SOPHOS
Cybersecurity delivered.

The State of Ransomware in Manufacturing and Production 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 419 respondents from the manufacturing and production sector.

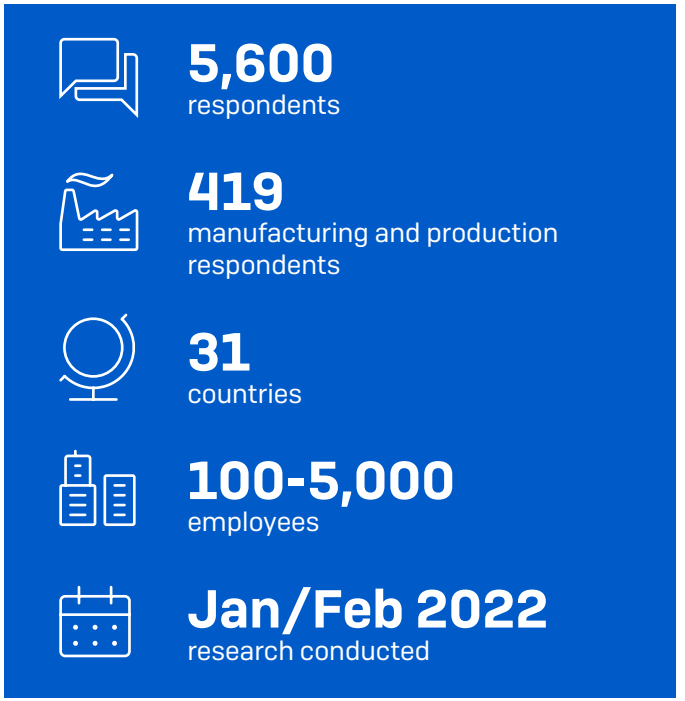
A Sophos Whitepaper. October 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in the manufacturing and production 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 419 from manufacturing and production. 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 have increased over the last year

55% of manufacturing and production organizations were hit by ransomware in 2021, up from 36% in 2020. This is a 52% increase over the course of a year, demonstrating that adversaries have become considerably more capable of executing the most significant attacks at scale. [Note: hit by ransomware was defined as one or more devices being impacted but not necessarily encrypted.]

Manufacturing and production, in fact, reported the lowest rate of ransomware attacks (joint with financial services) across all sectors in 2021. But with over half of the respondents in every sector reporting being hit last year, the reality is that all organizations are more likely to experience an attack than not.

Over half (57%) of manufacturing and production organizations hit by ransomware reported that cybercriminals encrypted their data. Again, this was the lowest rate reported across all sectors. For comparison, across all sectors, the average data encryption rate was 65%.

38% of manufacturing and production respondents said they were able to stop an attack before data could be encrypted – better than the cross-sector average of 31%. This may be a positive result of changes that organizations in this sector made to improve their cyber insurance positions, such as implementing new technologies, increasing staff training, and changing processes. We will explore this further later in the report.

The rise in successful ransomware attacks is part of an increasingly challenging threat environment that has affected organizations across all sectors. Respondents across all sectors reported an increase in cyber attack volume, complexity, and/or impact.

Manufacturing and production has been particularly impacted by the changing threat landscape, with 61% of respondents reporting an increase in the volume of attacks on their organizations over the last year (vs. 57% cross-sector average) and 66% reporting an increase in attack complexity (vs. 59% cross-sector average).

It may be that the sector's superior ability to stop data encryption has forced adversaries to up their games when it comes to attacks. Alternatively, it may simply reflect an increased focus on the sector by cyber criminals over the last year.

In terms of the changing impact of attacks on manufacturing and production, just over half (51%) reported an increase in the last year, which is in line with the cross-sector average.

Hit by ransomware

55%
of manufacturing and production organizations – lowest across sectors

66%
cross-sector average

Data encrypted in the attack

57%
of manufacturing and production 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
Manufacturing and production	61%	66%	51%
Cross-sector average	57%	59%	53%

Most 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 (96%) manufacturing and production organizations hit by ransomware and that had data encrypted in the last year got some encrypted data back.

