SOPHOS
Cybersecurity delivered.

# The State of Ransomware in Retail 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 422 respondents from the retail sector.

*A Sophos Whitepaper. September 2022*

# Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in the retail 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 the role insurance is playing in driving 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 422 from retail. 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 attacks are up over the last year

77% of retail organizations were hit by ransomware in 2021, up from 44% in 2020. This is a 75% rise over the course of a year, demonstrating that adversaries have become considerably more capable of executing attacks at scale. In fact, in 2021, retail reported the second highest rate of ransomware attacks of all 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.]

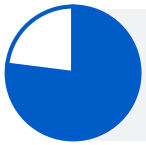
In addition to reporting an above-average rate of ransomware attacks, retail also had an above-average rate of data encryption with 68% of victims having data encrypted compared to a cross-sector average of 65%. Just 28% of retail respondents said they were able to stop the attack before the data could be encrypted, below the cross-sector average of 31%.

Interestingly, retail reported a considerable drop in extortion-only attacks, down from 12% in 2020 to 3% in 2021. While on the face of it this is good news, at Sophos we have seen an increase in adversaries combining both ransomware and extortion in an effort to increase the success rate of their campaigns. Therefore, this drop likely reflects a change in tactics by the adversaries rather than a move away from data extortion.

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

Over the last year, 55% of retail respondents reported an increase in the volume of cyberattacks, 55% reported an increase in attack complexity, and 51% reported an increase in the impact of attacks on their organization. While these numbers are concerning, they are all below the cross-sector average, indicating that retail was less affected than many other sectors.

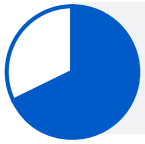
## Hit by ransomware



**77%**
retail organizations – second highest across sectors

**66%**
cross-sector average

## Data encrypted in the attack



**68%**
retail organizations

**65%**
cross-sector average

## 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 |
|---|---|---|---|
| Retail | 55% | 55% | 51% |
| Cross-sector average | 57% | 59% | 53% |

# Most retail victims get some encrypted data back

As ransomware has become more prevalent, organizations have gotten better at dealing with the aftermath of an attack. Almost all (99%) retail organizations hit by ransomware and that had data encrypted in the last year got some encrypted data back.

Backups were the #1 method used to restore encrypted data. Almost three in four (73%) retail organizations whose data was encrypted used this approach in 2021, a considerable increase from the 56% that used backups in 2020.

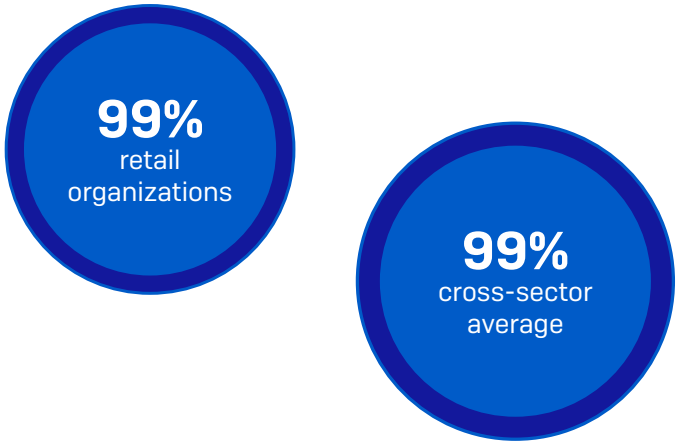
Despite the strong backup use, 49% of respondents in retail reported paying the ransom to get the data back. This ransom payment rate is above the cross-sector average of 46% in 2021 and a considerable increase from the 32% of retail respondents that reported paying the ransom in 2020. In addition, almost a third (32%) reported using other means to restore their data.

The percentage using backups, paying the ransom, and using other means clearly add up to more than 100%, indicating that many retail organizations use multiple restoration methods in parallel. Overall, 46% of retail victims used multiple methods to restore their data.

## Data restoration method

| | PAID THE RANSOM | USED BACKUPS | USED OTHER MEANS | MULTIPLE METHODS USED |
|---|---|---|---|---|
| Retail | 49% | 73% | 32% | 46% |
| Cross-sector average | 46% | 73% | 30% | 44% |

## Restored some encrypted data



## Less data is recovered after paying the ransom

On average, across all sectors, the average amount of data recovered after paying the ransom has dropped over the last year, coming in at 61% in 2021 - down from 65% in 2020. Retail experienced a similar downward trend with 62% of data being recovered on average in 2021, a drop from the 67% reported in 2020.

In parallel, the percentage of retail organizations that got ALL their data back also dropped, with just 5% restoring all their encrypted data in 2021 - down from 9% in 2020.

The key takeaway here is that paying the ransom will only restore a part of your encrypted data and you cannot count on the ransom payment to get you all your data back.

### Percentage of data restored after paying the ransom

**62%**
retail

**61%**
cross-sector average

### The percentage that got ALL data back after paying the ransom

**5%**
retail

**4%**
cross-sector average

# Retail made low ransom payments

Across all sectors, 965 respondents whose organization paid the ransom shared the exact amount, 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).

88 respondents from the retail sector shared the exact ransom payment made, and the average ransom payment by retail came in at $226,044.

While it is encouraging that this year's average ransom payment by retail is less than one-third of the cross-sector average, it represents a considerable increase from the $147,811 reported in 2020 by 36 retail respondents. It is clear that retail has not escaped the upward global trend in ransom payments over the last year.

Diving into the ransom payments further, over one-fifth (22%) of the retail organizations paid ransoms of less than US$1K, while over two-thirds (70%) paid a ransom amount of less than US$100K. These low payments help keep the sector average down compared to many other industries.

Furthermore, only 29% of retail respondents paid US$100K or more compared to 47% of all respondents globally. Just 4% in retail paid US$1M or more, considerably below the cross-sector average of 11%.

## Ransom paid by retail organizations

**US$226K** retail

**US$812K** cross-sector average

**22%**
paid less than US$1K

**70%**
paid less than US$100K

**29%**
paid US$100K or more

**4%**
paid US$1M or more

# Ransomware has a considerable financial, commercial, and operational impact on retail

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

92% of retail organizations hit by ransomware said the attack impacted their ability to operate (cross-sector average: 90%), while 89% said the attack caused their organization to lose business/revenue (cross-sector average: 86%). These data points indicate that the operational and commercial impact of ransomware on the retail sector was a little higher than the cross-sector average.

In terms of the overall cost 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.

