SOPHOS

# The State of Ransomware in Critical Infrastructure 2024

**Findings from an independent, vendor-agnostic survey of 5,000 leaders responsible for IT/cybersecurity, including 275 from the energy, oil/gas and utilities sector, across 14 countries, conducted in January-February 2024.**

*A Sophos Whitepaper. July 2024*

# Introduction

Sophos' annual study of the real-world ransomware experiences of organizations around the globe explores the full victim journey, from root cause to severity of attack, financial impact, and recovery time. This report focuses on the ransomware experiences of the energy, oil/gas and utilities sector, a core element of the critical infrastructure supporting businesses around the globe.

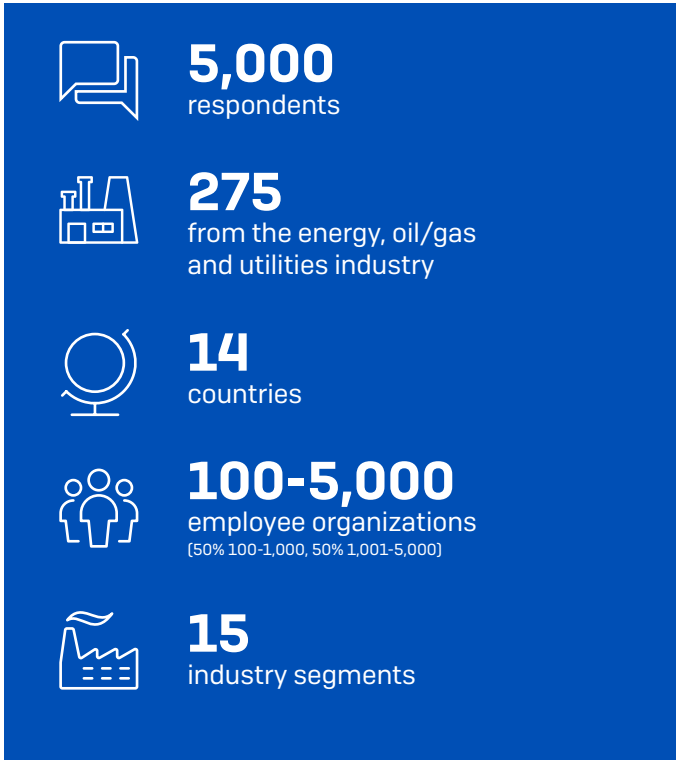
The report combines fresh new insights, including an exploration of the role of law enforcement in ransomware remediation, with year-on-year trends leveraging learnings from our previous studies. It reveals the realities facing energy, oil/gas and utilities providers today and how the impact of ransomware has evolved over the last five years.

## 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. This included 275 respondents from the energy, oil/gas and utilities 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 Critical Infrastructure

67% of energy, oil/gas and utilities organizations were hit by ransomware in the last year, level with the rate in 2023. In contrast, the global cross-sector attack rate declined slightly, with 59% experiencing an attack, down from 66% in the previous two years.


In the last year, has your organization been hit by ransomware?
Yes. n=275 (2024), n=150 (2023), 357 (2022), 197 (2021), 204 (2020)

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

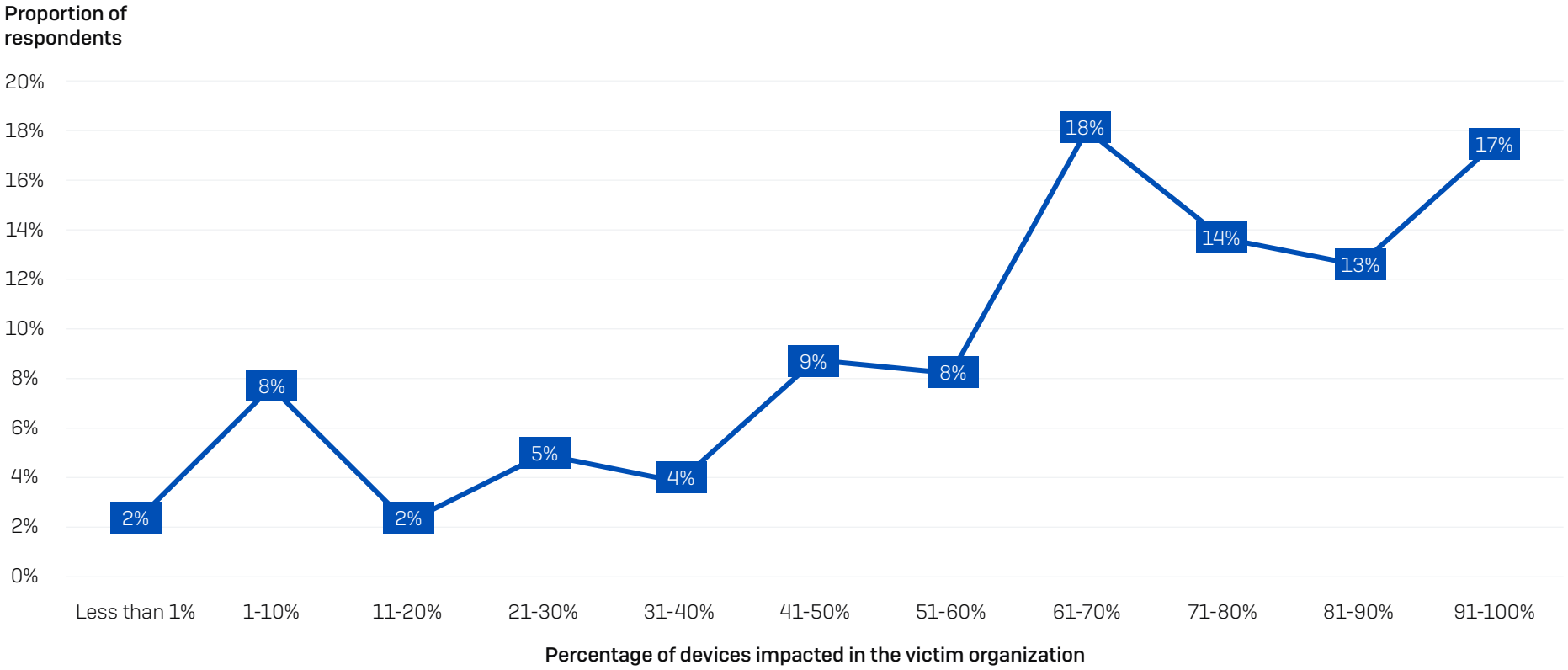
# Percentage of Computers Impacted in Critical Infrastructure

On average, 62% of computers in energy, oil/gas and utilities are impacted by a ransomware attack, considerably above the cross-sector average of 49%. Unlike other sectors where only a small percentage of organizations have their full environment encrypted, approximately one in five energy, oil/gas and utilities organizations (17%) 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 is highly unusual, with only 2% of affected organizations saying that fewer than 1% of their devices were affected.

Energy, oil/gas and utilities is the sector with the highest percentage of devices impacted by an attack, 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. *IT, technology and telecoms* reported the smallest percentage of devices impacted (33%), reflecting the strong cyber posture that is often seen in this sector.

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=183 energy, oil/gas and utilities organizations hit by ransomware

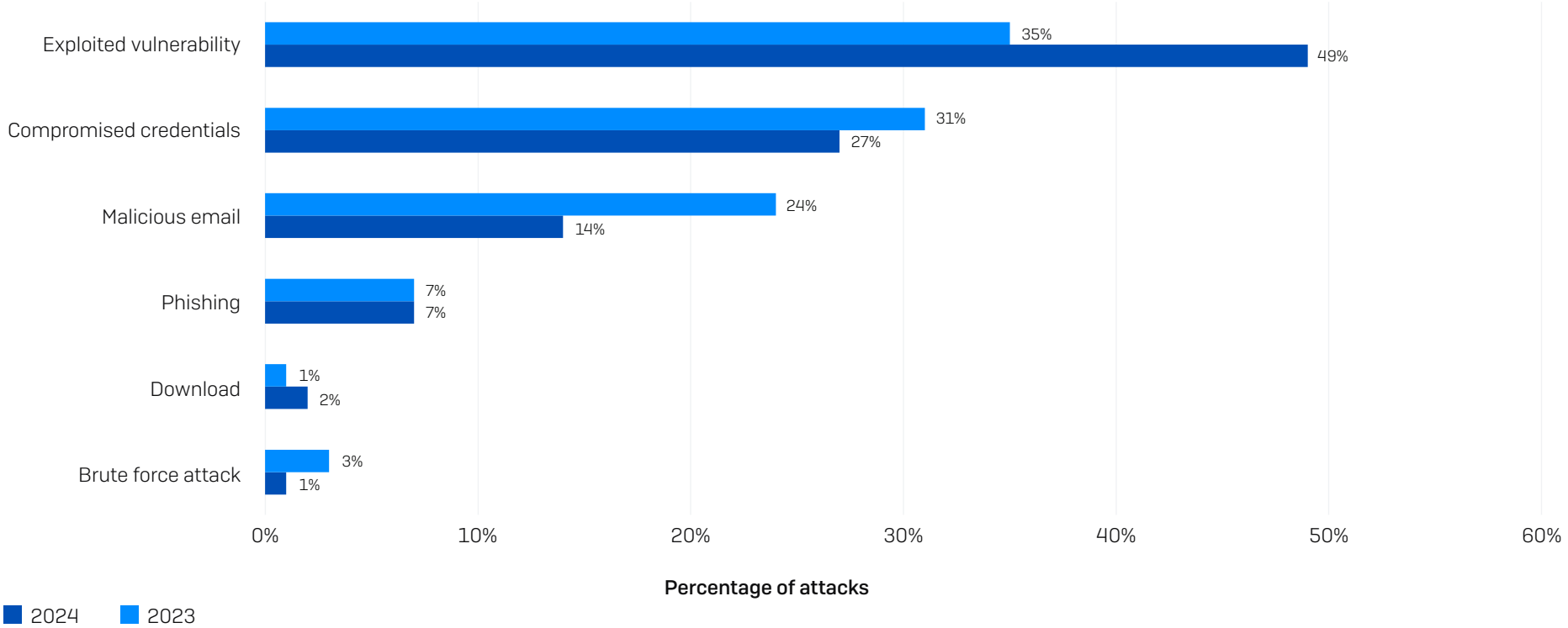
# Root Causes of Ransomware Attacks in Critical Infrastructure