Manufacturing and production organizations reported the lowest level of backup use across all sectors, with just 58% of respondents using this approach to restore encrypted data compared to the cross-sector average of 73%. This sector also reported a decrease in backup use compared with the previous year, when 68% of manufacturing and production organizations used backups for data restoration. This is a concerning finding as backups are essential for recovery from ransomware and many other incidents.

Interestingly, the low rate of backup use did not result in a high rate of ransom payments. The sector also reported one of the lowest rates of ransom payment in 2021, with just one in three manufacturing and production respondents (33%) paying ransom. That said, this is almost double the 19% in manufacturing and production that paid ransom in 2020.

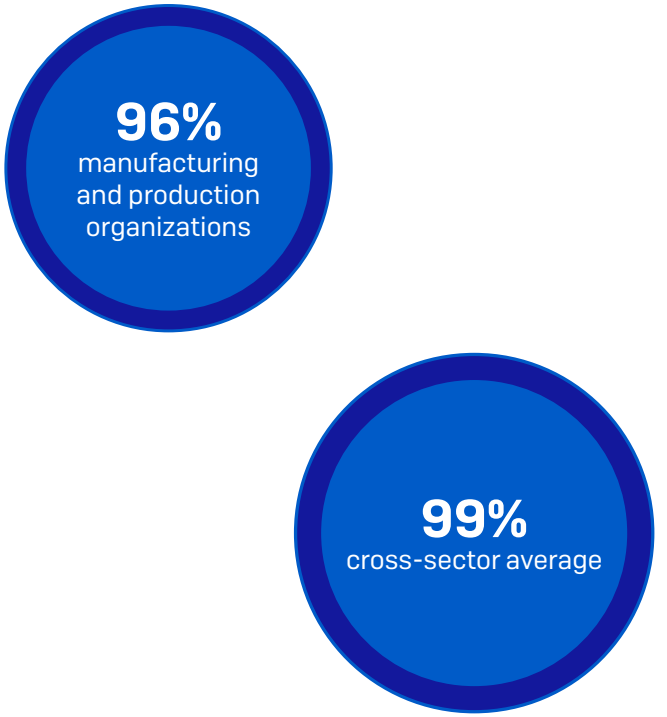
Furthermore, almost half of respondents (48%) reported using other means to restore their data.

The percentage using backups, paying ransom, and using other means clearly adds up to more than 100%, indicating that many manufacturing and production organizations use multiple restoration methods in parallel to accelerate incident recovery. Overall, 36% of manufacturing and production victims used multiple methods to restore their data.

Used multiple restoration methods

	PAID THE RANSOM	USED BACKUPS	USED OTHER MEANS	MULTIPLE METHODS USED
Manufacturing and production	33%	58%	48%	36%
Cross-sector average	46%	73%	30%	44%

Restored some encrypted data



Less data is recovered after paying the ransom

Across all sectors, the average amount of data recovered after paying ransom has dropped over the last year, coming in at 61% in 2021 - down from 65% in 2020. Defying this global trend, manufacturing and production respondents saw the amount of data recovered actually increase slightly over the year: from 55% in 2020 to 59% in 2021. While this increase is encouraging, the fact remains that, on average, respondents still got less than two-thirds of their encrypted data back.

At the same time, the percentage of manufacturing and production organizations that got ALL their data back remained constant at 7% year over year.

The key takeaway here is that paying the ransom might result in only partial restoration of encrypted data. It's unlikely that all encrypted data will be successfully restored.

Percentage of data restored after paying the ransom

59%
manufacturing and production

61%
cross-sector average

The percentage that got ALL data back after paying the ransom

7%
manufacturing and production

4%
cross-sector average

Manufacturing and production made highest ransom payments

Across all sectors, 965 respondents whose organization 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).