In line with this trend, the overall cost to retail organizations to remediate a ransomware attack also dropped over the last year, down from US$1.97M in 2020 to US$1.27 in 2021.

There are several factors likely contributing to this below-average cost for retail. The first is the higher rate of cyber insurance coverage for this sector, which we will cover later in this report. Insurance providers are often skilled at guiding victims swiftly and effectively through the incident response process, reducing the remediation cost. Secondly, the below-average increase in the complexity and impact of ransomware attacks on retail has likely had a commensurate impact on recovery costs.

In terms of the time taken to recover from a ransomware attack, the recovery time in retail was in line with the cross-sector average, with just over half (53%) of retail organizations recovering within a week. Fewer than two in five (17%) retail respondents said it took them between one and six months to recover.

## Impact on the ability to operate

**92%**
retail

**90%**
cross-sector average

## Impact on business/revenue

**89%**
retail

**86%**
cross-sector average

## The average cost to remediate the most recent attack

**US$1.27M** retail

**US$1.40M** cross-sector average

## Time to recover from ransomware attacks

| DURATION | RETAIL | CROSS-SECTOR AVERAGE |
|---|---|---|
| Up to a week | 53% | 53% |
| 1-6 months | 17% | 20% |

## Retail has the second highest rate of cyber insurance coverage against ransomware

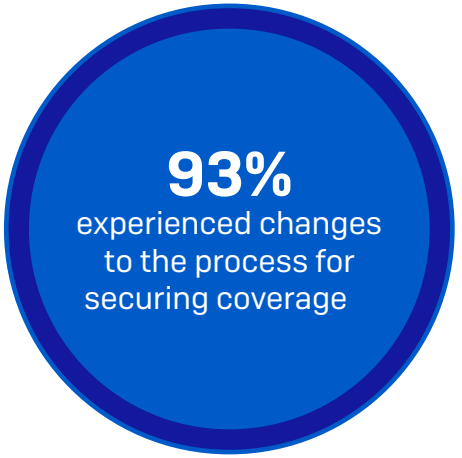
88% of retail respondents reported they have coverage against ransomware attacks, compared with a cross-sector average of 83%.

For 93% of those with cyber insurance in retail, the process for securing coverage changed over the last year:

- 41% said fewer insurance providers are offering cyber insurance
- 57% said the level of cybersecurity they need to qualify for cyber insurance is now higher
- 43% said policies are now more complex
- 37% said the process takes longer
- 35% 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, ransom attacks have increased and ransoms and payout costs have soared. As a result, some insurance providers have left the market as it has simply become unprofitable for them.

With fewer organizations providing cyber insurance coverage, it's a seller's market. They call the shots and they 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 will significantly improve an organization's ability to secure the necessary coverage.

# Cyber insurance is driving retail to improve cyber defenses

As the cyber insurance market hardens and it becomes more challenging to secure coverage, 97% of retail organizations that have cyber insurance have made changes to their cyber defense to improve their cyber insurance position:

- 66% have implemented new technologies/services
- 55% have increased staff training/education activities
- 53% 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 |
|---|---|---|---|---|
| **Retail** | 97% | 66% | 55% | 53% |
| **Cross-sector average** | 97% | 64% | 56% | 52% |

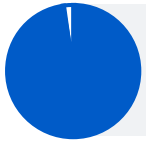
# Retail has below-average ransom payout rates

Across all sectors, cyber insurance almost always pays out towards some costs in the event of a ransomware attack. Retail organizations with cyber insurance against ransomware reported a 98% payout rate, in line with the cross-sector average.

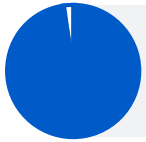
Retail reported that the insurance paid out for clean-up costs in 82% of attacks, above the cross-sector average of 77%. However, what is notable is that retail respondents reported a below-average rate of ransom payout with the insurer paying the ransom in 35% of attacks compared with 40% on average across all sectors. This suggests that the victims are often paying the ransoms out of their own funds.

It's worth remembering that while cyber insurance will help get you back to your previous state, it doesn't cover "betterment" i.e., you need to invest in better technologies and services to address the weaknesses that led to the attack.

## Insurance payout rate:

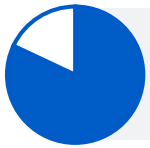


**98%**
retail



**98%**
cross-sector average

## Clean-up costs payout:



**82%**
retail

**77%**
cross-sector average

## Ransom payout:

**35%**
retail

**40%**
cross-sector average

## Conclusion

The ransomware challenge facing retail organizations continues to grow. The proportion of organizations hit by ransomware has increased considerably in twelve months, with cyber criminals succeeding in encrypting data in over half of the attacks.

In the face of this near-normalization of ransomware, retail organizations have gotten better at dealing with the aftermath of an attack: virtually everyone (99%) now gets some encrypted data back. Backups were the number one method used to restore encrypted data.

Retail has an above-average rate of ransom payment, with 49% paying compared to the cross-sector average of 46%. At the same time, the average ransom paid in this sector was less than a third of the cross-sector average. The proportion of encrypted data restored by retail after paying the ransom is slightly above average: 62% vs. 61%.

The overall cost to remediate a ransomware attack in retail fell over the last year (down from US$1.97M in 2020 to US$1.27 in 2021) and continues to be below the cross-sector average, which this year came in at US$1.4M.

Many retail organizations choose to reduce the risk 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. However, while retail has an above-average clean-up cost payout rate, the sector has a below-average ransom payout rate.

It is getting harder for retail organizations to secure cyber insurance coverage. This has driven almost all retail organizations to make changes to their cyber defenses to improve their cyber insurance position.