All energy, oil/gas and utilities organizations hit by ransomware were able to identify the root cause of the attack. Exploited vulnerabilities (49%) topped the list as the most common attacker entry method in 2024, followed by compromised credentials, used in over one in four attacks (27%). While the running order of the four most common root causes remains consistent with our 2023 study, the proportion of attacks starting with the exploitation of unpatched vulnerabilities has increased considerably over the last year.

The entry methods reported by energy, oil/gas and utilities are in line with the global cross-sector, which also has exploited vulnerabilities as the most common root cause (32%) of ransomware attacks and compromised credentials in second position (29%).

Overall, energy, oil/gas and utilities is the sector most likely to fall victim to the exploitation of unpatched vulnerabilities. Government organizations are particularly vulnerable to attacks that start with abuse of compromised credentials: 49% (*state/local*) and 47% (*central/federal*) of attacks began with the use of stolen login data. *IT, technology and telecoms* and *retail* both reported that 7% of ransomware incidents began with a brute force attack – it may be that their reduced exposure to unpatched vulnerabilities and compromised credentials forces adversaries to focus, in part, on other approaches.

See the appendix for a detailed breakdown of 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=183 energy, oil/gas, and utilities organizations hit by ransomware

# Backup Compromise in Critical Infrastructure

98% of energy, oil/gas and utilities organizations hit by ransomware in the past year said that the cybercriminals attempted to compromise their backups during the attack. Four in five (79%) of these backup compromise attempts were successful – the highest rate of successful backup compromise across all sectors.

Energy, oil/gas and utilities 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 ($2.5M vs. $5.5M median initial ransom demand)
- Organizations whose backups were compromised were considerably more likely to pay the ransom to recover encrypted data (64% vs. 39%)
- Median overall recovery costs came in 4X more than that of those that did not have backups compromised ($3,000,000 vs. $750,000)

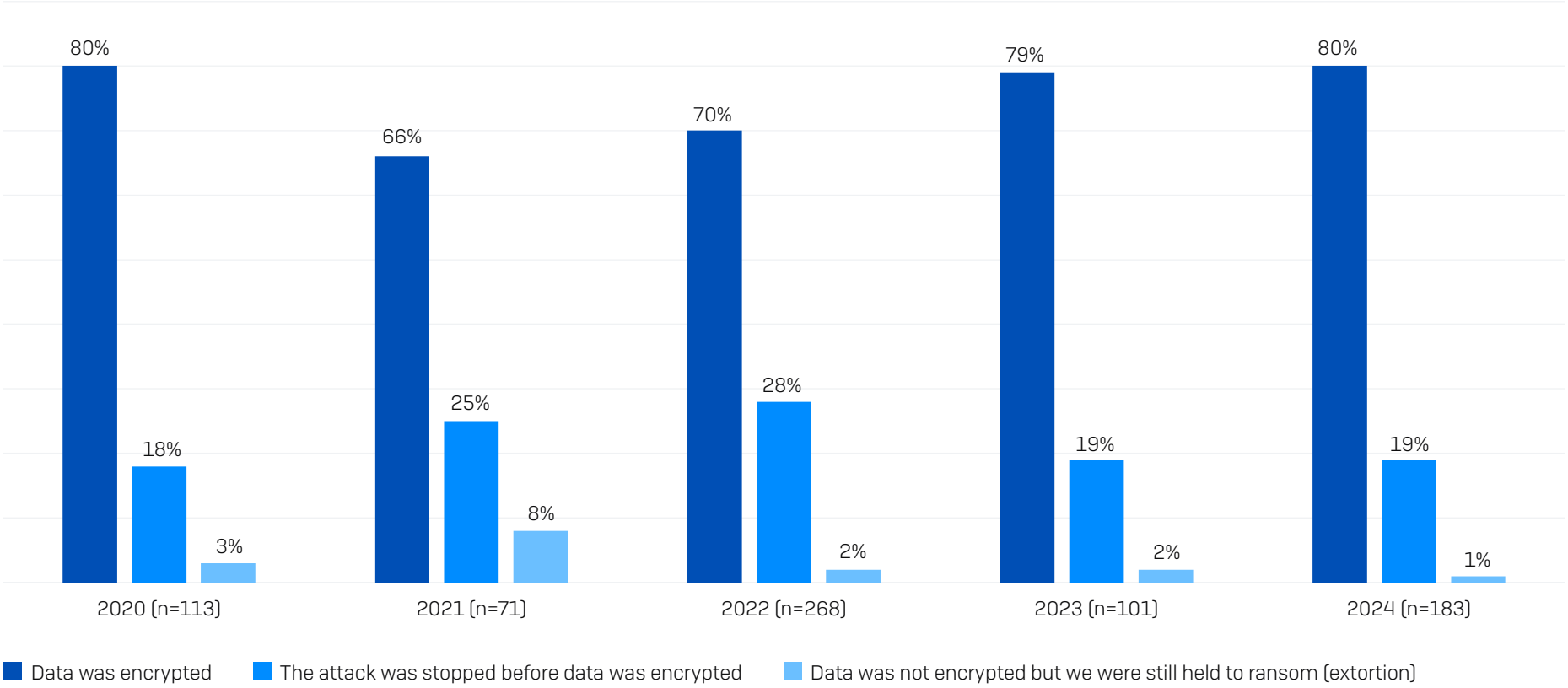
# Rate of Data Encryption in Critical Infrastructure

80% of ransomware attacks on energy, oil/gas and utilities organizations resulted in data encryption in our 2024 study, in line with the encryption rate reported by this sector in 2023 (79%) and higher than the 2024 cross-sector average of 70%.

1% of energy, oil/gas and utilities organizations also experienced an extortion-based attack, where the data was not encrypted but they were held to ransom anyway.

Across sectors, energy, oil/gas and utilities reported one of the highest rates of data encryption (joint with *central/federal government*) after *state/local government* (98%) and *lower education* (85%). *Financial services* (49%) followed by *retail* (56%) reported the lowest rates of data encryption. *Distribution and transport* is the sector most likely to have experienced an extortion-based attack, with 17% saying that data was not encrypted but they were held to ransom anyway – almost three times the rate of any other sector.

See the appendix for a detailed breakdown of the 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. Energy, oil/gas and utilities organizations reported that in 50% of the incidents where data was encrypted, data was also stolen – higher than the 36% 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.

**50%**
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=183)

Across sectors, energy, oil/gas and utilities fares second worst on propensity to have data exfiltrated as well as encrypted, with only the *IT, technology and telecoms* sector (53%) reporting a higher rate. Conversely, the education sector is least likely to report data theft in an attack, with *higher education* reporting the lowest overall propensity to have data encrypted and stolen (18%), followed by *lower education*, which shares the second spot with *healthcare* (both 22%).

