by ransomware in the last year



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.

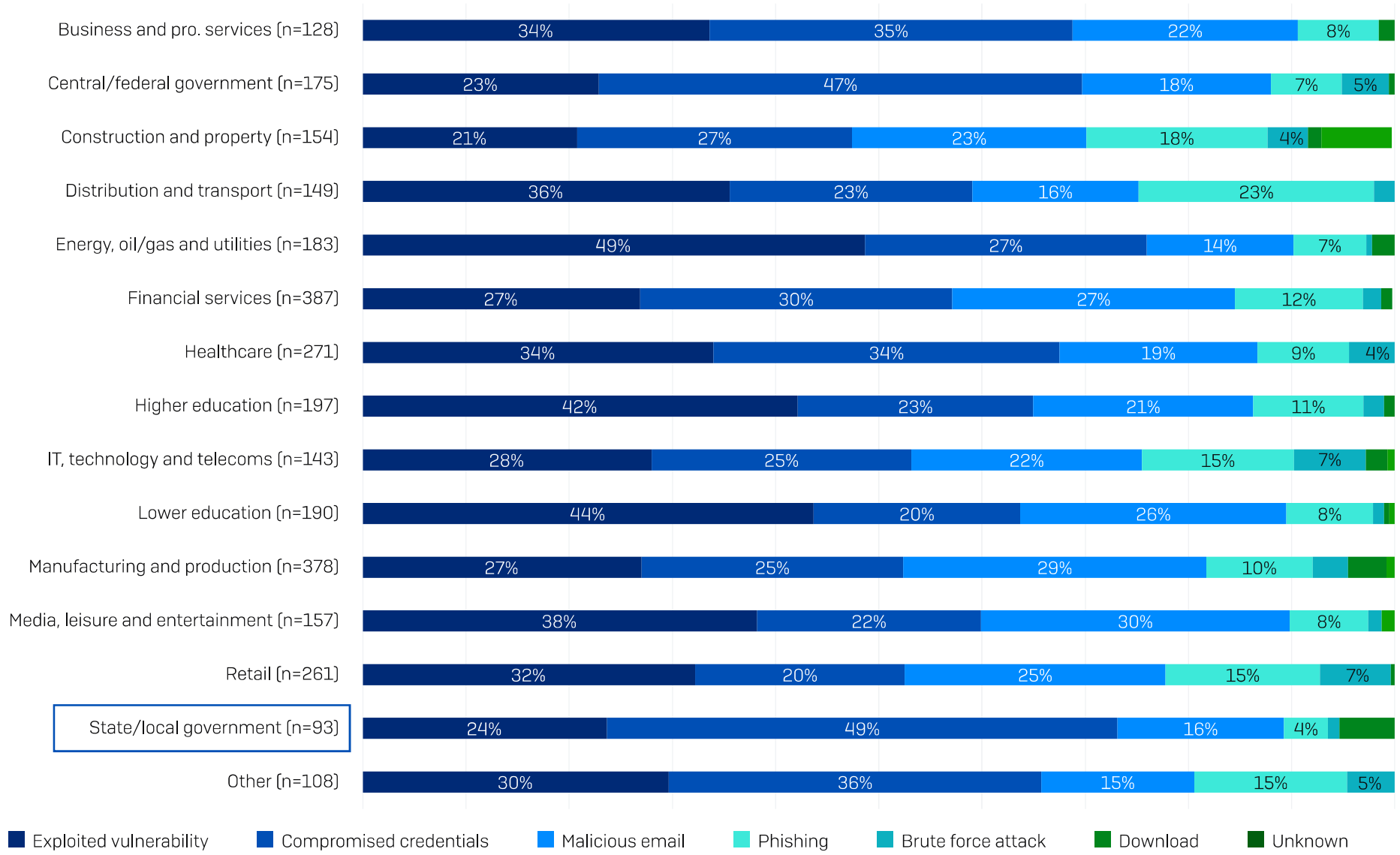
## Percentage of Computers Impacted by Industry

