SOPHOS
Cybersecurity delivered.

The State of Ransomware in State and Local Government 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 199 respondents from the state and local government sector.

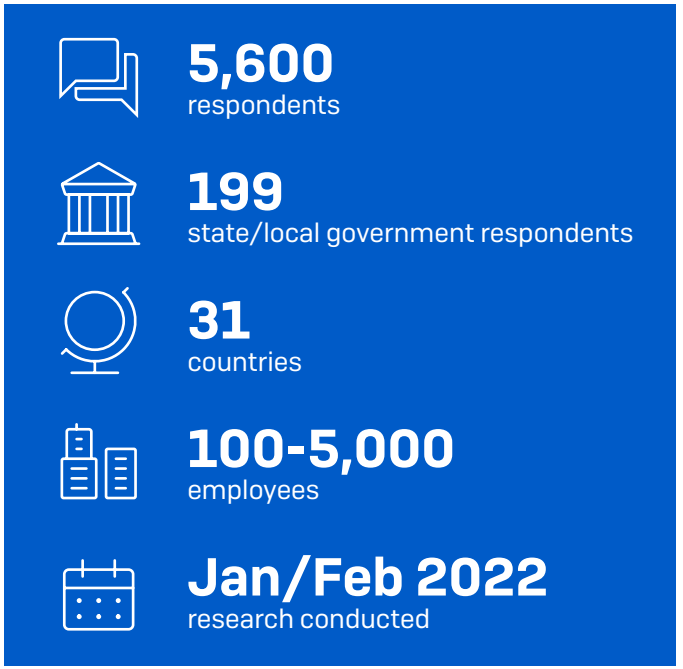
A Sophos Whitepaper. September 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in the state and local government sector has revealed an ever more challenging attack environment. Together with the growing financial and operational burden ransomware places on its victims, it also shines new light on the relationship between ransomware and cyber insurance - including how insurance drives changes to cyber defenses.

About the survey

Sophos commissioned research agency Vanson Bourne to conduct an independent, vendor-agnostic survey of 5,600 IT professionals, including 199 from state and local government. Respondents were from mid-sized organizations (100-5,000 employees) across 31 countries. The survey was conducted during January and February 2022, and respondents were asked to answer based on their experiences over the previous year.



Ransomware attack rate increased over the last year

58% of local government organizations were hit by ransomware in 2021, up from 34% in 2020. This is a 70% rise over the course of a year, demonstrating that adversaries have become considerably more capable of executing the most significant attacks at scale.

All sectors reported an increased attack rate in 2021 and in fact state and local government reported one of the lower ransomware attack rates across all the sectors surveyed. For comparison, 66% of respondents across all sectors reported being hit by ransomware over the last year. (Note: "hit by ransomware" was defined as one or more devices being impacted but not necessarily encrypted.)

While the rate of attack was below the cross-sector average, state and local government organizations reported one of the highest rates of data encryption following an attack, with almost three-quarters (72%) of respondents saying that the adversaries succeeded in encrypting data. Globally, across all industries, 65% of attacks resulted in data encryption, which is a 20% increase from the 54% that reported data encryption after an attack in 2020.

Only 20% of state and local government organizations were able to stop such attacks before data could be encrypted. This figure is considerably lower than the global average of 31%, suggesting that state and local government organizations are poorly equipped to identify and stop attacks before damage is done.

One interesting – and anomalous - finding is the considerable increase in extortion-only attacks affecting state and local government organizations over the last year, with the rate increasing from just 2% of ransomware attacks in 2020 to 8% in 2021. This is the highest encryption-only rate reported across all sectors in 2021 and bucks the global 2021 trend for a decline in extortion-only attacks.

The global drop is likely a result of adversaries combining both ransomware and extortion in their attacks in an effort to increase pay-out rates. It will be interesting to see from next year's results whether the 2021 state and local government experience reflects a lag behind other sectors or an ongoing situation.

Hit by ransomware

58%
state/local government organizations

66%
cross-sector average

Data encrypted in attacks

72%
state/local government organizations – one of the highest across sectors

65%
cross-sector average

The changing threat environment for state and local government

The rise in successful ransomware attacks is part of an increasingly challenging threat environment that has affected organizations across all sectors, including state and local government.

In state and local government, 59% of respondents perceived an increase in the volume of attacks on their organizations over the last year, 59% reported an increase in attack complexity, and 56% experienced an increase in the impact of cyberattacks.

It's clear that as adversaries continue to evolve their attacks and take advantage of AI and automation technology to expand their reach, the challenge for all defenders continues to grow.

Increase in volume, complexity, and impact of attacks over the last year

	INCREASE IN VOLUME OF CYBER ATTACKS	INCREASE IN COMPLEXITY OF CYBER ATTACKS	INCREASE IN THE IMPACT OF CYBER ATTACKS
State/local government	59%	59%	56%
Cross-sector average	57%	59%	53%

Most state and local government victims get some encrypted data back

As ransomware has become more prevalent, organizations have gotten better at dealing with the aftermath of attacks. Almost all state and local government organizations (99%) hit by ransomware and that had data encrypted got some encrypted data back.

While backups were the number one method used to restore data – employed by 63% of state and local government organizations whose data was encrypted – usage is considerably below the global average rate of 73%. This indicates that there are immediate opportunities for this sector to strengthen its attack resilience by improving its ability to use backups to restore encrypted data.

In parallel, 32% of state and local government organizations paid ransom to restore encrypted data. This is the lowest reported ransom payment rate across all sectors and is considerably below the global average of 46%. It also represents a more than 30% decrease in the rate of ransom payments compared to 2020, when 42% of local government organizations paid up.

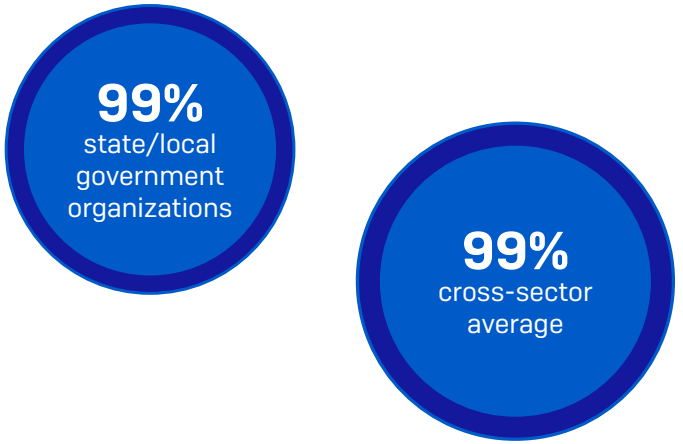
Furthermore, 45% of state and local government respondents said they used other means to restore data – considerably higher than the 30% global average.

These numbers demonstrate that many state and local government organizations are using multiple restoration approaches in parallel to maximize the speed and efficacy with which they can get back up and running. In fact, more than a third (37%) used more than one method to get their encrypted data back in the most significant attacks.