# Data Recovery

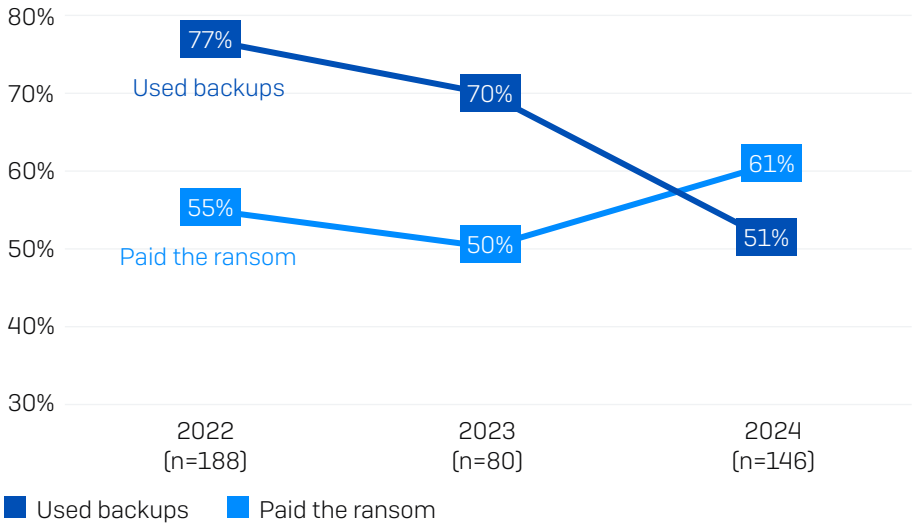
Almost all energy, oil/gas and utilities organizations (99%) that had data encrypted got their data back. Of them, 61% paid the ransom to get encrypted data back, whereas only 51% restored encrypted data using backups – the lowest rate of backup use reported across all sectors. This is the first time that energy, oil/gas and utilities organizations have reported a higher propensity to pay the ransom than use backups.

| Use backups to restore data | Paid the ransom and got data back | Use other means to get data back |
|---|---|---|
| **51%** | **61%** | **24%** |

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)

24% of the energy, oil/gas and utilities organizations used other means to get data back – while the survey did not explore this area further, this could include working with law enforcement or using decryption keys that had already been made public.

This year's findings represent a marked change from the previous two years when the sector enjoyed impressive rates of backup use (70% in 2023 and 77% in 2022).




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.

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). This time, 35% of energy, oil/gas and utilities organizations that had data encrypted reported using more than one method, higher than the 26% reported in 2023.

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

# Ransom Demands

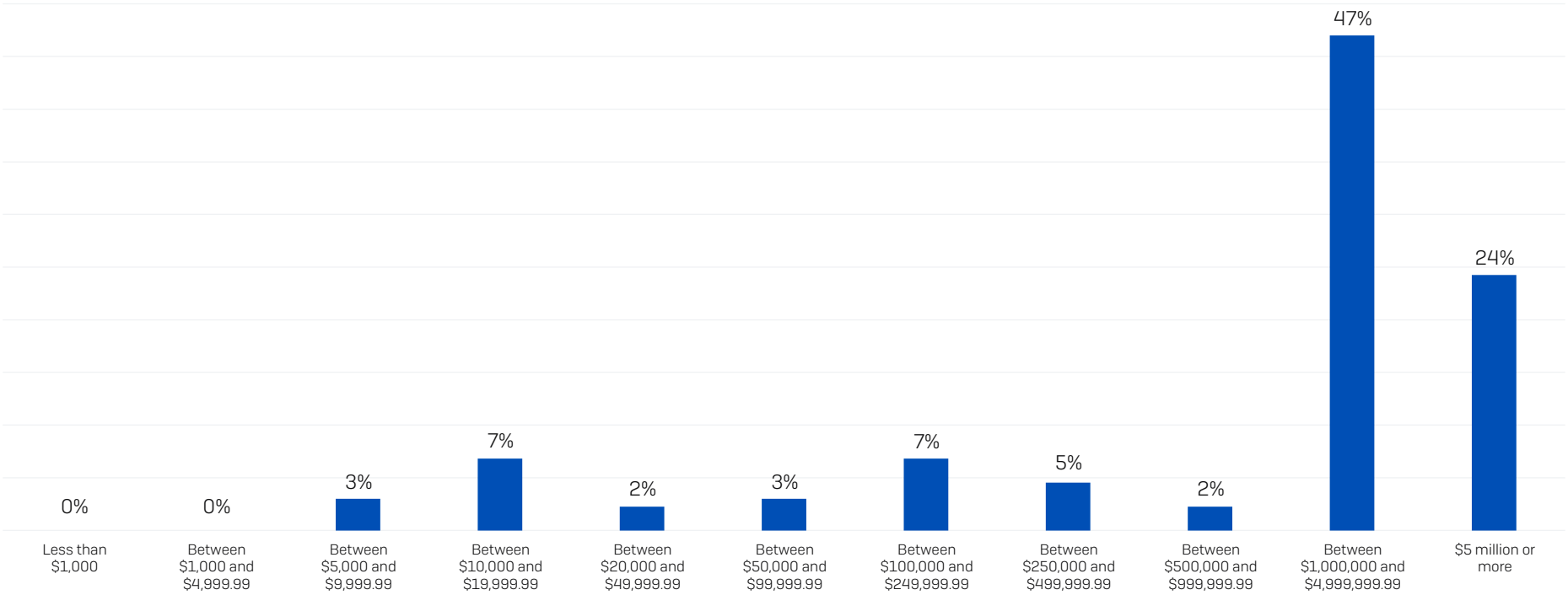
This year, for the first time, we included both ransom demands and payments in this report. Across the 132 energy, oil/gas and utilities organizations that had their data encrypted and were able to share the attackers' initial ransom demand, the average ask was $2.54M (median) and $3.9M (mean).

One of the most notable findings in this year's study is that 71% of ransom demands made to energy, oil/gas and utilities organizations are for $1M or more, with one-quarter of the demands (24%) for $5M or more.

These huge demands are not exclusive to the energy, oil/gas and utilities sector, with all named sectors (excluding "*other*") reporting median ransom demands of $1M or higher. *Central/federal government* reported the highest median ($7.7M) and mean ($9.9M ) demands, whereas *retail* and *IT, technology and telecoms* received the lowest median demands ($1M), followed by construction ($1.1M).

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=132

# Ransom Payments

86 energy, oil/gas and utilities respondents whose organizations paid the ransom shared the actual sum paid.

- Median payment: $2,540,000
- Mean payment: $3,225,093

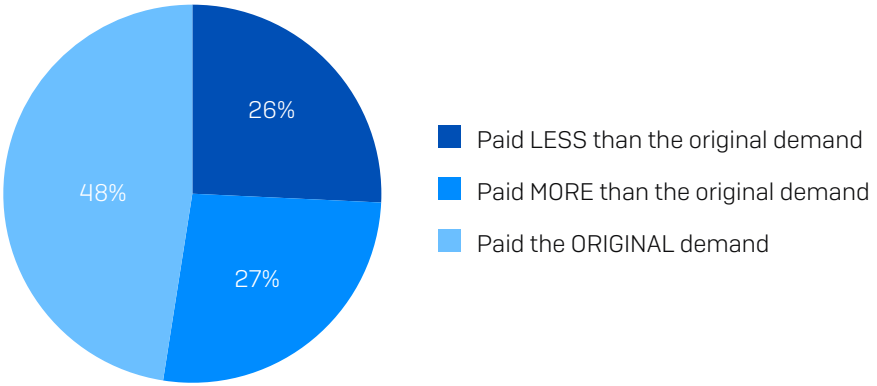
Ransom payments vary considerably by industry. *IT, technology and telecoms* reported the lowest median ransom payment ($300,000), followed by *distribution and transport* ($440,000). At the other end of the scale, both *lower education* and *central/federal government* paid median ransoms of $6.6M.

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

# Propensity to Negotiate Ransom Amounts in Critical Infrastructure

The study has revealed that energy, oil/gas and utilities victims don't always pay the initial sum demanded by the attackers. A little less than half (48%) of respondents said their payment matched the original request. 26% paid less than the original demand, and 27% paid more.

**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=86.

Looking at the data by industry, energy, oil/gas and utilities has the highest propensity to pay the original ransom amount demanded by attackers. It is also the sector with the second lowest propensity to pay less than the original demand.

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), fol-lowed 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 negotiation between the original demand and the eventual payment.

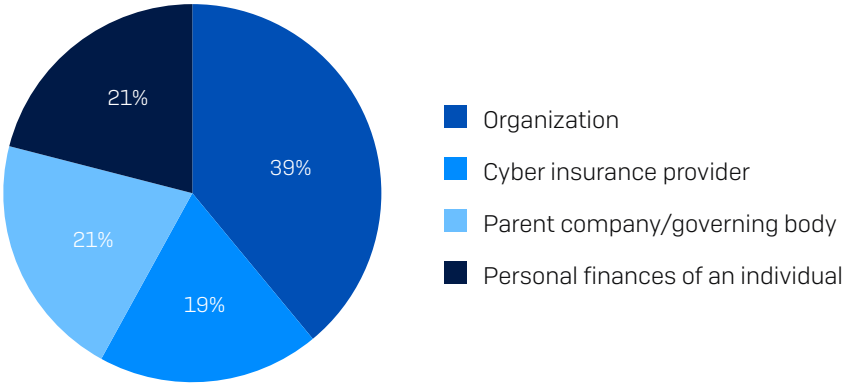
See the appendix for a detailed breakdown of ransom demand vs. ransom payment by industry.