Percentage of devices impacted



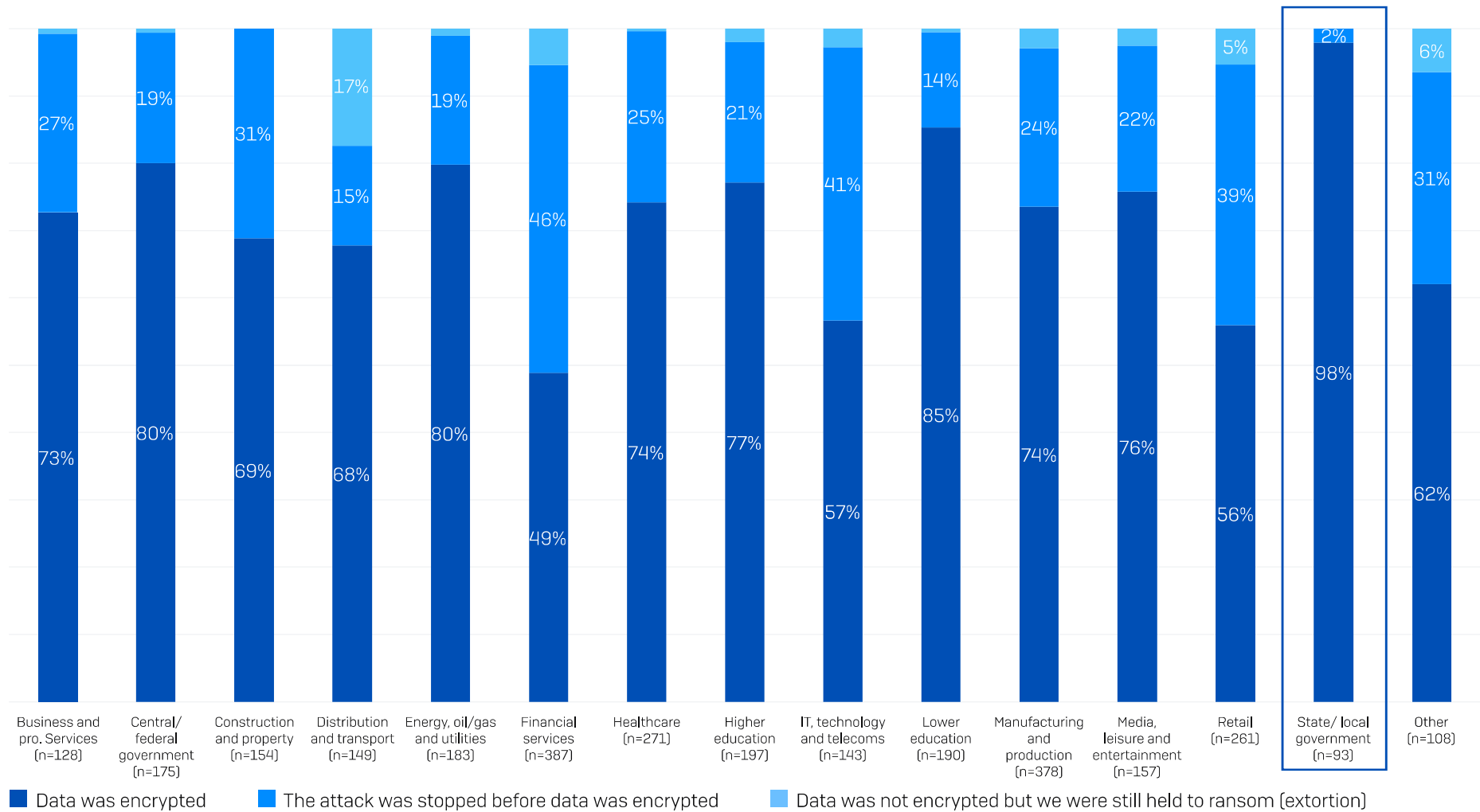
What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