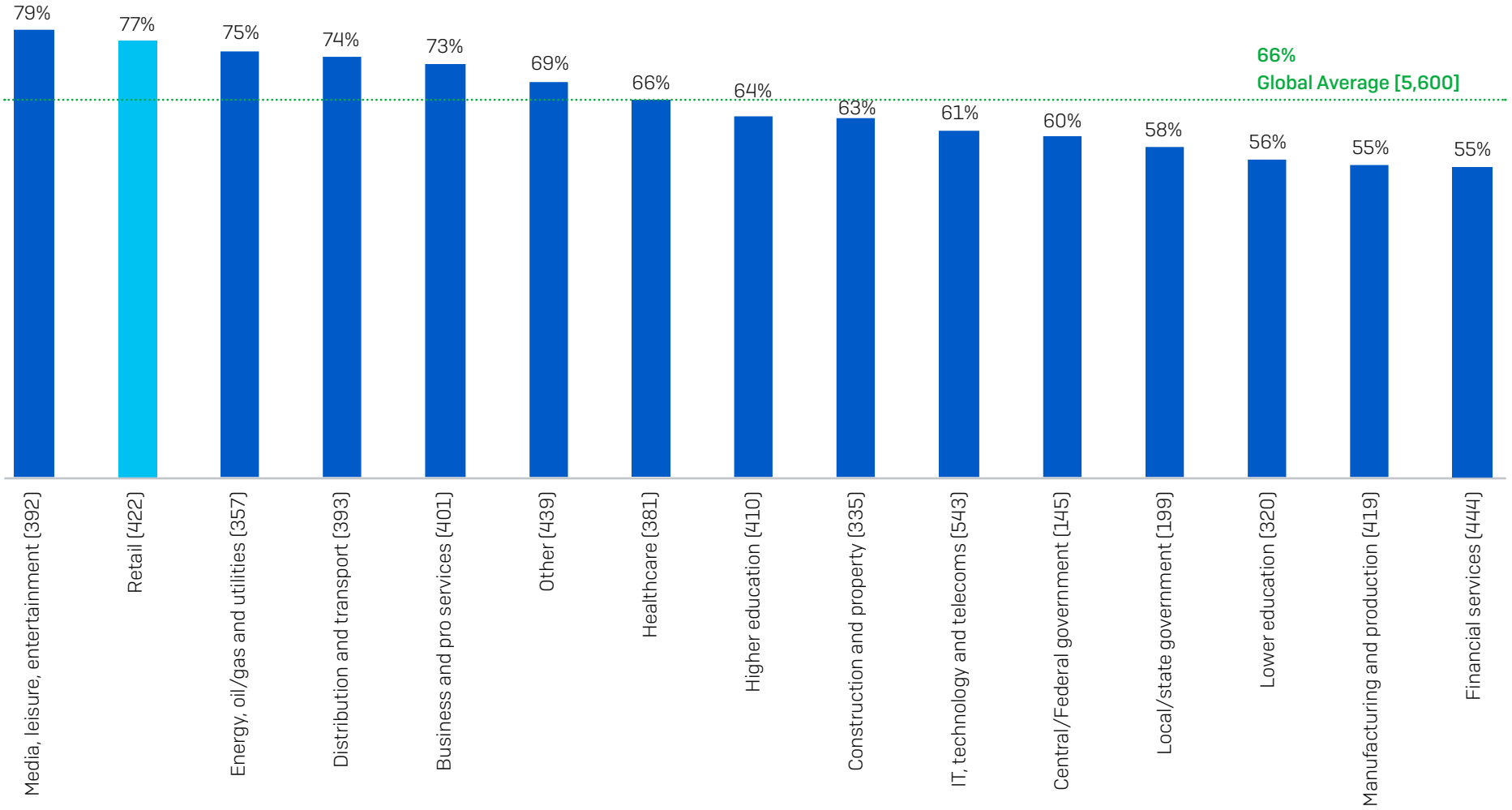
## Recommendations

In light of these findings, optimizing your ransomware defenses 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 their attack – if you don't have the time or skills in-house, work with a specialist MDR (managed detection and response) cybersecurity service.
- Harden your environment by searching for and closing down security gaps: unpatched devices, unprotected machines, open RDP ports, etc. 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.

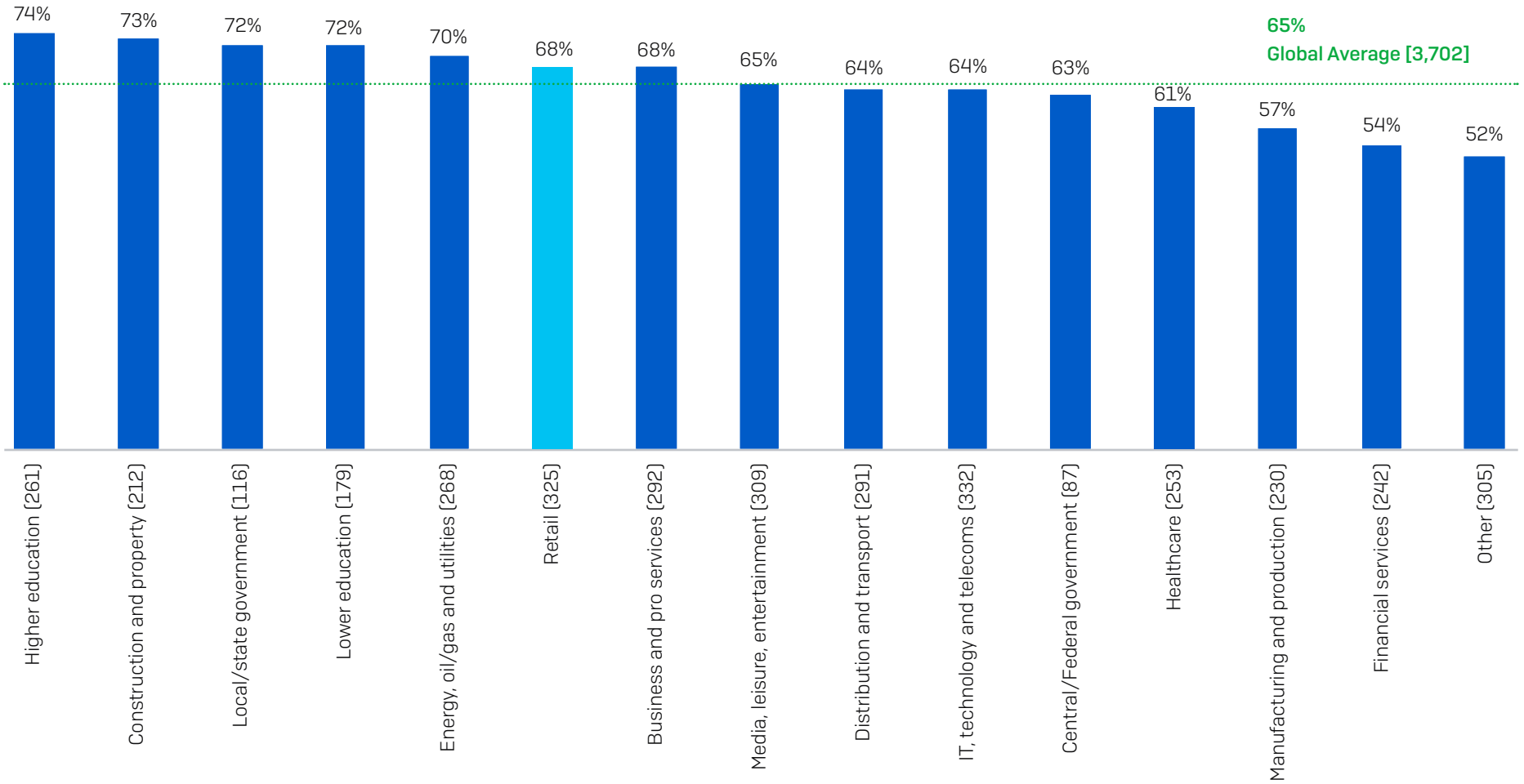
See the Sophos ransomware threat intelligence center for detailed information on individual ransomware groups.