# Source of Ransom Funding in Critical Infrastructure

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 energy, oil/gas and utilities respondents re-porting multiple sources of monies in 82% of cases
- The primary source of ransom funding in energy, oil/gas and utilities organizations is the organization itself, covering 39% of the payment on average; the organization's parent company and/or governing body typically provides 21%
- Insurance providers are heavily involved in ransom payments, contributing in 83% 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=89

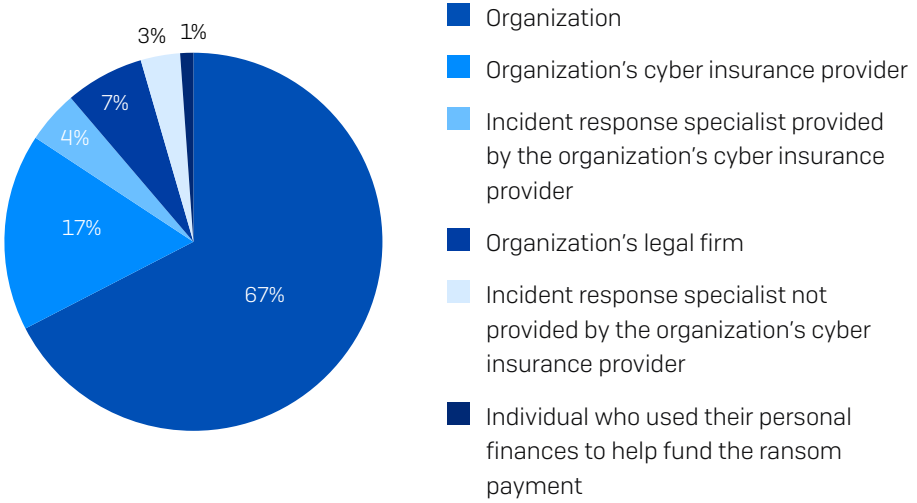
# Ransom Transaction Execution

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

In the energy, oil/gas and utilities sector, the victim organization made two-thirds (67%) of the transactions – the highest across all sectors. Insurance providers transferred the funds for over one-fifth (21%) of ransom payments, either directly (17%) or through their appointed incident response specialist (4%). 7% were executed by the victim's legal firm.

Only 8% (with rounding) of transfers were made by incident response specialists, whether appointed by the insurance provider (4%) or another party, typically the victim (3%).

### Executor of ransom payment transfer

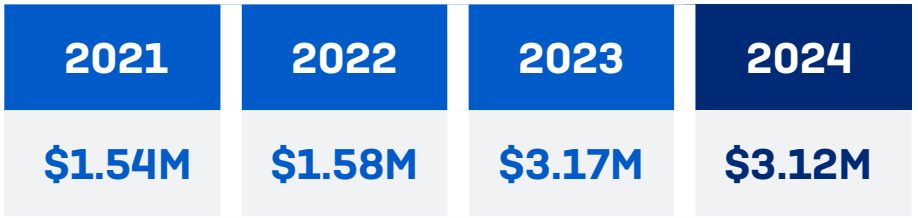



Who made the ransom payment transaction i.e., who transferred the money to the attacker's account? n=89.

# Recovery Costs in Critical Infrastructure

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024, energy, oil/gas and utilities organizations reported a mean cost of $3.12M to recover from a ransomware attack, very similar to the $3.17M reported in our 2023 survey.

In contrast, the cross-sector average showed a 50% increase in recovery costs, coming in at $2.73M in 2024, an increase of almost $1M from 2023 ($1.82M)




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=183 (2024)/101 (2023)/ 268 (2022)/ 71 (2021). N.B. 2022 and 2021 question wording also included "ransom payment".

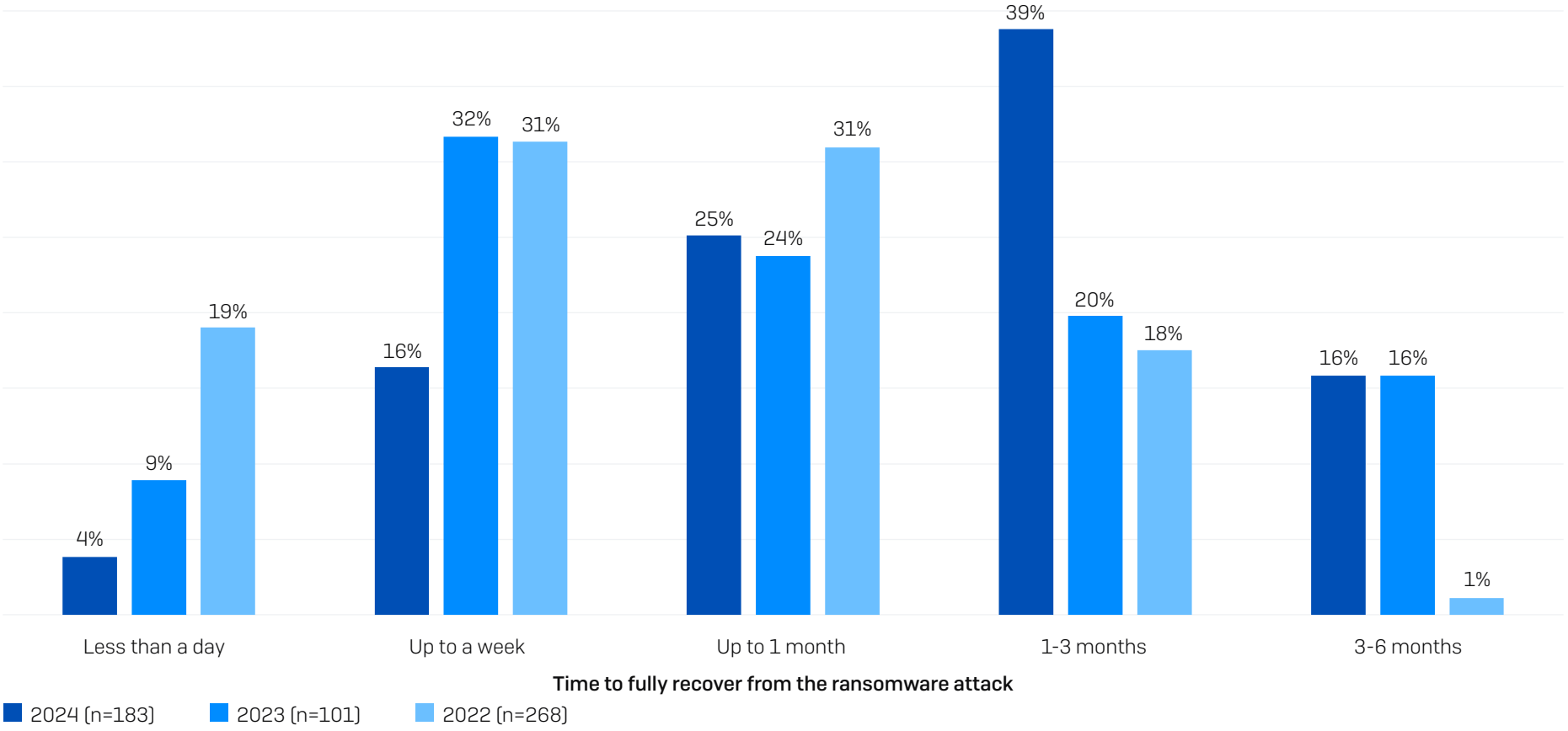
The median recovery cost data for energy, oil/gas and utilities organizations revealed a 4X increase, from $750,000 in 2023 to $3,000,000 in 2024. These figures are considerably above the cross-sector average where median recovery costs doubled from $375,000 to $750,000 over the last year.

# Recovery Time in Critical Infrastructure

The time taken to recover from a ransomware attack is steadily increasing in energy, oil/gas and utilities organizations. Our 2024 research revealed:

- 20% of ransomware victims in energy, oil/gas and utilities are fully recovered in a week or less, down from 41% in 2023 and 50% in 2022
- 55% in energy, oil/gas and utilities now take more than a month to recover, up from 36% in 2023 and 19% 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.