38 respondents from manufacturing and production shared the exact ransom payments made, revealing that the average ransom came in at a huge $2,036,189 – the highest of all sectors. This is a tremendous increase from the $147,917 reported in 2020 by 15 manufacturing and production respondents. Note: The 2020 average ransom figure is based on a low response base and should be considered indicative rather than statistically significant.

Diving into the ransom payments further, manufacturing and production has one of the broadest spreads of ransoms across all sectors, with respondents reporting a wide range of payments: one in ten (11%) paid less than US$1K while nearly one-third of the respondents (37%) paid more than US$100K. 8% of respondents paid above US$1M or more.

While a number of very high-value ransoms have pushed the overall average up, there is clearly an upward trend in payments year over year.

Ransom paid by manufacturing and production organizations:

US$2,036K manufacturing and production

US$812K cross-sector average

11%
paid less than US$1K

37%
paid more than US$100K

8%
paid US$1M or more

Ransomware has a considerable impact on manufacturing and production

Ransom sums are just part of the story, as the impact of ransomware affects organizations far beyond encrypted databases and devices.

77% of manufacturing and production organizations hit by ransomware said attacks impacted their ability to operate (cross-sector average: 90%), while 71% said attacks caused their organizations to lose business/revenue (cross-sector average: 86%). Although these numbers are below the cross-sector average, they reflect the considerable impact of ransomware on operations and revenue.

Impact on the ability to operate

77%
manufacturing and production

90%
cross-sector average

Impact on business/revenue

71%
manufacturing and production

86%
cross-sector average

The cost to remediate ransomware attacks has decreased

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

In line with this trend, the overall cost to remediate ransomware attacks for manufacturing and production organizations dropped over the last year, down from US$1.52M in 2020 to US$1.23 in 2021. Having said that, US$1.23M is still a very large sum that likely has a material impact on SMB organizations in any sector.

At first sight, it may seem counter-intuitive that the average recovery bill is less than the average ransom payment. However, in many cases, insurance providers cover ransom payments.

There are several factors likely contributing to the below-average recovery bills for manufacturing and production. First is the lower-than-average impact of ransomware on the operations and revenue of this sector. Secondly, the sector's impressive ability to stop the attacks before data is encrypted helps keep remediation costs low. Finally, as we will see further on in this report, manufacturing and production reported the highest insurance payout rate for certain costs associated with attacks (costs of downtime and lost opportunities, etc.) which likely had a commensurate impact on the total recovery costs for this sector.

In terms of the time taken to recover from ransomware attacks, the manufacturing and production sector reported quick recovery, with two-thirds of victims (67%) getting back up and running within a week. This is considerably higher than the global cross-sector average (53%), indicating that manufacturing and production is well-placed to recover from attacks.

Further demonstrating this point, just 10% in manufacturing and production said it took them between one and six months to recover, compared to the global average of 20% who recovered within this time.

The average cost to remediate the most recent attack

US$1.23M manufacturing and production

US$1.40M cross-sector average

Time to recover from ransomware attacks

DURATION	MANUFACTURING AND PRODUCTION	CROSS-SECTOR AVERAGE
Within a week	67%	53%
1-6 months	10%	20%

Cyber insurance coverage against ransomware

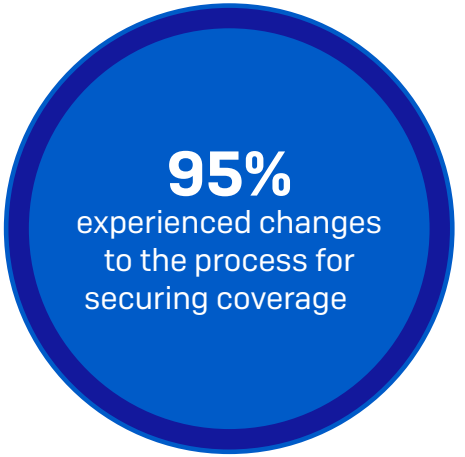
Only 75% of manufacturing and production respondents reported having coverage against ransomware attacks, compared with a cross-sector average of 83%. This leaves many organizations exposed to the high costs of ransomware recovery.