# Retail Has One of the Highest Rates of Ransomware Attacks



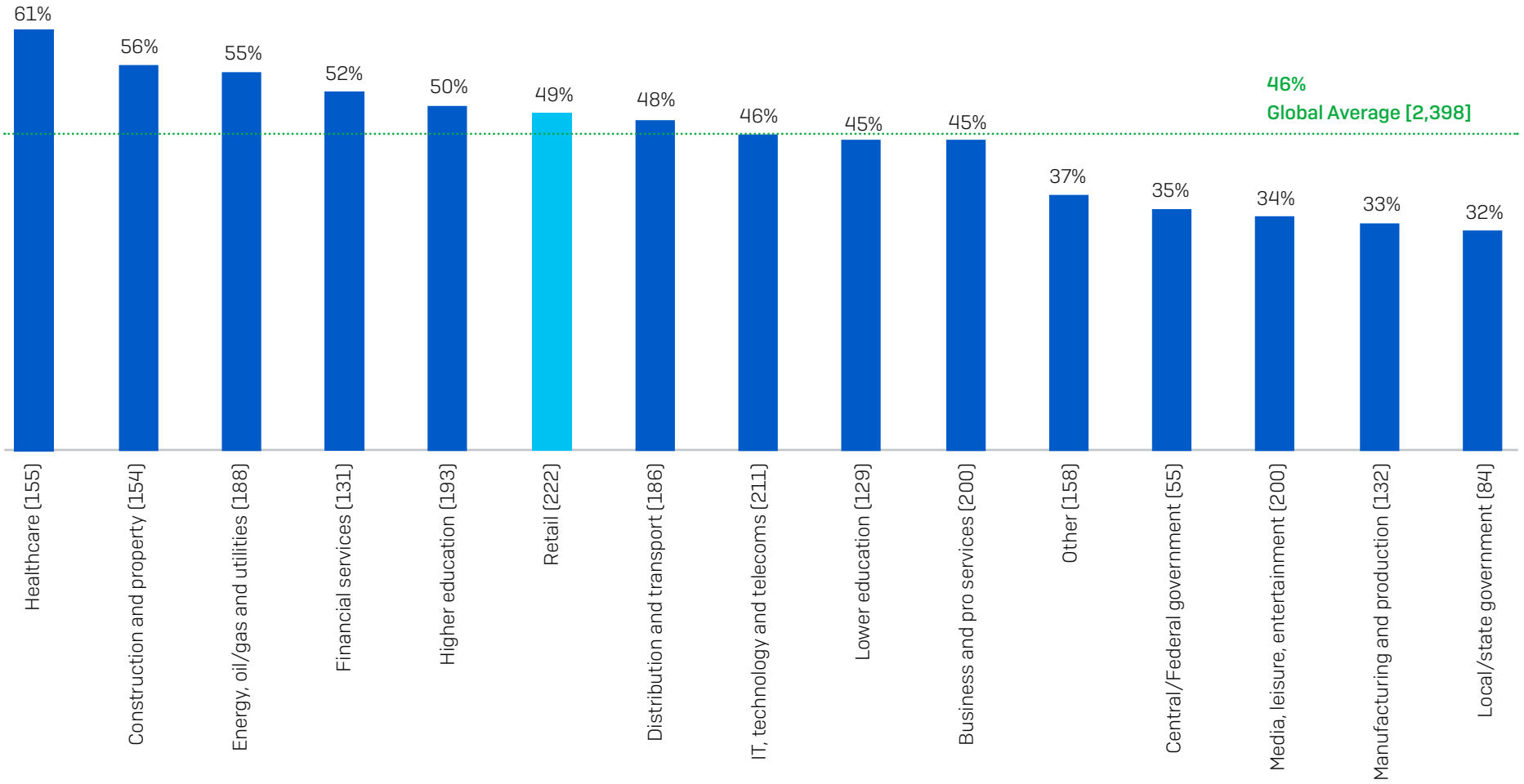

*In the last year, has your organization been hit by ransomware? (n=5,600): Yes*

# Retail Has Above-Average Encryption Rate



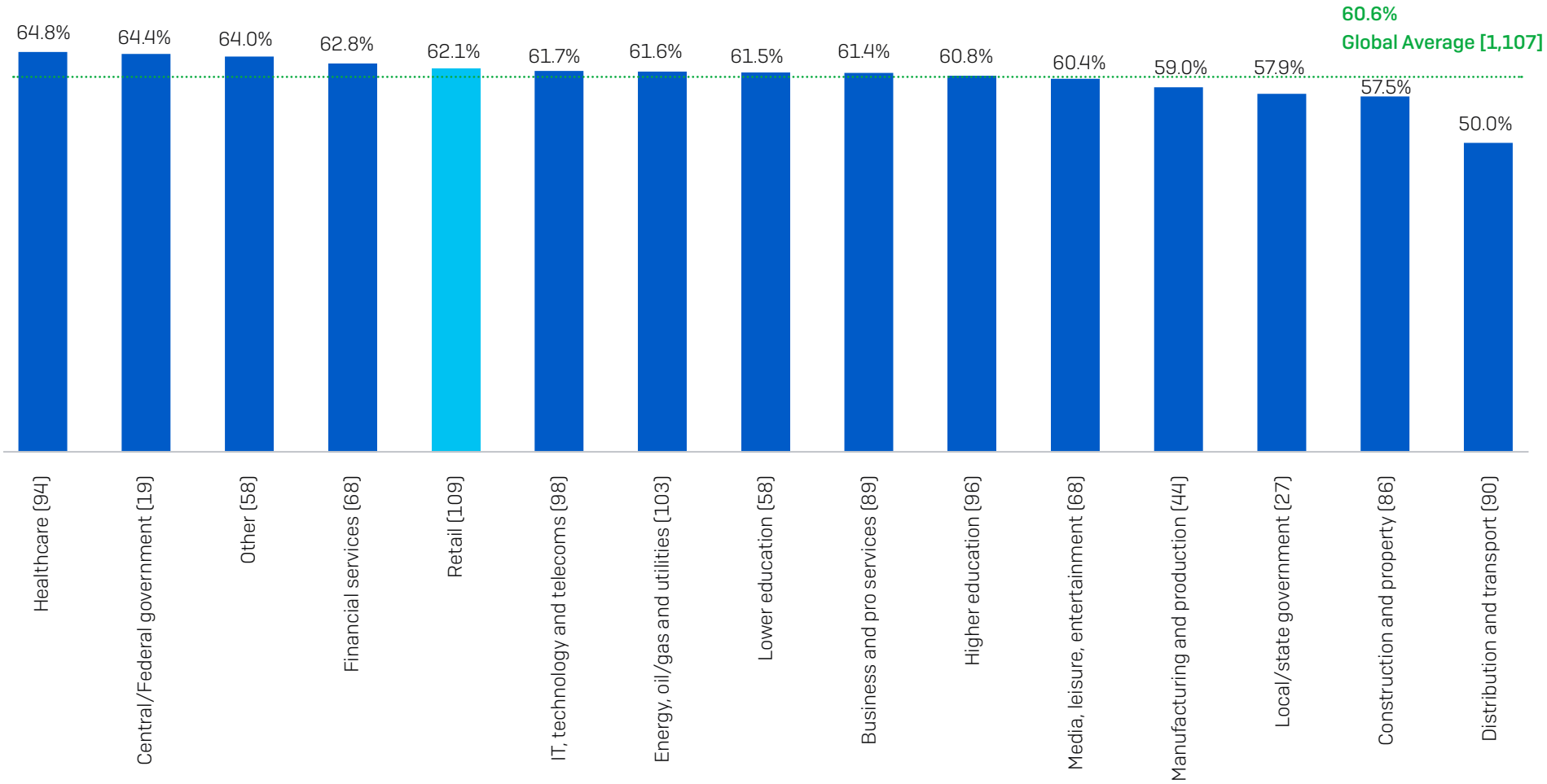

*Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes*

# Retail Ransom Payment Rate is Above Average




*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*

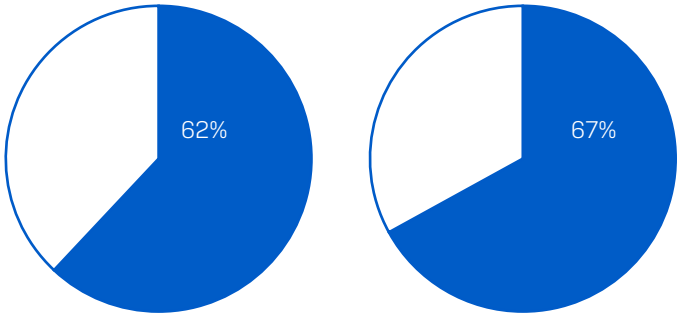
# Retail Got More Data Back Than Average After Paying the Ransom