Data restoration method

	USED BACKUPS	PAID THE RANSOM	USED OTHER MEANS	MULTIPLE METHODS USED
State/local government	63%	32%	45%	37%
Cross-sector average	73%	46%	30%	44%

Restored some encrypted data



Proportion of encrypted data recovered after paying ransom has fallen

Across all sectors, the average percentage of data recovered after paying ransom has dropped over the last year, coming in at 61% in 2021 – down from 65% in 2020.

State and local government experienced a similar downward trend. Just 58% of encrypted data was recovered on average in 2021 - below the cross-sector average recovery rate and a considerable drop from the 70% reported by this sector in 2020.

The key takeaway here is that, at best, paying ransom generally only results in the partial restoration of encrypted data. Ransom payments cannot be counted on to restore all data.

Percentage of data restored after paying the ransom

58%
state/local government

61%
cross-sector average

State and local government made low ransom payments

Across all sectors, 965 respondents whose organizations paid ransom shared the exact amounts, revealing that average ransom payments have increased considerably in 2021. Overall, the average ransom payment came in at US$812,360, a 4.8X increase from the 2020 average of US$170K (based on 282 respondents).

Twenty respondents from the state and local government sector shared exact ransom payment amounts, with the average coming in at $213,801 – less than one-third of the cross-sector average of $812,360. Given the low response base, state and local government ransom payment data should be considered indicative rather than statistically significant.

Diving deeper, we can see that ransom payments are often extremely low in this sector, with one in three (30%) paying less than US$1K. Overall, 90% of the state and local government respondents said their organizations paid ransom of less than US$100K. These low payments help keep the sector's average considerably down compared to all other industries.

Only 10% of state and local government respondents paid US$100K or more, compared to nearly half (47%) of all respondents globally. Just one respondent said their organization paid US$1M or more, which is considerably below the global average of 11%.

Ransom paid by state/local organizations

US$213K state/local government

US$812K cross-sector average

30%
paid less than US$1K

90%
paid less than US$100K

10%
paid US$100K or more

Only one respondent
paid US$1M or more

Ransomware greatly impacts state and local government victims

The ransom sums are just part of the story, and the impact of ransomware ranges much more widely than the encrypted databases and devices.

Looking at the impact of ransomware on the day-to-day running of the sector, 82% of respondents said their organizational ability to operate was impacted by the ransomware attacks. This is a little below the global average of 90%.

In terms of the overall remediation bill, across all sectors, the average cost to rectify the impact of the most recent ransomware attack was US$1.4M in 2021 – down from US$1.85M in 2020.

State and local government organizations, however, reported the lowest overall recovery cost of all sectors, with the final bill averaging $0.66M. This represents a drop of almost $1 million from the average cost of $1.64M reported by the sector in 2020.

While it is encouraging that state and local government experienced such reductions in remediation costs, $660K remains a considerable amount of money for any organization - particularly those in a sector often short of funds.

Moving on to recovery time, just over half (52%) of state and local government organizations that were hit by ransomware were up and running again within a week of each attack, in line with the global average. One in five (21%) respondents reported that it took them between one and six months to recover.

Impact on the ability to operate

82%
state/local government

90%
cross-sector average

The average cost to remediate the most recent attack

US$0.66M state/local government

US$1.40M cross-sector average

Time to recover from ransomware attacks

DURATION	STATE/LOCAL GOVERNMENT	CROSS-SECTOR AVERAGE
Up to a week	52%	53%
1-6 months	21%	20%

Cyber insurance coverage against ransomware is below average

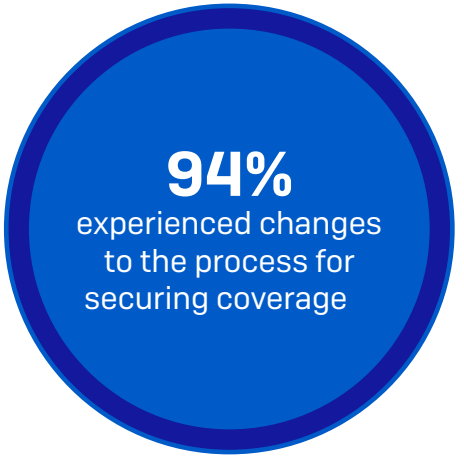
Eight in ten (80%) state and local government respondents said their organizations have cyber insurance against ransomware. While this is below the global average of 83%, it represents a considerable increase from the 51% of public sector respondents (note: not exclusively state and local government) that reported having ransomware coverage in 2019.

For 94% of those with cyber insurance in state and local government, the process for securing coverage changed over the last year:

- 43% said fewer insurance providers are offering cyber insurance
- 55% said the level of cybersecurity they need to qualify for cyber insurance is now higher
- 41% said policies are now more complex
- 33% said the process takes longer
- 28% said it is more expensive

These changes are closely linked to ransomware, which is the single largest driver of cyber insurance claims. In recent years, ransomware attacks have increased, and ransoms and pay-out costs have soared. As a result, some insurance providers have left the market as it has simply become unprofitable for them.

With fewer cyber insurance coverage providers, it's a seller's market. They call the shots and can be selective about which clients they cover. The insurance providers that remain are looking to reduce risk and exposure, and are also pushing up prices considerably. Strong cyber defenses significantly improve an organization's ability to secure the necessary coverage.



Cyber insurance is driving improvements in cyber defenses

As the cyber insurance market hardens and it becomes more challenging to secure coverage, 96% of state and local government organizations that have cyber insurance have made changes to their cyber defenses in order to improve their cyber insurance positions:

- 63% have implemented new technologies/services
- 56% have increased staff training/education activities
- 51% have changed processes/behaviors

Cyber insurance drives improvement in cyber defenses

	HAVE CHANGED CYBER DEFENSES TO IMPROVE INSURANCE POSITION	HAVE IMPLEMENTED NEW TECHNOLOGIES/ SERVICES	HAVE INCREASED STAFF TRAINING/ EDUCATION ACTIVITIES	HAVE CHANGED PROCESSES/ BEHAVIORS
State/local government	96%	63%	56%	51%
Cross-sector average	97%	64%	56%	52%

Ransom payment by insurance providers is above average

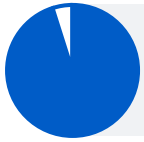
Across all sectors, cyber insurance almost always pays out towards some costs in the event of a ransomware attack. State and local government organizations reported a 95% pay-out rate, which is slightly below the cross-sector average of 98%.

Diving into the details, we see that the insurance covered the clean-up costs for state and local government in just 44% of cases. This is the lowest rate across all sectors and is considerably below the cross-sector average of 77%. Given the high cost of remediating attacks, this is a concerning finding.

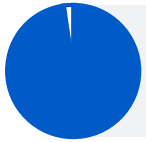
However, state and local government respondents reported an above-average rate of ransom pay-outs, with insurers paying out in almost half (49%) of incidents. With very low ransom payments common in this sector, it may be that the insurers are able to leverage their experience to keep these costs down.

It's worth remembering that while cyber insurance will help an organization get back to its previous state, "betterment" isn't covered. The organization would still need to invest in better technologies and services to address the weaknesses that led to the attack.