The cyber insurance market has hardened over the last year. 95% of those with cyber insurance in manufacturing and production experienced changes in the processes for securing coverage:

- 35% said fewer insurance providers are offering cyber insurance
- 56% said the level of cybersecurity needed to qualify for cyber insurance is now higher
- 53% said policies are now more complex
- 30% said the process takes longer
- 42% 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, 97% of manufacturing and production organizations that have cyber insurance have made changes to their cyber defense to improve their cyber insurance position:

- 70% have implemented new technologies/ services – highest across all sectors
- 63% have increased staff training/education activities – highest across all sectors
- 59% have changed processes/behaviors

The percentage that implemented new technologies and services and increased staff, training, and education is the highest across all sectors. This improves organizations' insurance positions, elevates their cyber defenses, and decreases the likelihood of falling victim to costly attacks.

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
Manufacturing and production	97%	70%	63%	59%
Cross-sector average	97%	64%	56%	52%

Manufacturing and production has below-average ransom pay-out rates

Across all sectors, cyber insurance almost always pays out towards some costs in the event of a ransomware attack. In fact, manufacturing and production organizations with cyber insurance reported a 97% pay-out rate.

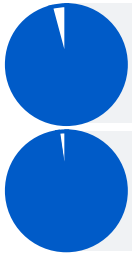
Diving into the details, the sector reported the pay-out rate for clean-up costs at 75%, which is in line with the global average of 77%.

However, what is notable is that the sector reported the lowest rate of ransom pay-out of all industries: 30% vs the 40% global average. This low pay-out rate is likely linked to the overall low ransom payment rate by the sector. However, given that manufacturing and production reported the highest average ransom, organizations in this sector should make sure they have the coverage they need in their insurance policies.

Furthermore, the sector reported the highest pay-out rate for other costs involved in attacks, like the costs of downtime and lost opportunities. The pay-out rate came in at 34% compared with a global average rate of 27%.

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:



97%
manufacturing and production

98%
cross-sector average

Clean-up costs payout:

75%
manufacturing and production

77%
cross-sector average

Ransom payout:

30%
manufacturing and production – lowest pay-out rate across sectors

40%
cross-sector average

Other costs pay-out:

34%
manufacturing and production – highest pay-out rate across sectors

27%
cross-sector average

Conclusion

The ransomware challenge facing manufacturing and production 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, manufacturing and production organizations have gotten better at dealing with the aftermath of attacks: virtually everyone (96%) now gets some encrypted data back. Backups were the number one method used to restore encrypted data. However, this sector reported the lowest rate of backup use across sectors.

Manufacturing and production reported one of the lowest rates of ransom payment, with 33% paying out compared to the global average of 46%. At the same time, the sector reported paying the highest average ransom amount at US$2,036,189. In comparison, the cross-sector average ransom was US$812,360.

The proportion of encrypted data restored by manufacturing and production after paying the ransom has increased from 2020. However, it remains below the global average, with 59% of data recovered compared to the cross-sector average of 61%.

In positive news, the overall costs to remediate ransomware attacks in manufacturing and production fell over the last year (down from US$1.52M in 2020 to US$1.23 in 2021) and remains below the global average of US$1.4M.

Many manufacturing and production organizations are choosing to reduce the risks associated with ransomware attacks by taking out cyber insurance coverage. For them, it's reassuring to know that insurers pay some costs in almost all claims. However, while the sector has the highest pay-out rate for "other costs" it also has the lowest ransom pay-out rate.

It's getting harder for manufacturing and production organizations to secure coverage. This has driven almost all manufacturing and production organizations to make changes to their cyber defenses in order to improve their cyber insurance positions. While the sector reported the lowest ratio of insurance coverage against ransomware across all sectors, it is heartening to know that the sector leads the way in terms of implementing new technologies and services and increasing staff training.