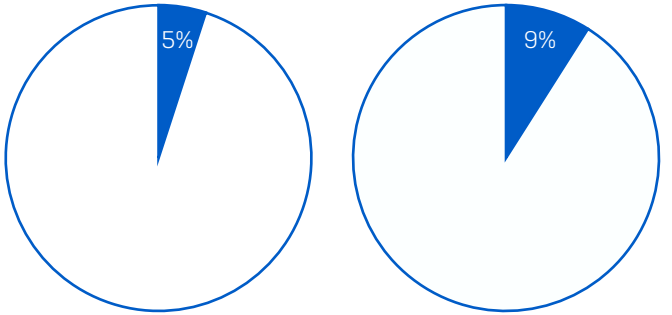

*How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)*

# Retail Organizations Recovered Less Data in the Last Year

## Percentage of data restored after paying the ransom

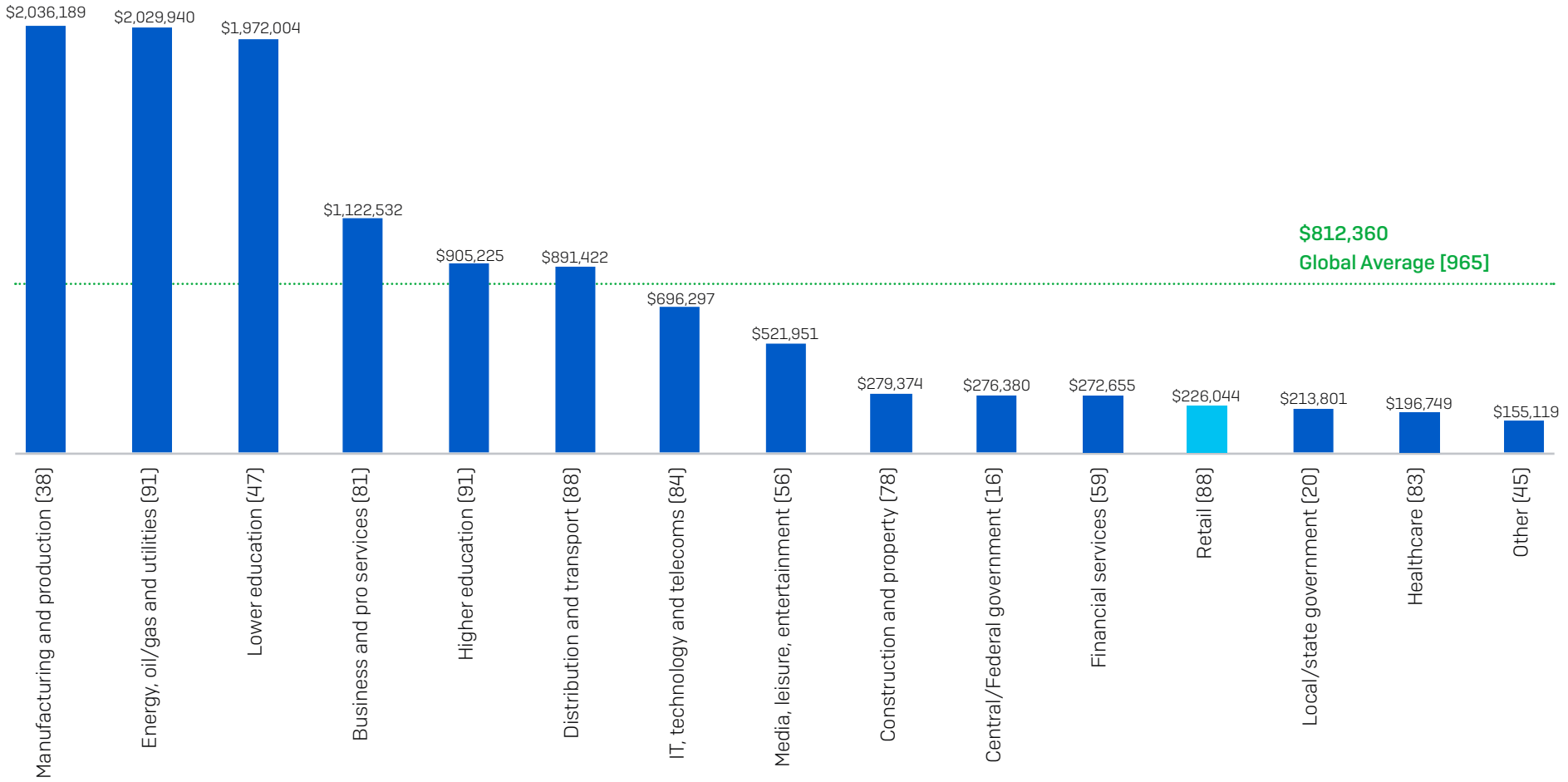