Insurance payout rate:



95%
state/local government



98%
cross-sector average

Clean-up costs payout:

44%
state/local government – lowest across all sectors

77%
cross-sector average

Ransom payout:

49%
state/local government

40%
cross-sector average

Conclusion

The ransomware challenge facing state and local government organizations continues to grow. The proportion of organizations hit by ransomware has increased considerably over the last year, with cyber criminals succeeding in encrypting data in over half of the attacks.

In the face of this near normalization of ransomware, government organizations have gotten better at dealing with the aftermath of attacks: virtually everyone now gets some encrypted data back. While backups were the number one method used to restore encrypted data, usage of backups was considerably below the global average in state and local government organizations, indicating there is room for improvement.

The state and local government sector is least likely to pay ransom, with just 32% of organizations whose data was encrypted paying ransom in an attempt to get it back - compared to the global average of 46%. Given that, on average, just 58% of encrypted data was restored in this sector after paying ransom, organizations are wise to be cautious about paying up.

Financially, this sector reported a considerable drop in the overall costs to remediate attacks, down from $1.64M in 2020 to $0.66M in 2021. This was the lowest average across all sectors and is considerably below the global 2021 average of US$1.4M.

Ransomware also had a major impact on the sector's ability to function, with more than 80% saying their operations were impacted.

Many state and local government organizations are choosing to reduce the risks associated with ransomware attacks by taking cyber insurance coverage. For them, it is reassuring to know that insurers pay some costs in almost all claims.

95% of state and local government organizations with insurance coverage against ransomware reported that providers paid out following attacks, slightly below the cross-sector average of 98%. However, while the sector's ransom pay-out rate was above average (49%), only 44% said that the insurance providers paid clean-up costs, considerably below the cross-sector average of 77%.

It's getting harder for state and local government organizations to secure coverage. The constriction of the insurance market has driven almost all organizations in this sector to make changes to their cyber defenses in order to improve their cyber insurance positions.

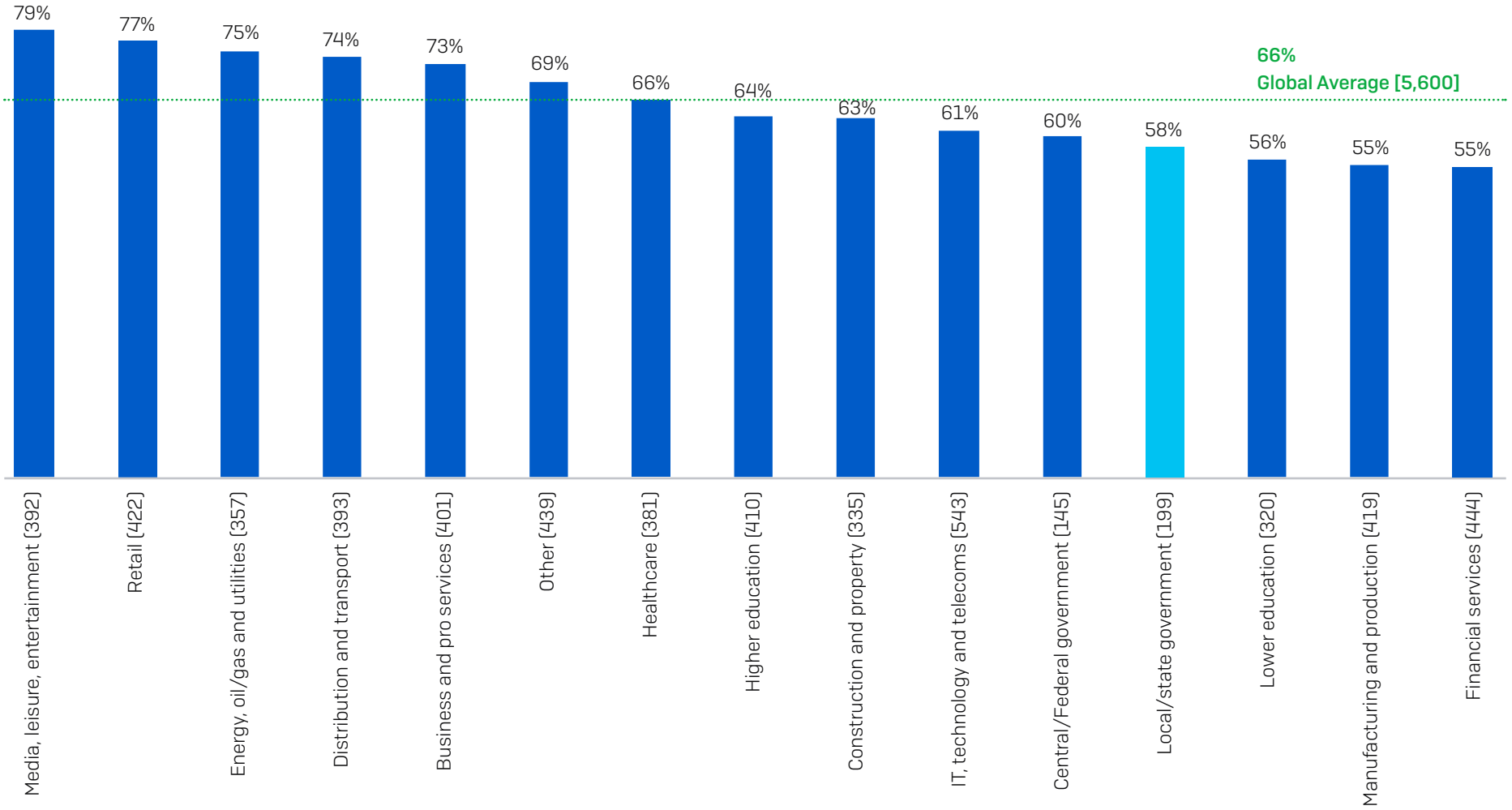
Recommendations

In light of these findings, optimizing ransomware defense is more important than ever. Our five top tips are:

- Ensure high-quality defenses at all points in your environment. Review your security controls and make sure they continue to meet your needs.
- Proactively hunt for threats so you can stop adversaries before they can execute attacks. If you don't have the time or skills in-house, work with a specialist managed detection and response (MDR) cybersecurity service.
- Harden your environment by searching for and closing security gaps: unpatched devices, unprotected machines, open RDP ports, and related weaknesses. Extended Detection and Response (XDR) is ideal for this purpose.
- Prepare for the worst. Know what to do if a cyber incident occurs and who you need to contact.
- Make backups and practice restoring from them. Your goal is to get back up and running quickly, with minimal disruption.