### 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.

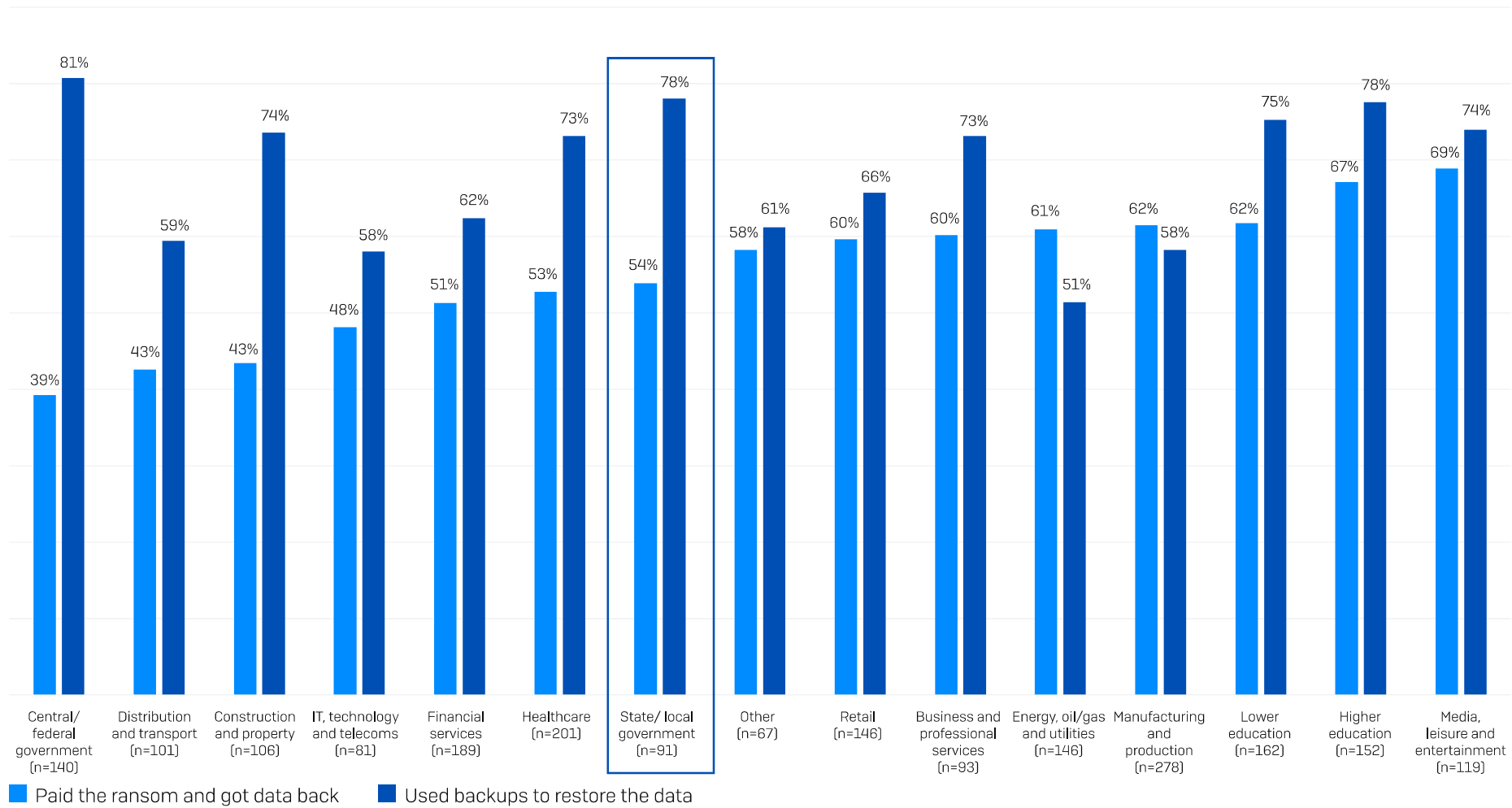
### Data Encryption Rate by Industry



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