## Percentage that got ALL their data back after paying the ransom



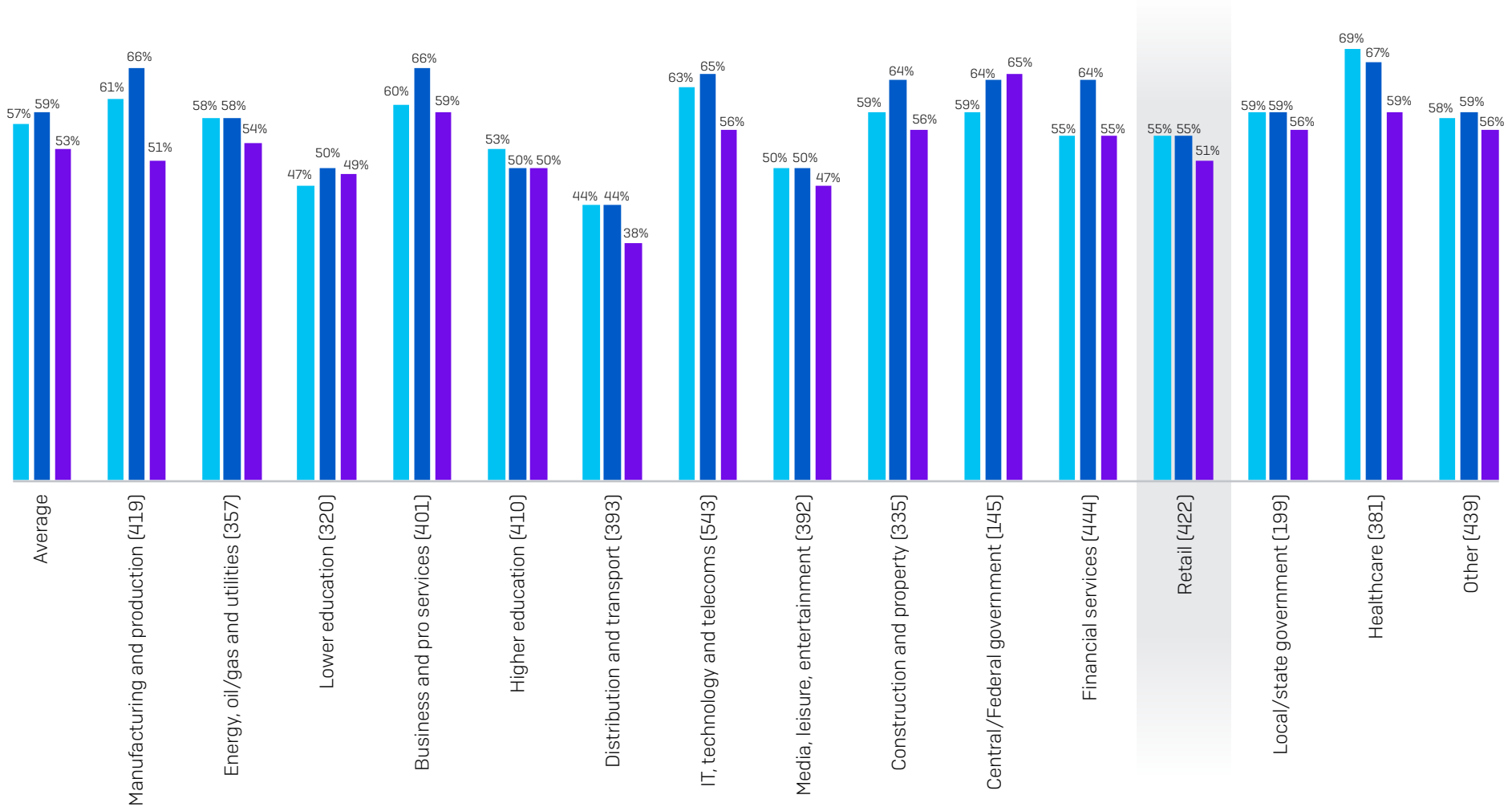

*How much of your organization's data did you get back in the most significant ransomware attack?*
*(109/ 33 retail organizations that paid the ransom and got data back)*