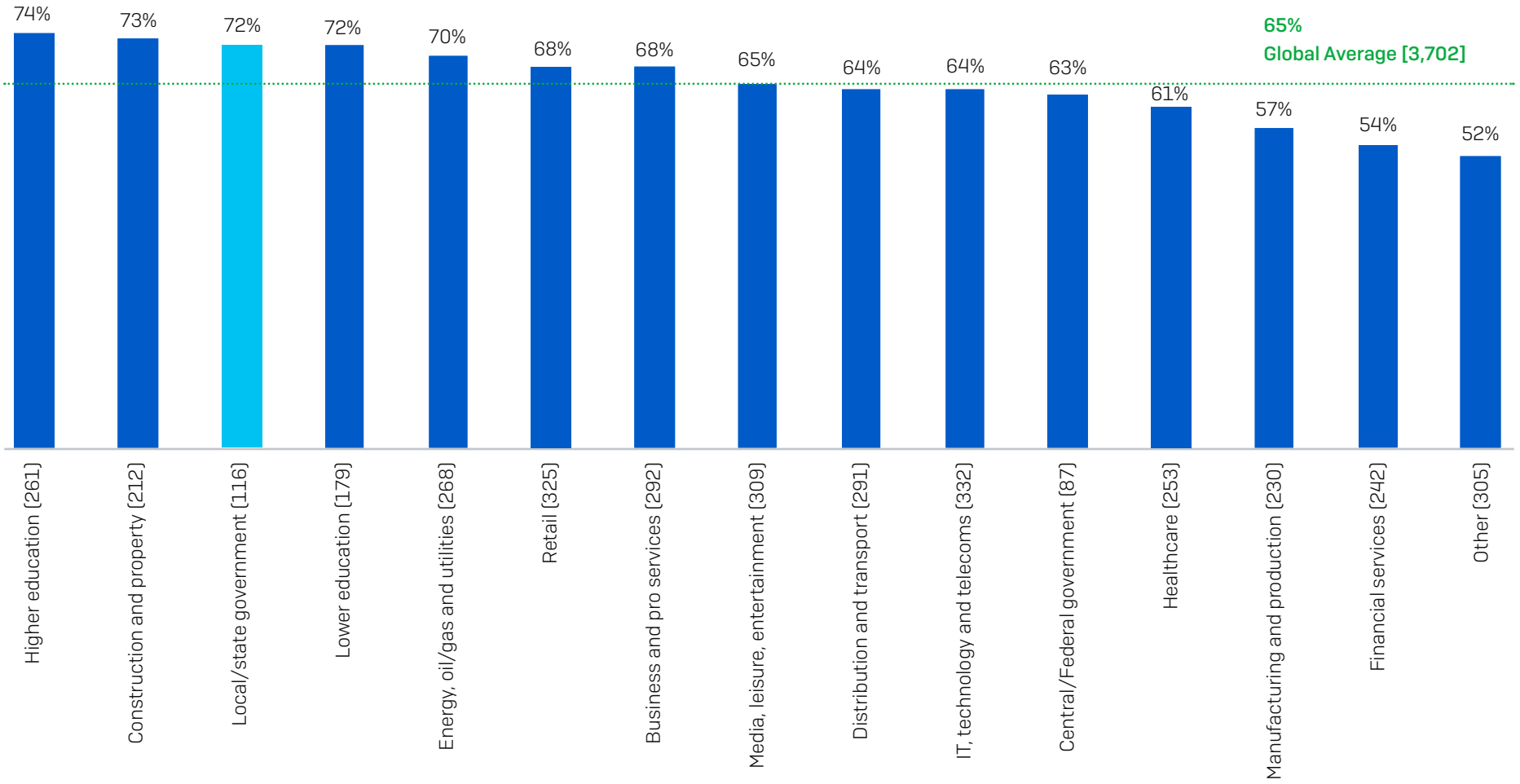
See the Sophos ransomware threat intelligence center for detailed information about individual ransomware groups.

State and Local Government Has Below-Average Attack Rate



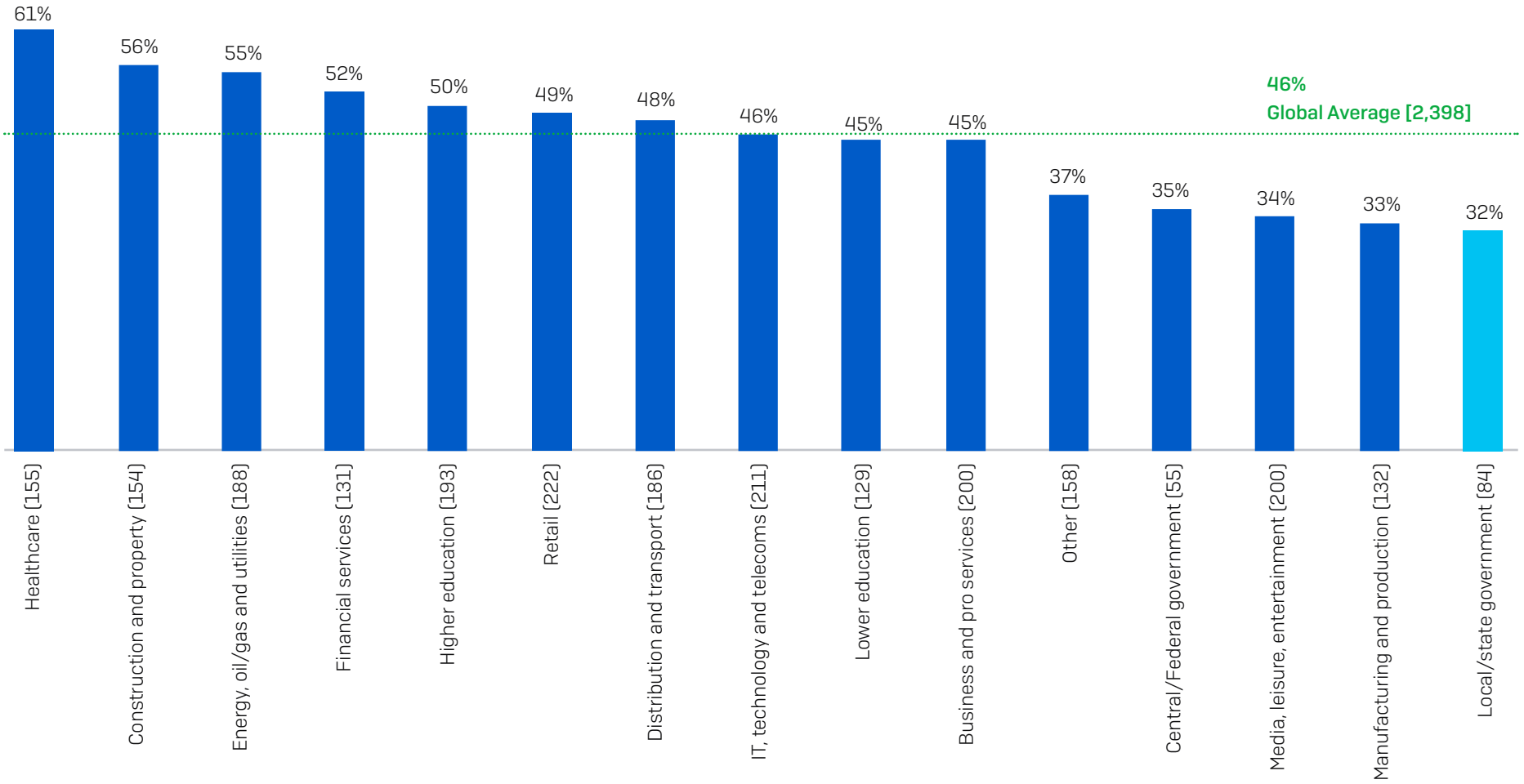
In the last year, has your organization been hit by ransomware? (n=5,600): Yes