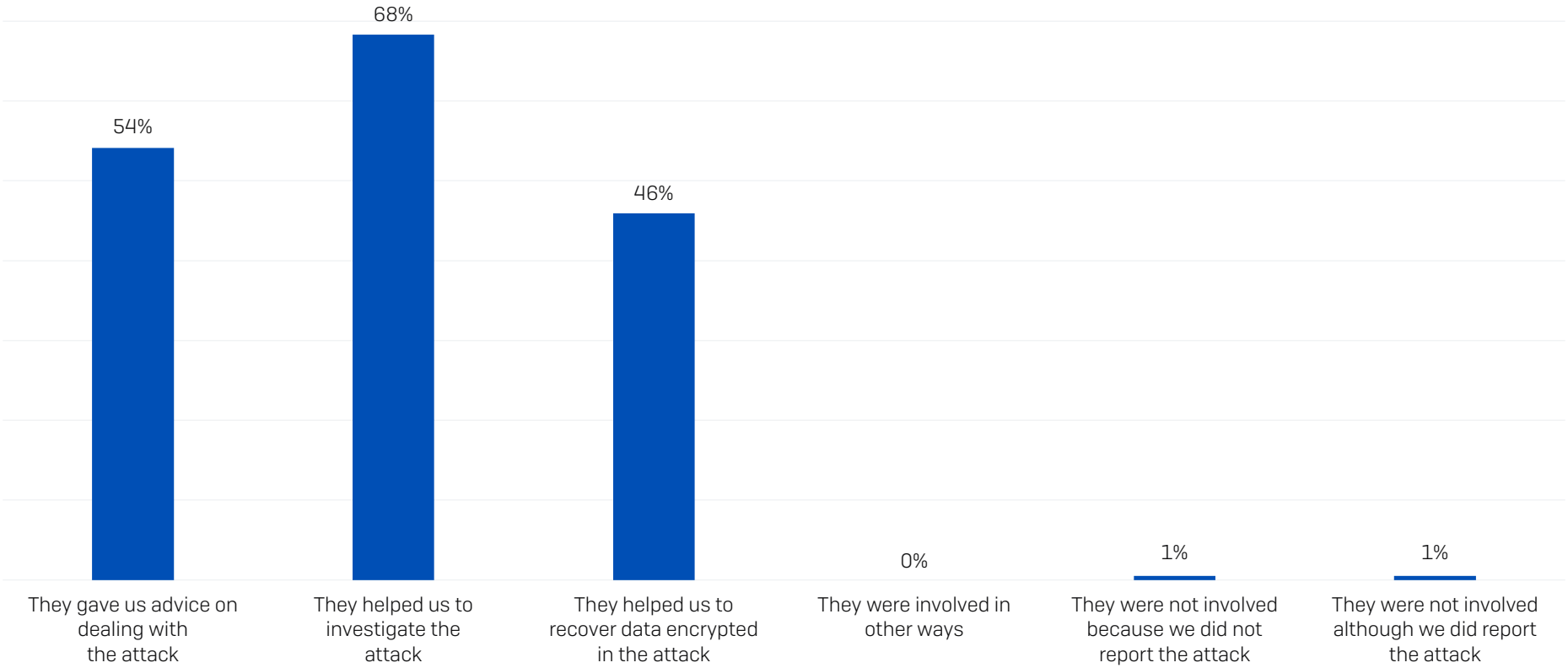



How long did it take your organization to fully recover from the ransomware attack? Base numbers in chart.

# Involvement of Law and Order in Critical Infrastructure

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.

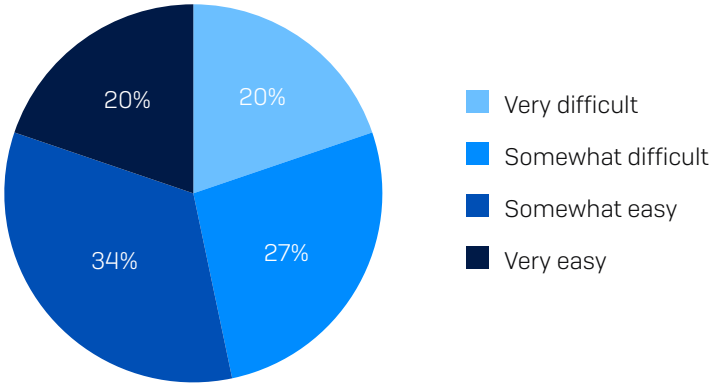
Reflecting the normalization of ransomware, 99% of energy, oil/gas and utilities organizations that were hit by ransomware engaged with law enforcement and/or official government bodies due to the attack. 54% reported that they received advice on dealing with the attack, 68% got help investigating the attack, and 46% said they received help recovering 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=183.

# Ease of Engagement in Critical Infrastructure

Just over half (54%) of those who engaged with law enforcement and/or official bodies in relation to the attack said the process was easy (20% very easy, 34% somewhat easy). 20% said the process was very difficult, while 27% described it as somewhat difficult. While it is encouraging that some found the process easy, there is clearly room to improve the engagement experience for the sector.




How easy or difficult was it for your organization to engage with law enforcement and/or official bodies in relation to the attack? n=182 (excluding "don't know" responses).

# Conclusion

Ransomware remains a major threat to energy, oil/gas and utilities organizations of all sizes around the globe. While the attack rate globally has dropped, energy, oil/gas and utilities experienced the same frequency of attacks as last year. Additionally, the impact of an attack on energy, oil/gas and utilities organizations that fall victim has increased, with the sector reporting one of the highest rates of data encryption and the recovery time from a ransomware attack increasing. 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 around half of the attacks (49%) starting with the exploitation of unpatched vulnerabilities in energy, oil/gas and utilities, 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, including endpoint, email, and firewall technologies, is a must. Endpoints (including servers) are the primary destination for ransomware actors, so ensure 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