# Retail Made Low Ransom Payments



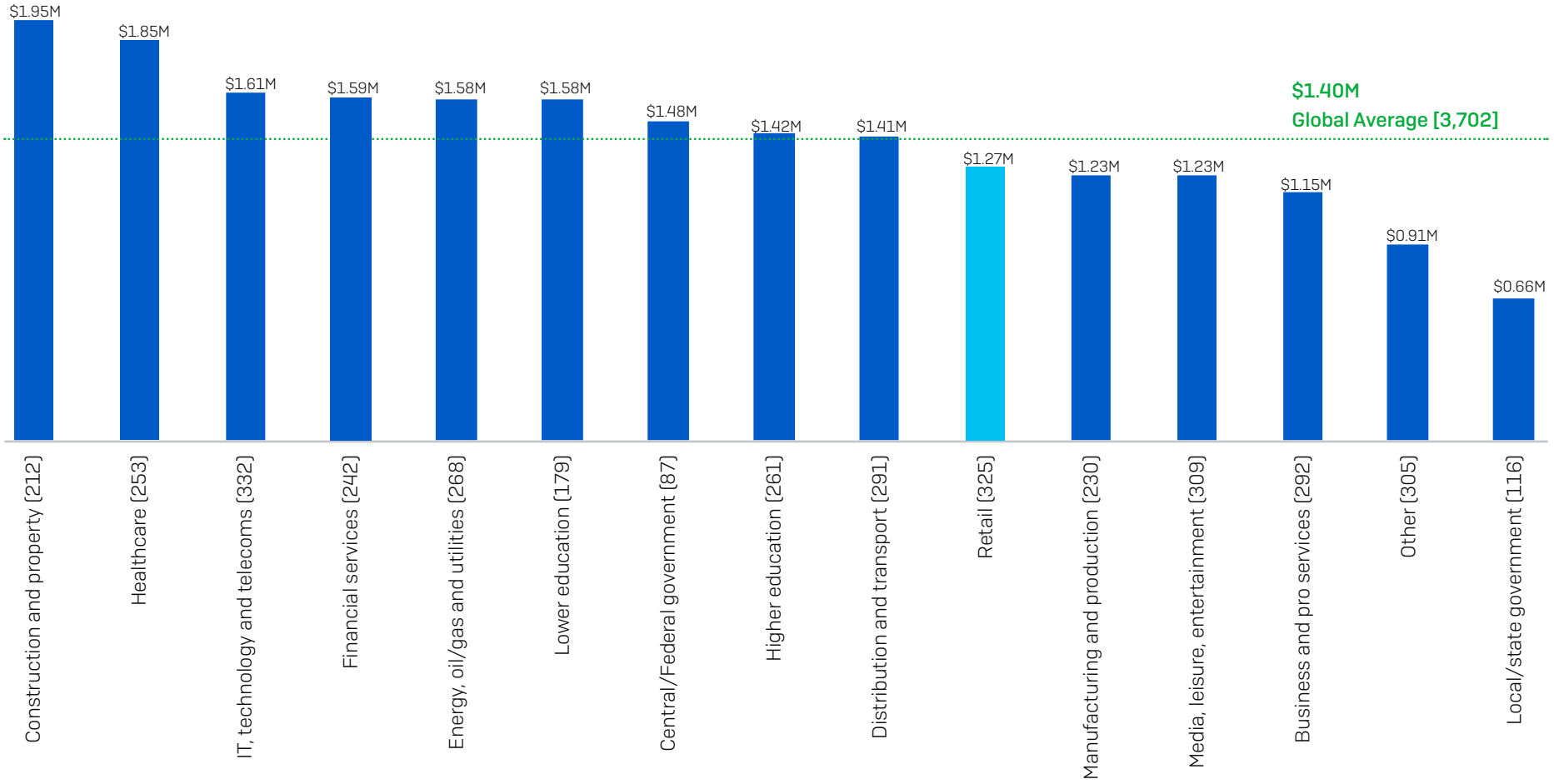

*How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses. N.B. For sectors with low base numbers, findings should be considered indicative.*

# How Retail Stacks: Changing Experience of Attacks



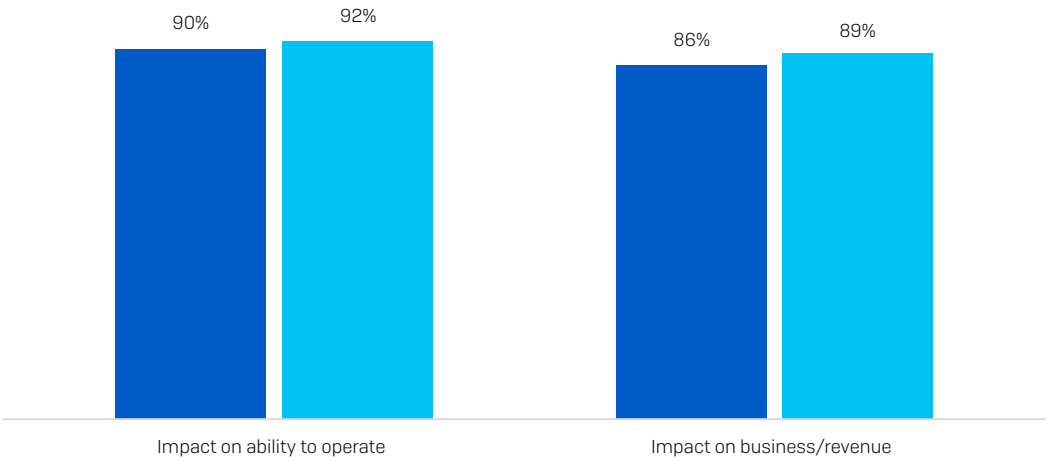

*With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600 respondents): Increased a lot, Increased a little*