State and Local Government Has a High Encryption Rate



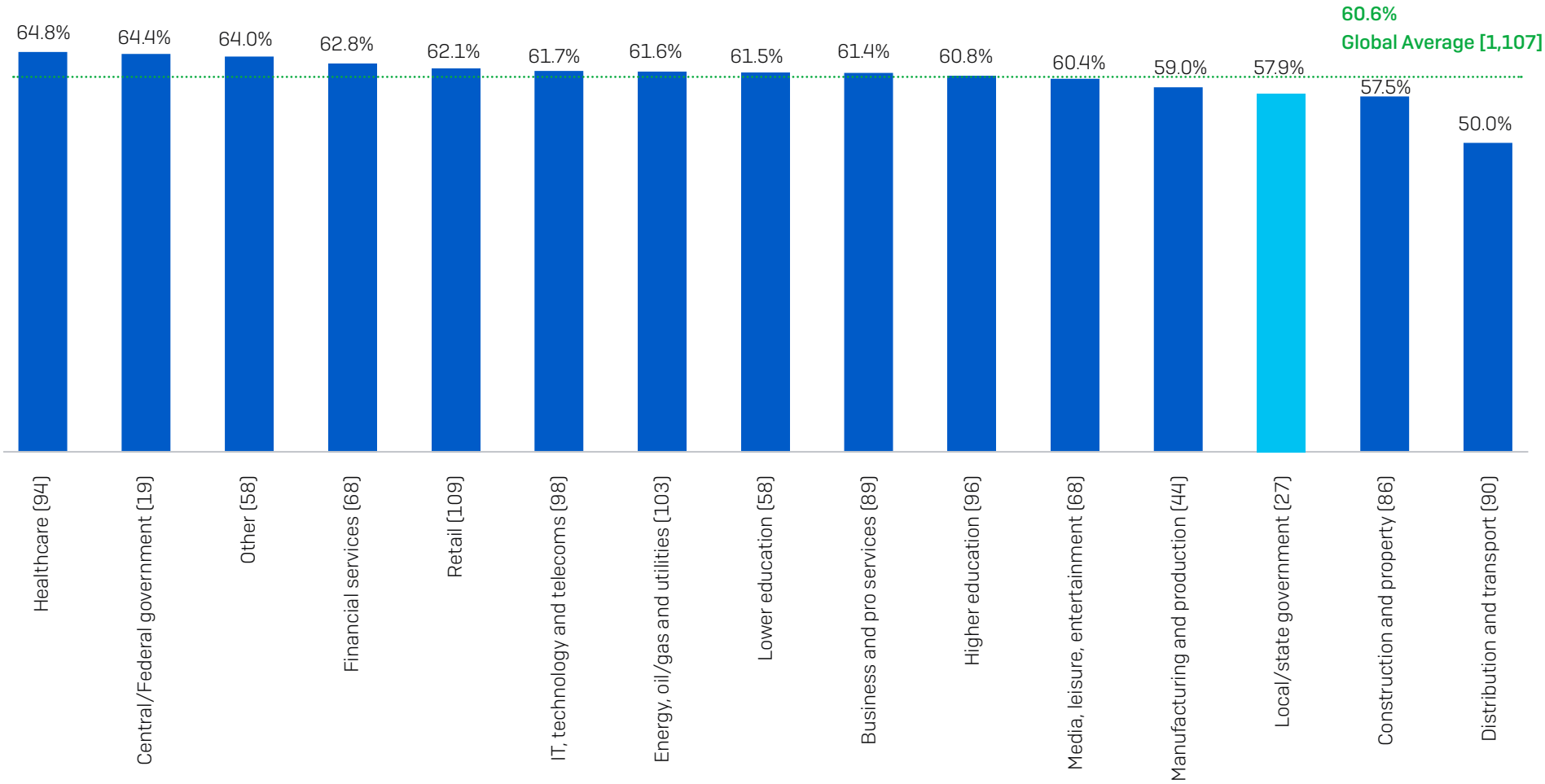
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

State and Local Government Has Lowest Ransom Payment Rate



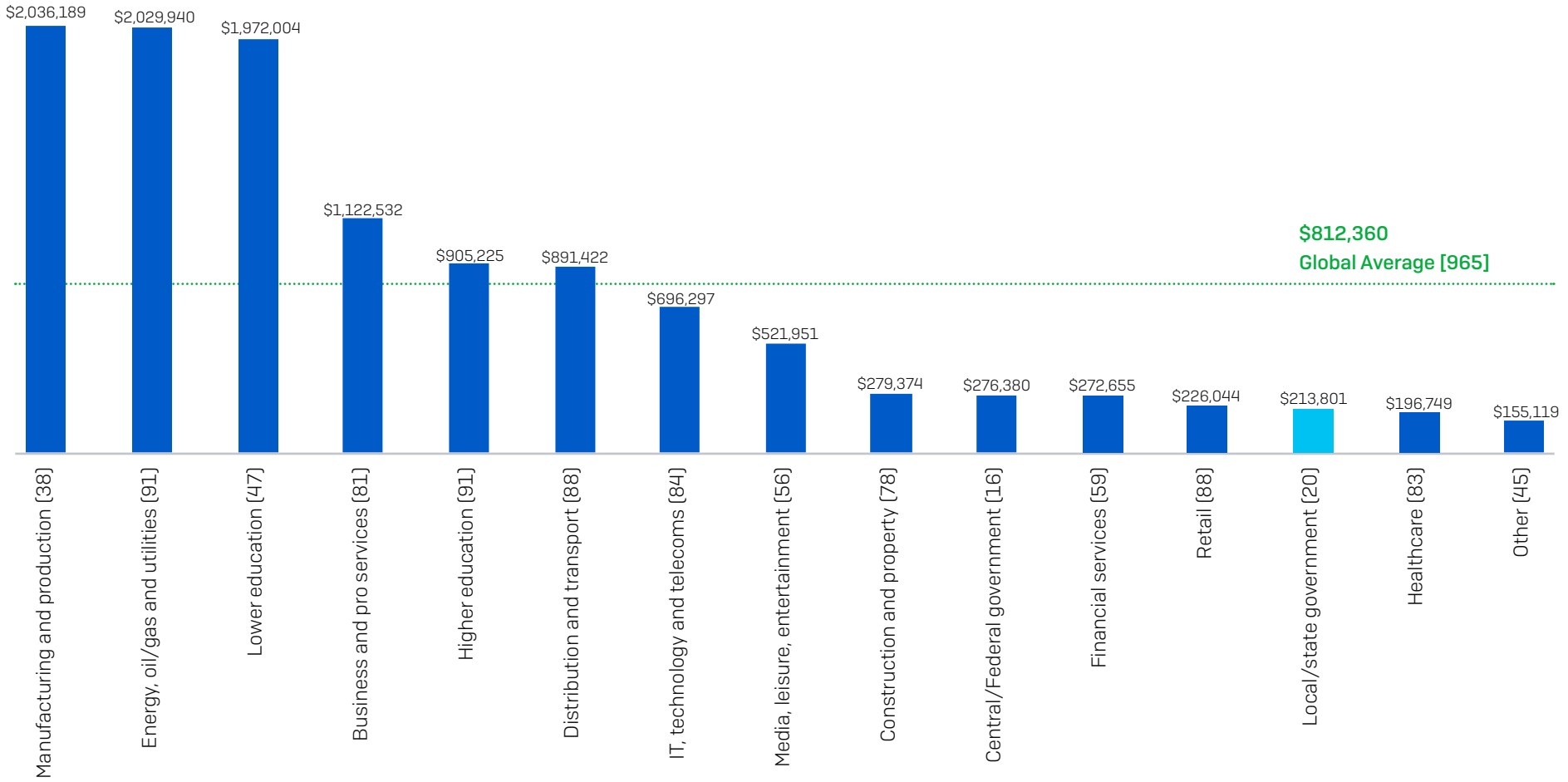
Did your organization get any data back in the most significant ransomware attack?
[n=2,398 organizations that had data encrypted]: Yes, we paid the ransom and got data back