## Data Recovery Method by Industry

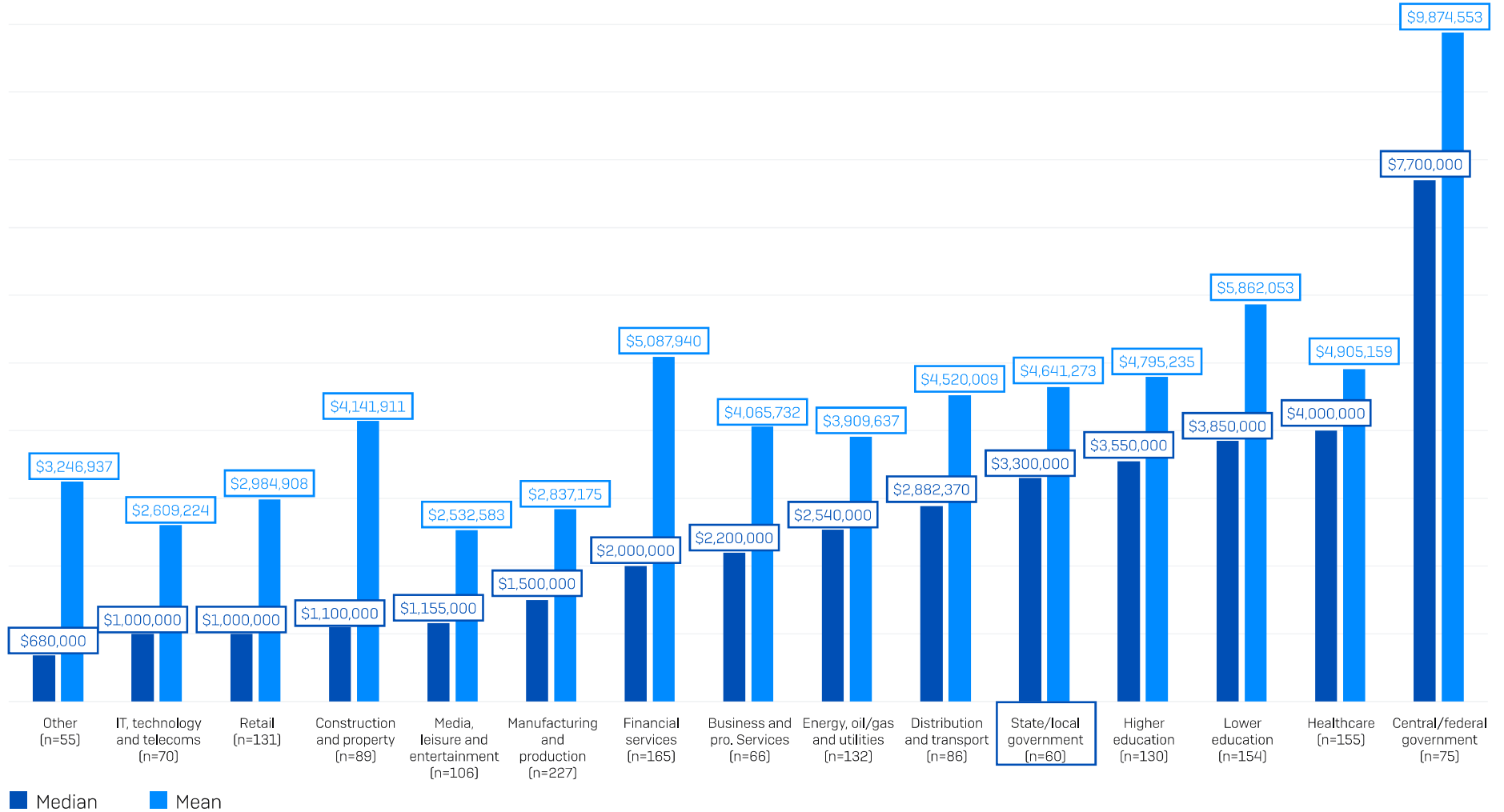
Percentage that got encrypted data back that used the recovery method