# Retail Experiences Below-Average Cost to Rectify Attacks




*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)*

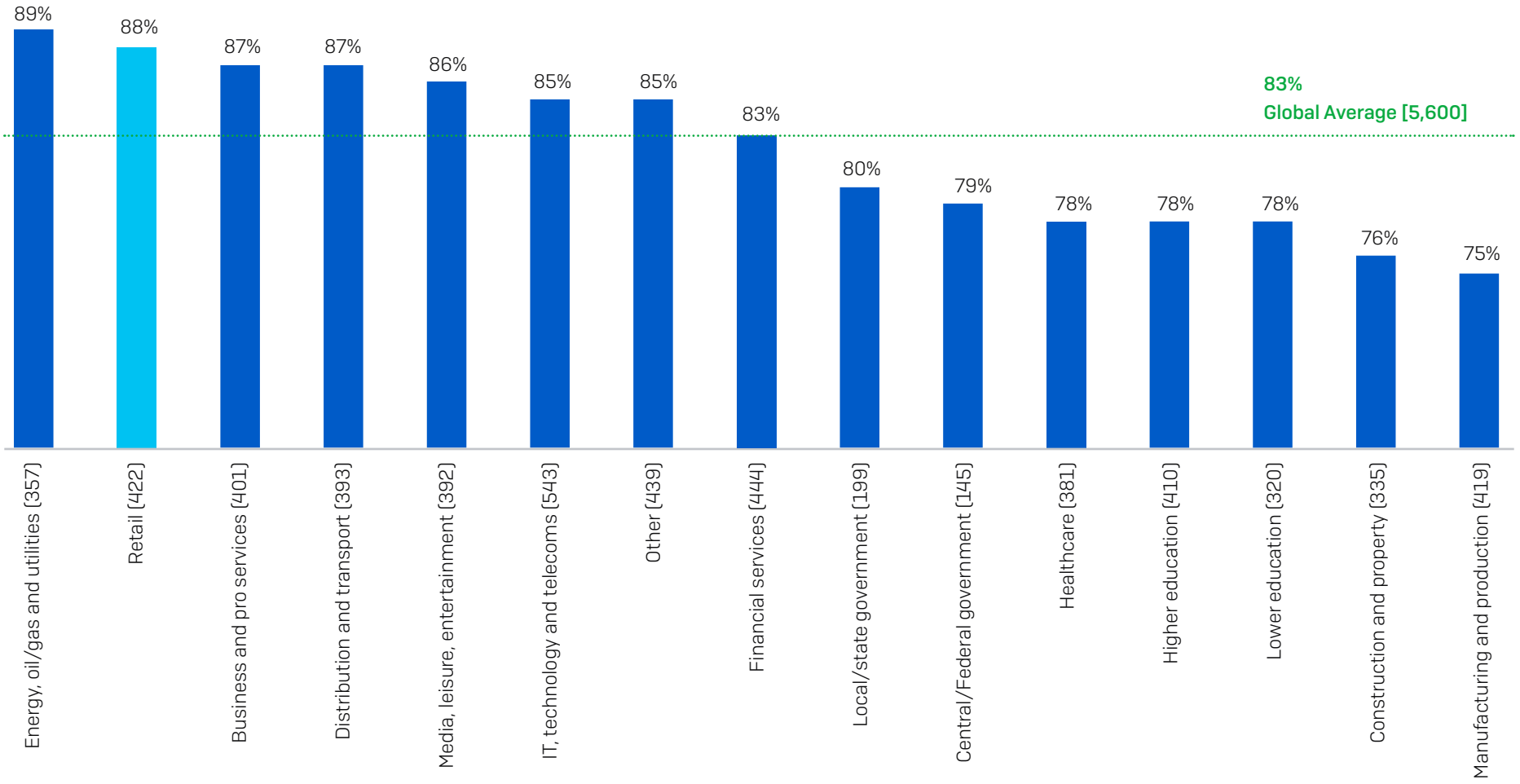
# Operational/Commercial Impact of Ransomware on Retail




Note: Only private sector organizations were asked about loss of business/revenue.

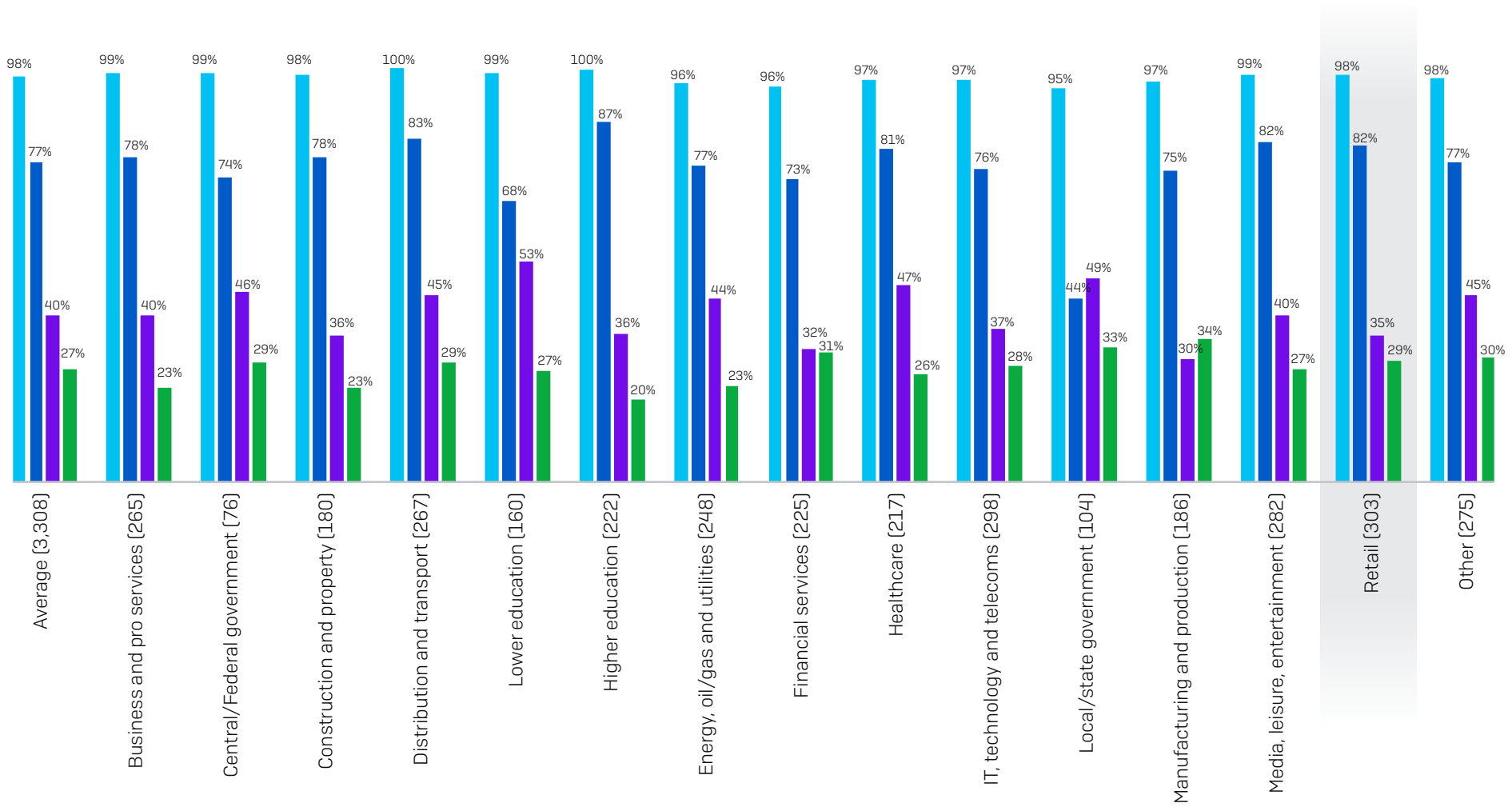
*Did the most significant ransomware attack impact your organization's ability to operate? Did the most significant ransomware attack cause your organization to lose business/revenue? (n=3702; 325 retail organizations that were hit by ransomware in the previous year) Excluding some answer options.*

# Retail Has the Second Highest Cyber Insurance Coverage Rate 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 Retail 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.



2022-08-16 (WP-PC)

SOPHOS