Percentage of Encrypted Data Recovered After Paying the Ransom



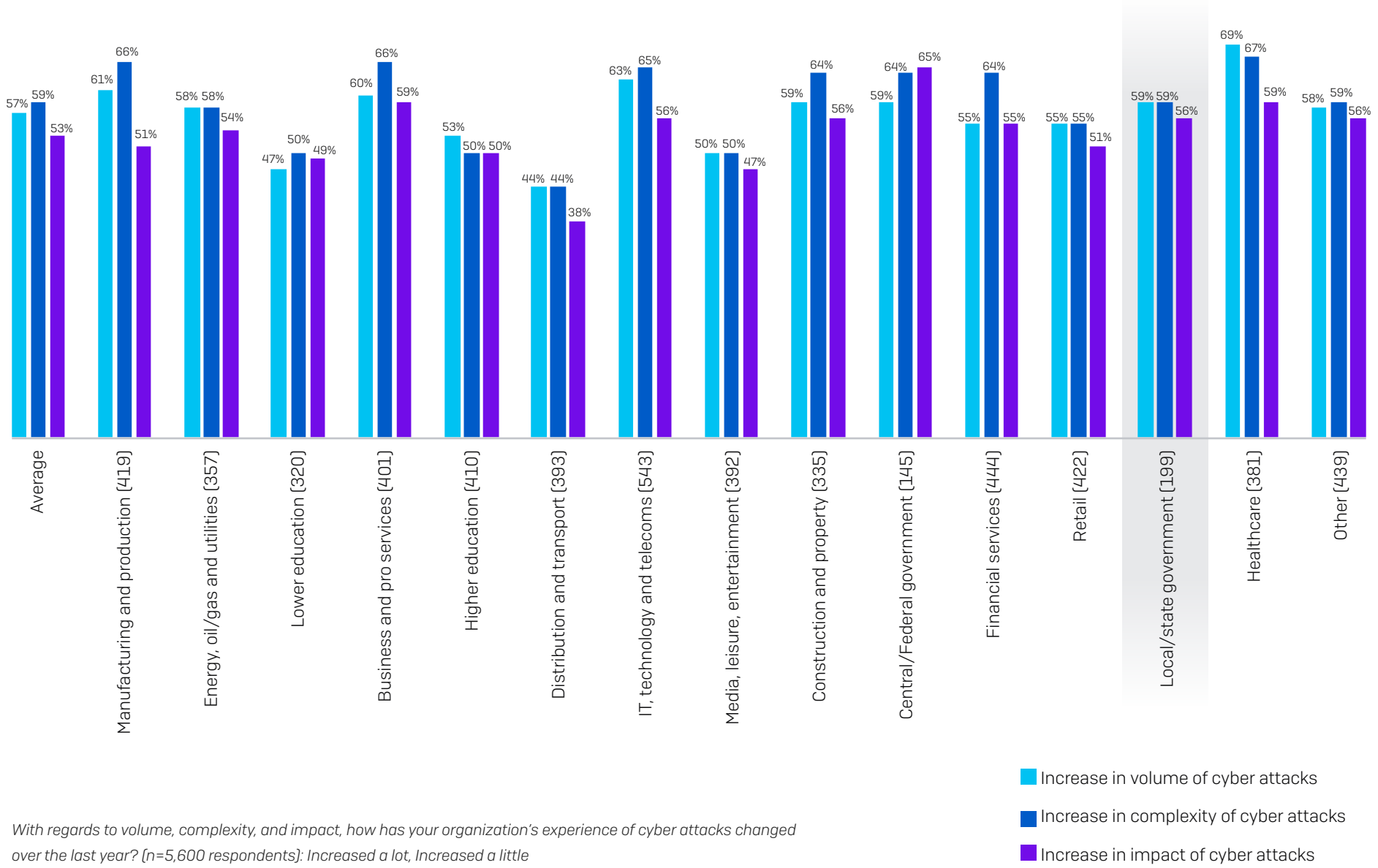
How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)

State and Local Government Made Low Ransom Payments



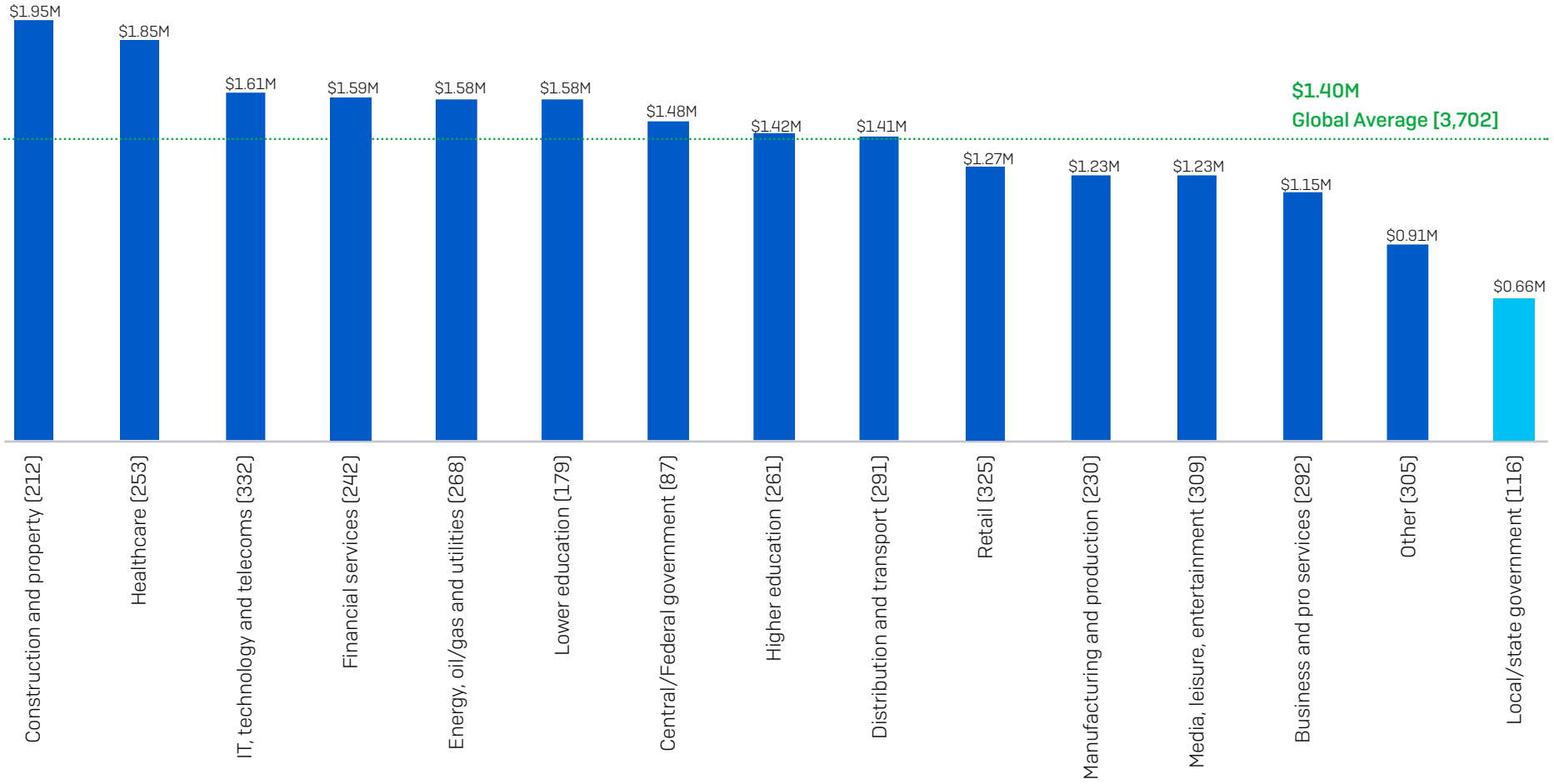
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses. N.B. For sectors with low base numbers, findings should be considered indicative.