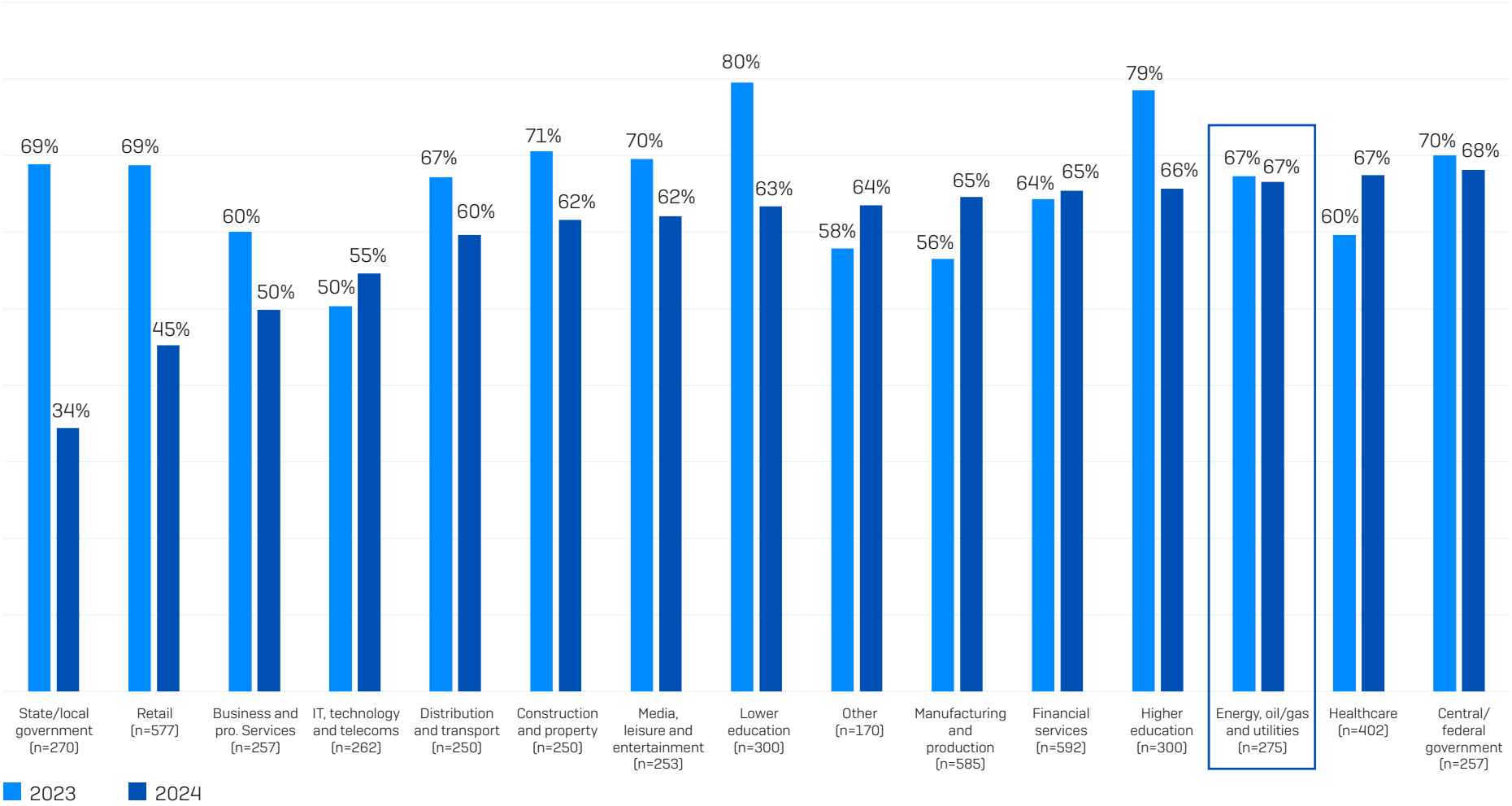
## About Vanson Bourne

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

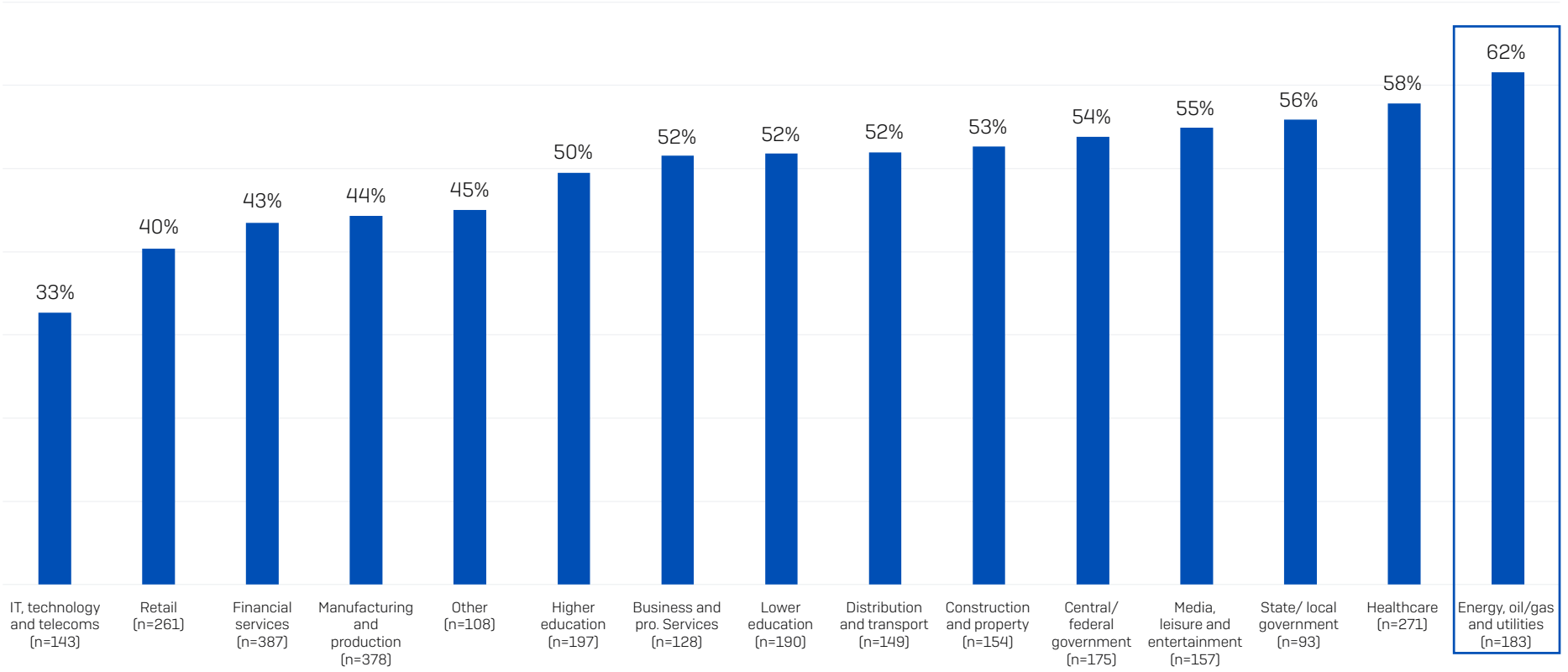
**Percentage of organizations hit by ransomware in the last year**




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.

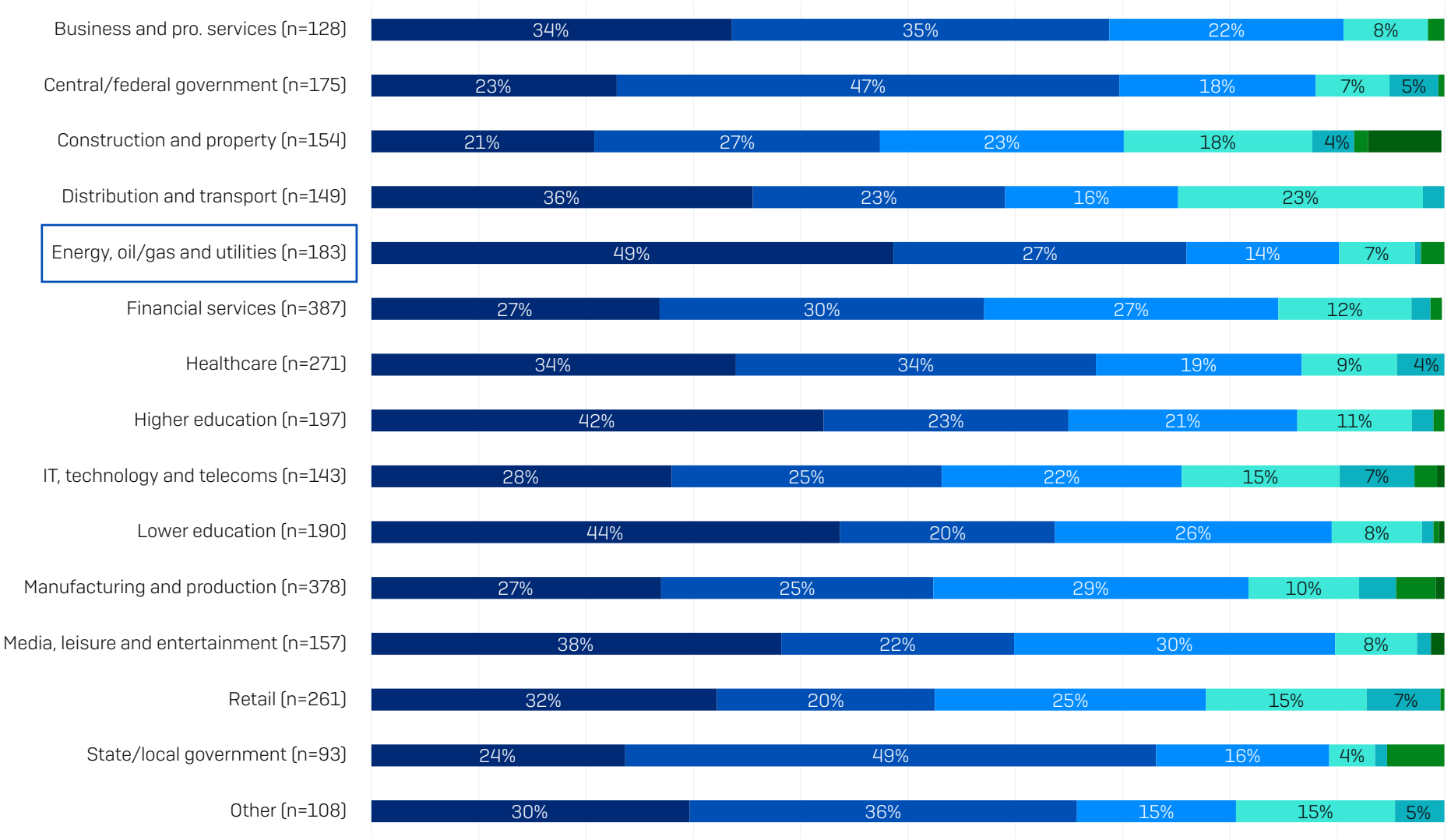
## Percentage of Computers Impacted by Industry