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

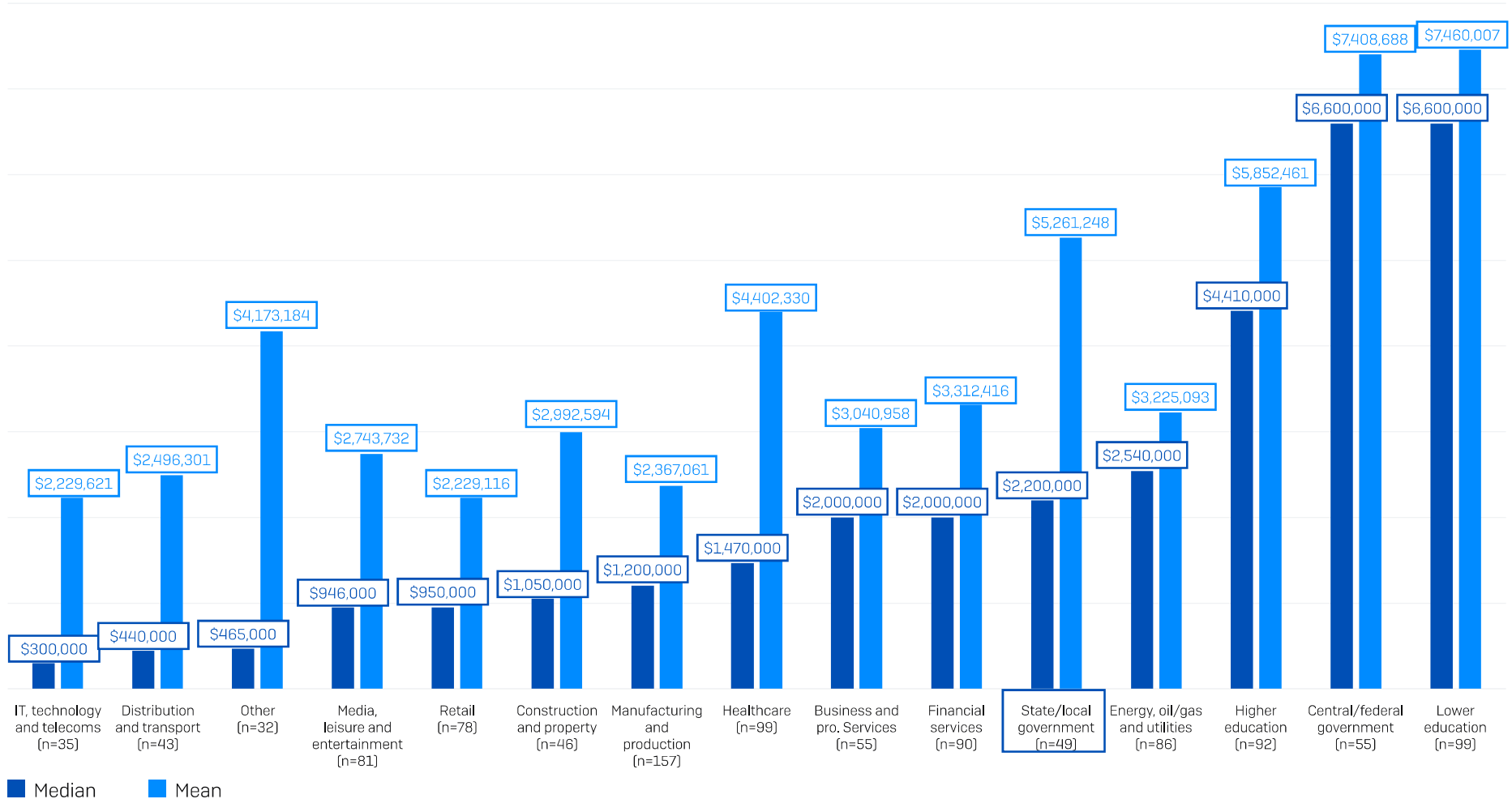


How much was the ransom demand from the attacker(s)? Base numbers in chart. Ordered by median demand.