How Government Stacks: Changing Experience of Attacks



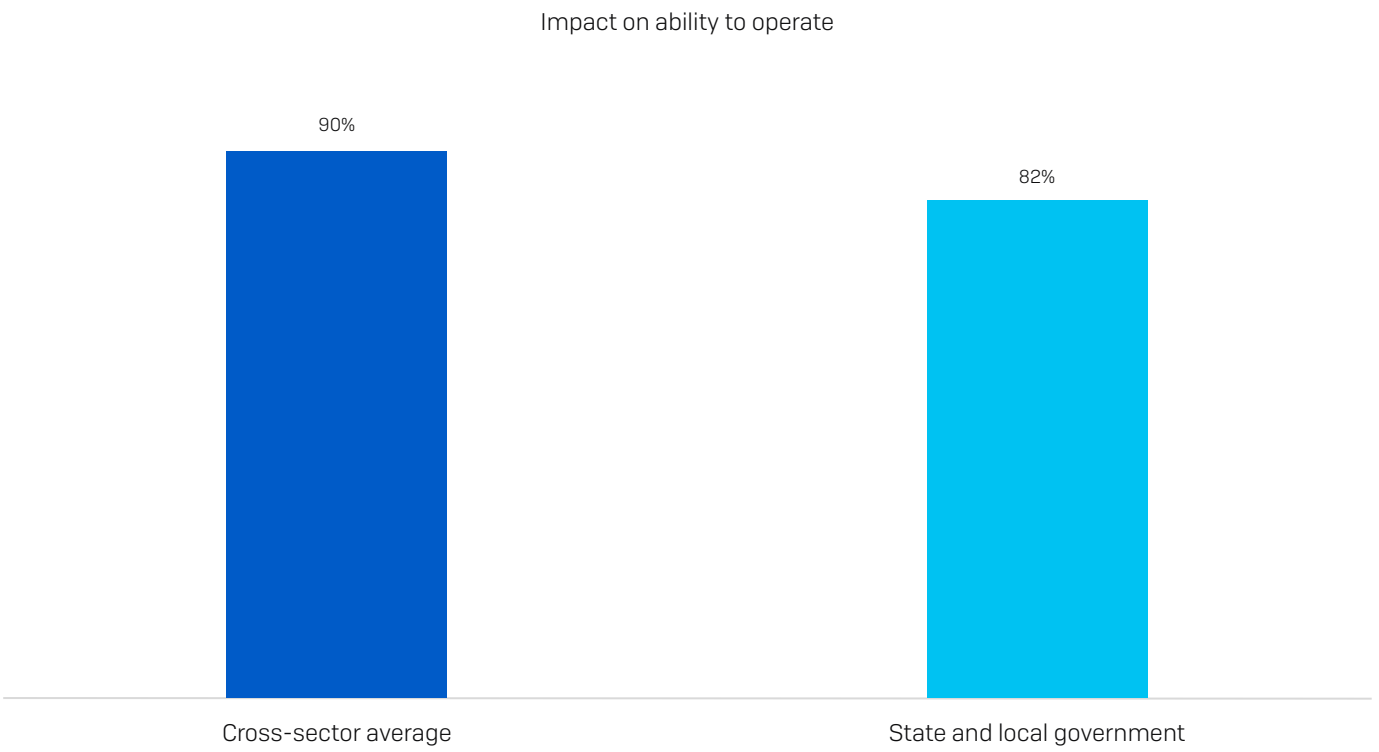
With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600 respondents): Increased a lot, Increased a little