**Percentage of devices impacted**



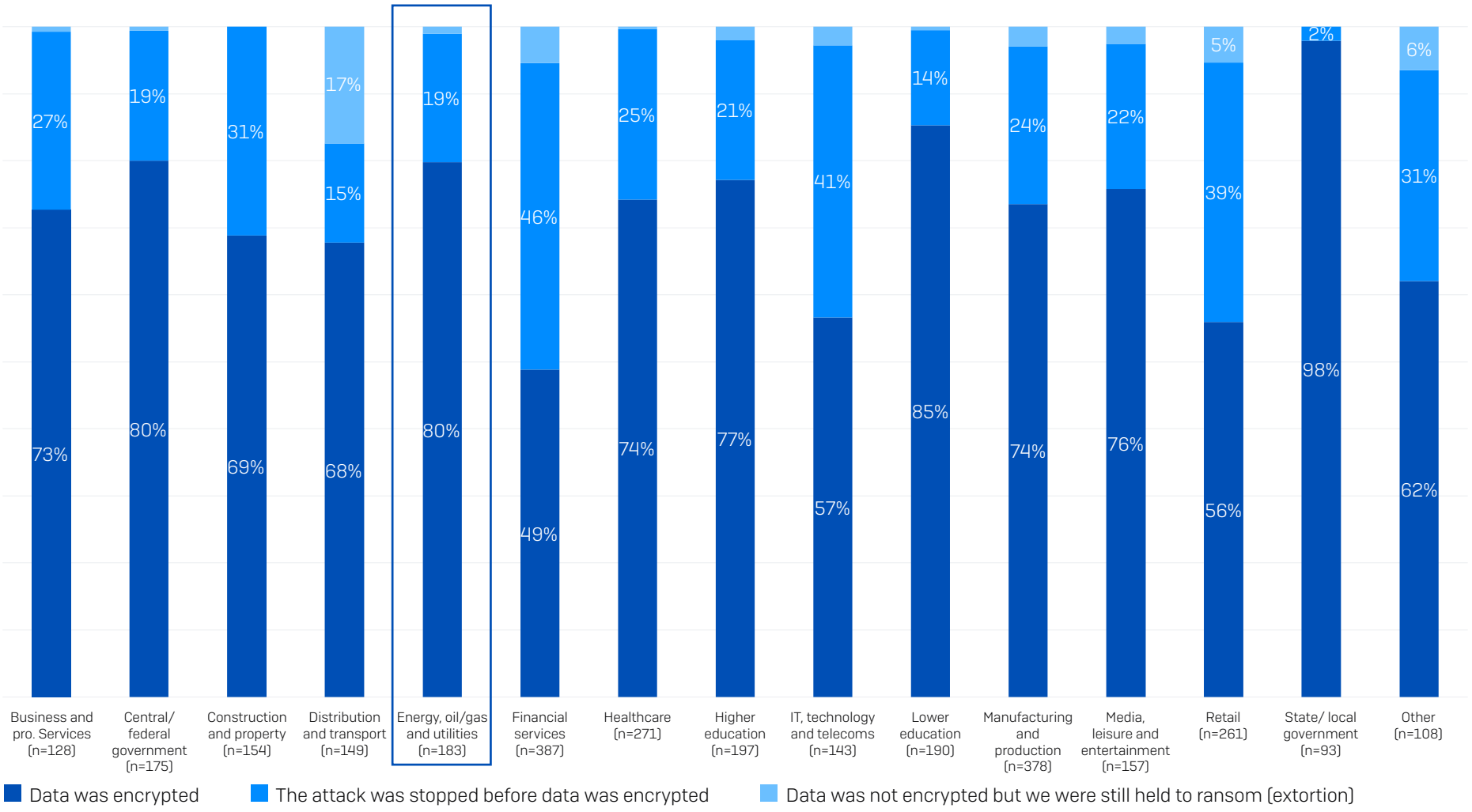

What percentage of your organization's computers were impacted by ransomware in the last year? n=2,974 organizations hit by ransomware. Industry base numbers in chart.

## 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.

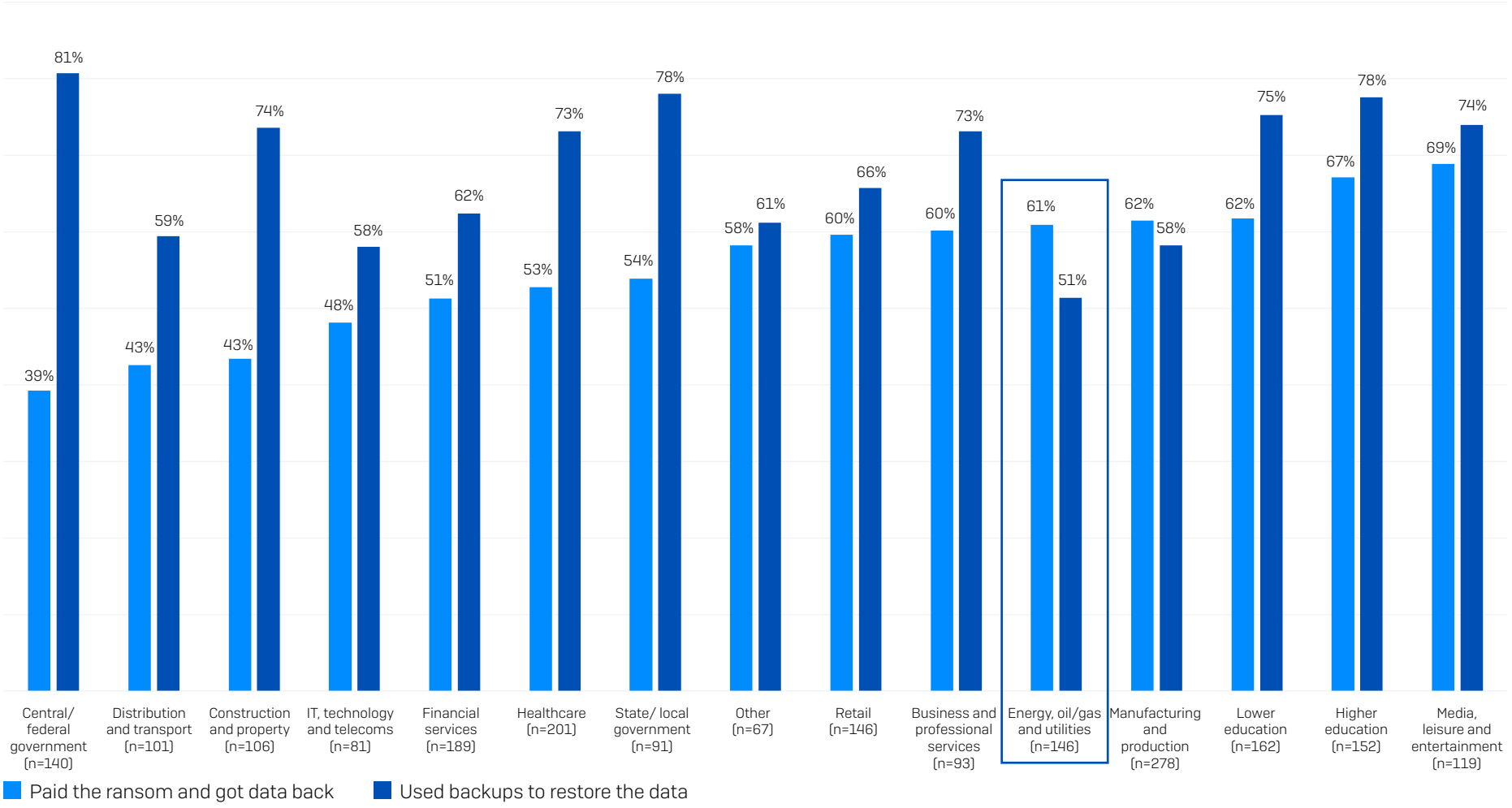
## Data Encryption Rate by Industry




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

## Data Recovery Method by Industry

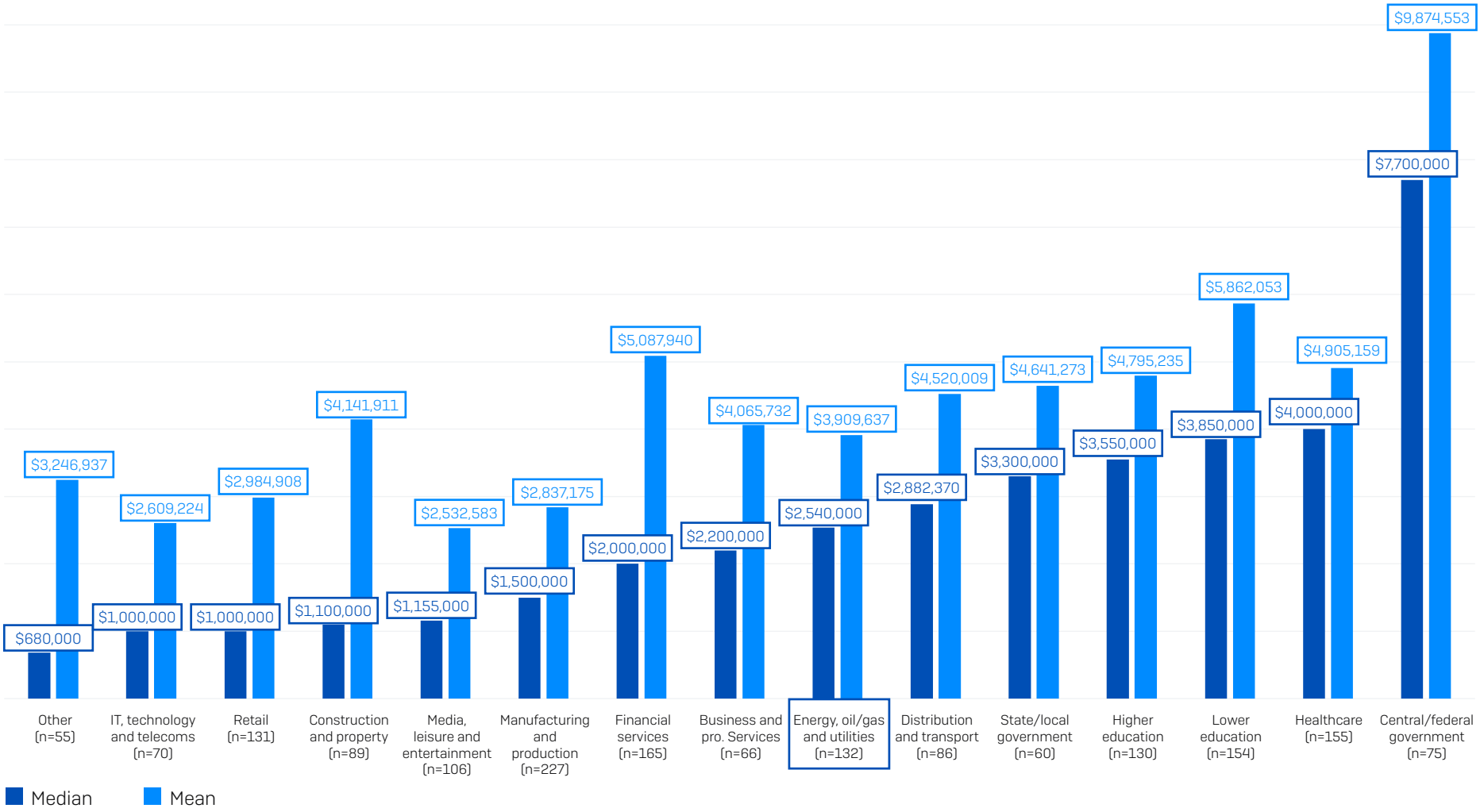
**Percentage that got encrypted data back that used the recovery method**