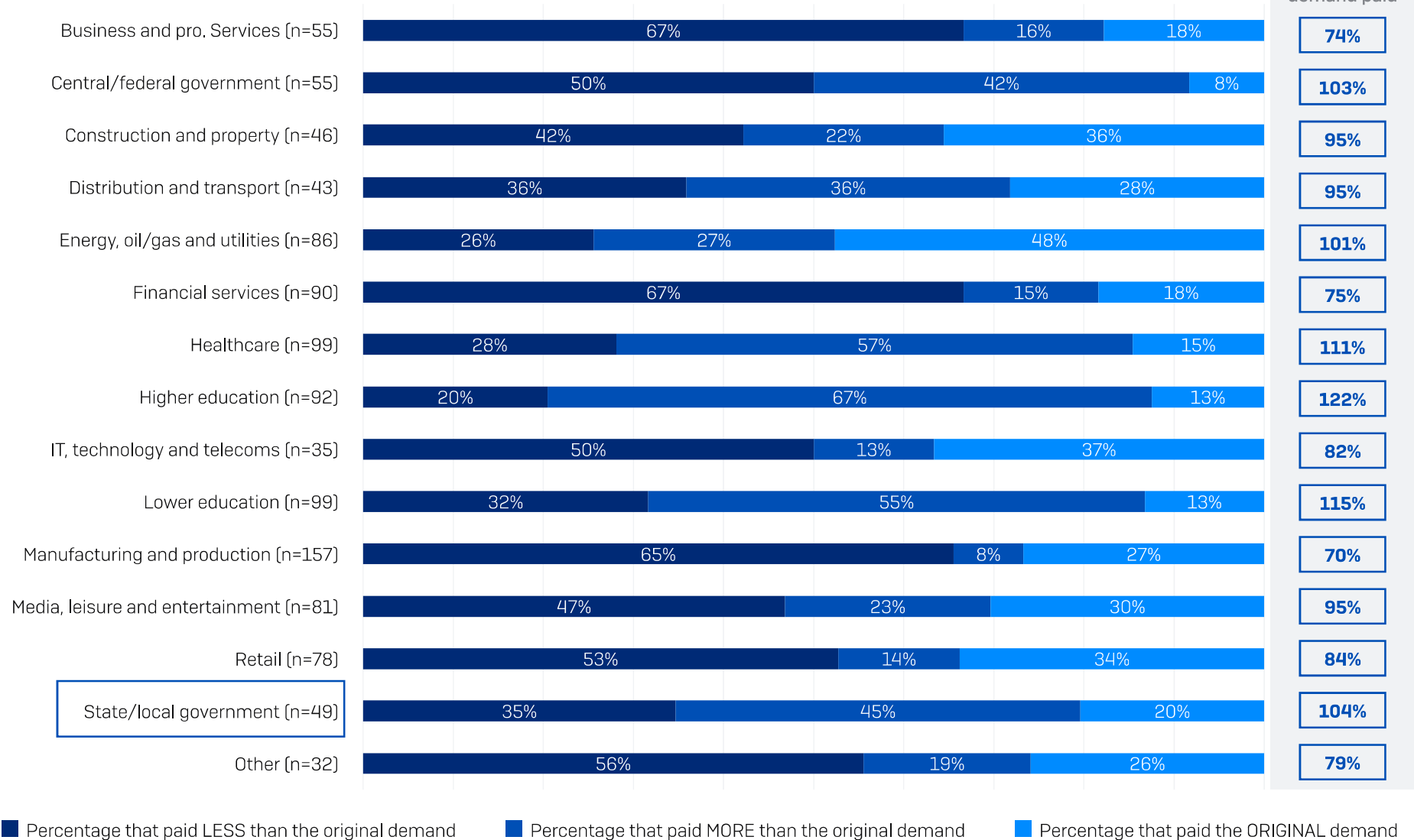
## Ransom Payment by Industry

### 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.

© 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.

2024-08-08 WP-EN (NP)

**Secure Content Technologies**  
info@securecontenttechnologies.com  
www.securecontenttechnologies.com | (513) 779-1165

The SOPHOS logo consists of the word 'SOPHOS' in a bold, blue, sans-serif font.