Cost to Rectify Attacks in State/Local Government Organizations



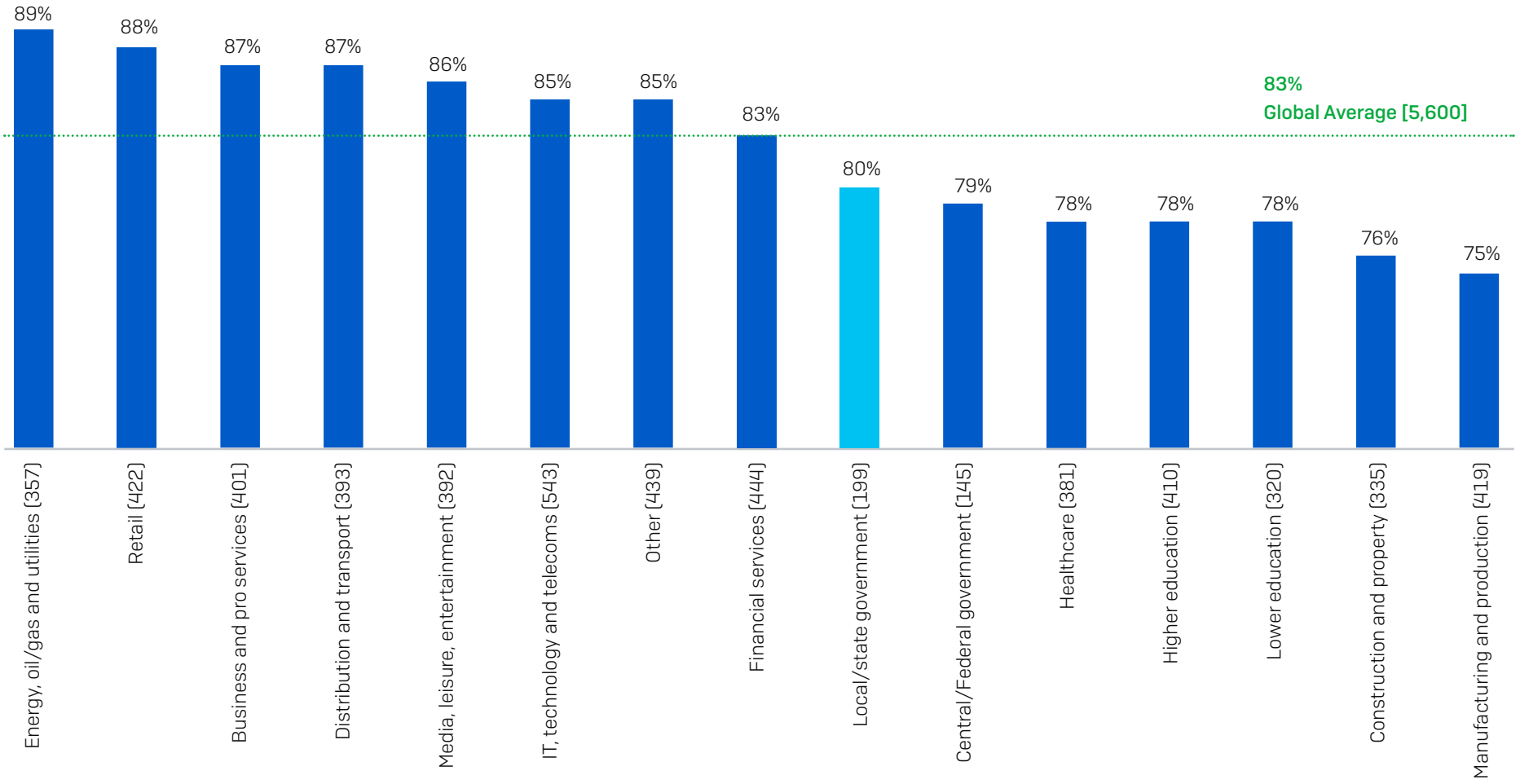
What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? (3,702 organizations that were hit by ransomware)

Operational Impact of Ransomware on Victims



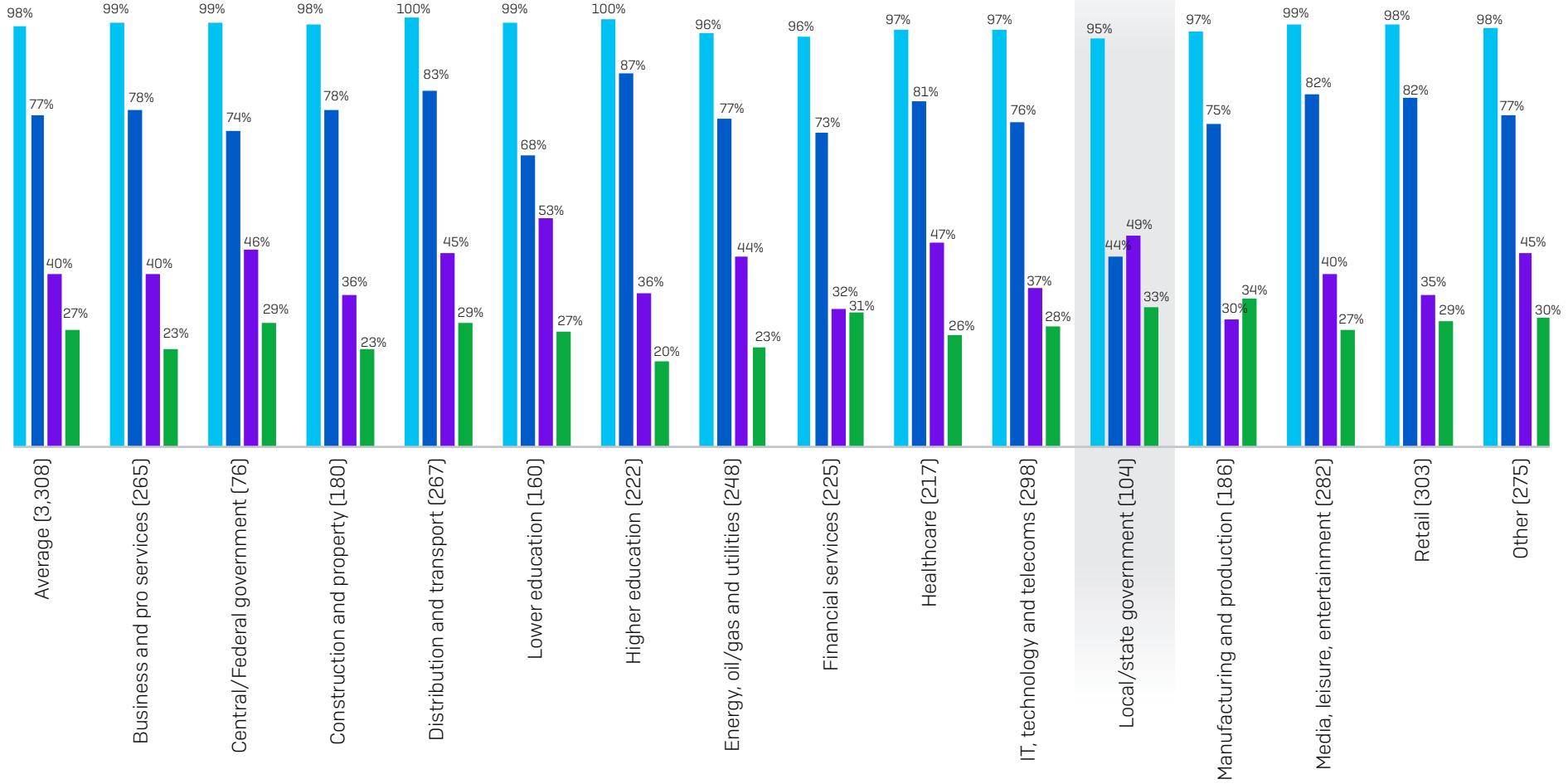
Did the most significant ransomware attack impact your organization's ability to operate? (n=3702; 116 local government organizations that were hit by ransomware in the previous year) Excluding some answer options.

State and Local Government Has Low Cyber Insurance Coverage for Ransomware



Does your organization have cyber insurance that covers it if it is hit by ransomware? (base numbers in chart). Yes; Yes, but there are exceptions/exclusions in our policy

How Local/State Government Stacks: Cyber Insurance Payout Rate by Sector



Did the cyber insurance pay out to address the costs associated with the most significant ransomware attack that your organization suffered? (n=3,308 organizations that were hit by ransomware in the previous year and had cyber insurance cover against ransomware). Yes, it paid clean-up costs (e.g. cost to get the organization back up and running); Yes, it paid the ransom; Yes, it paid other costs (e.g. cost of downtime, lost opportunity etc.)

Learn more about ransomware and how Sophos can help you defend your organization.

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.

2022-09-19 (WP-PC)

SOPHOS