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

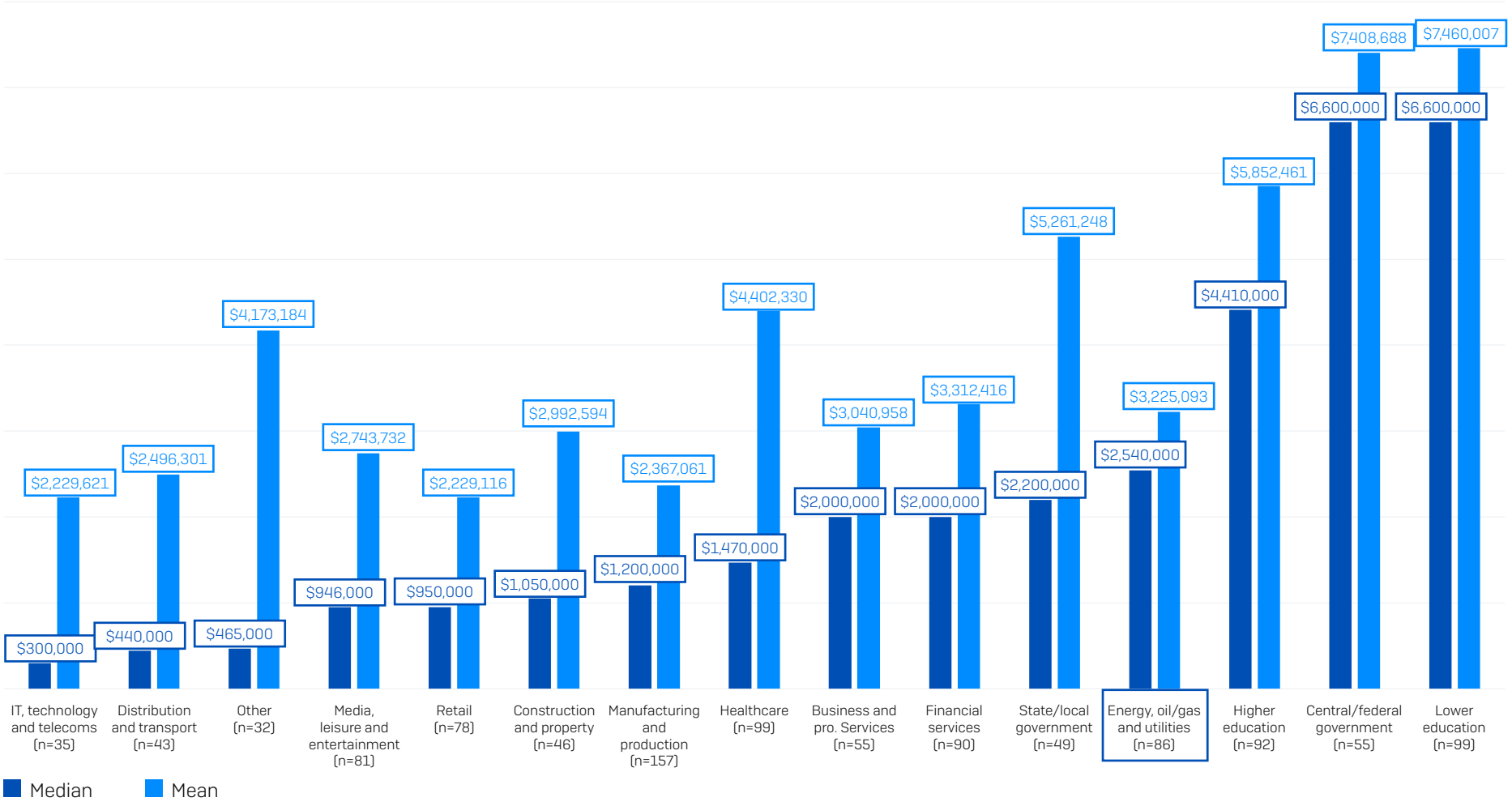
### Ransom demand




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

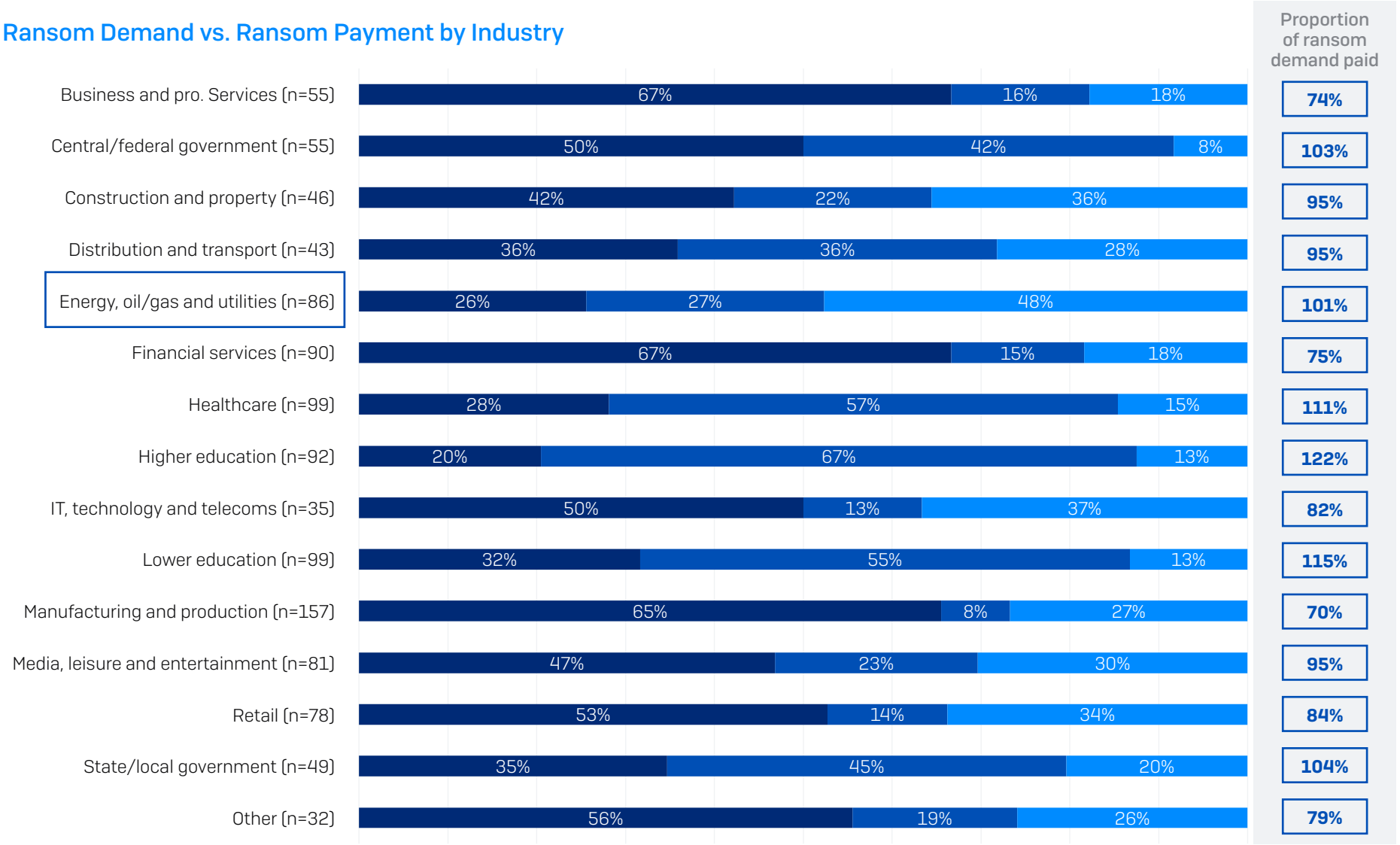
## Ransom Payment by Industry

### 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.



2024-07-10 WP-EN (PC)

SOPHOS