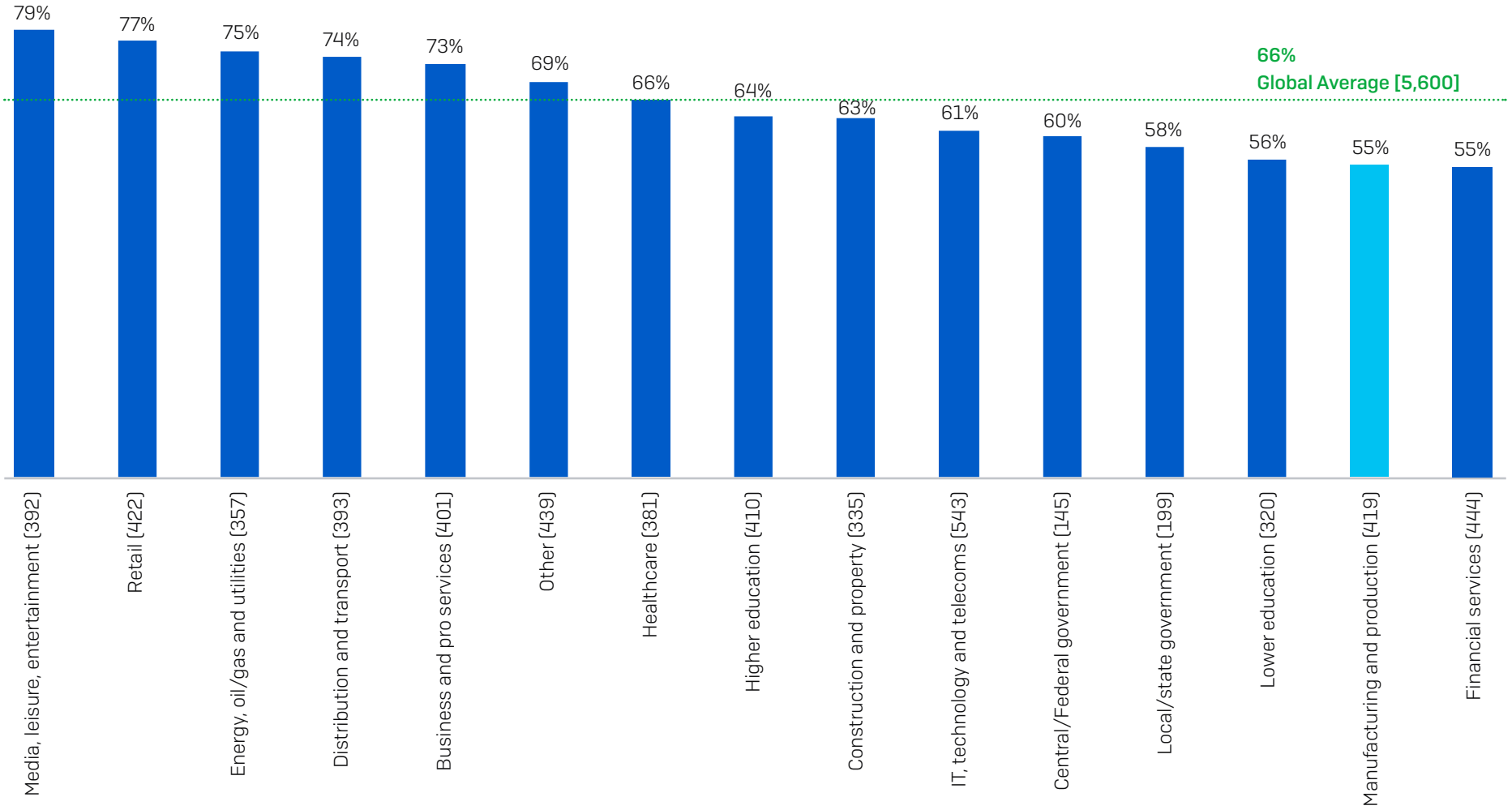
Recommendations

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.

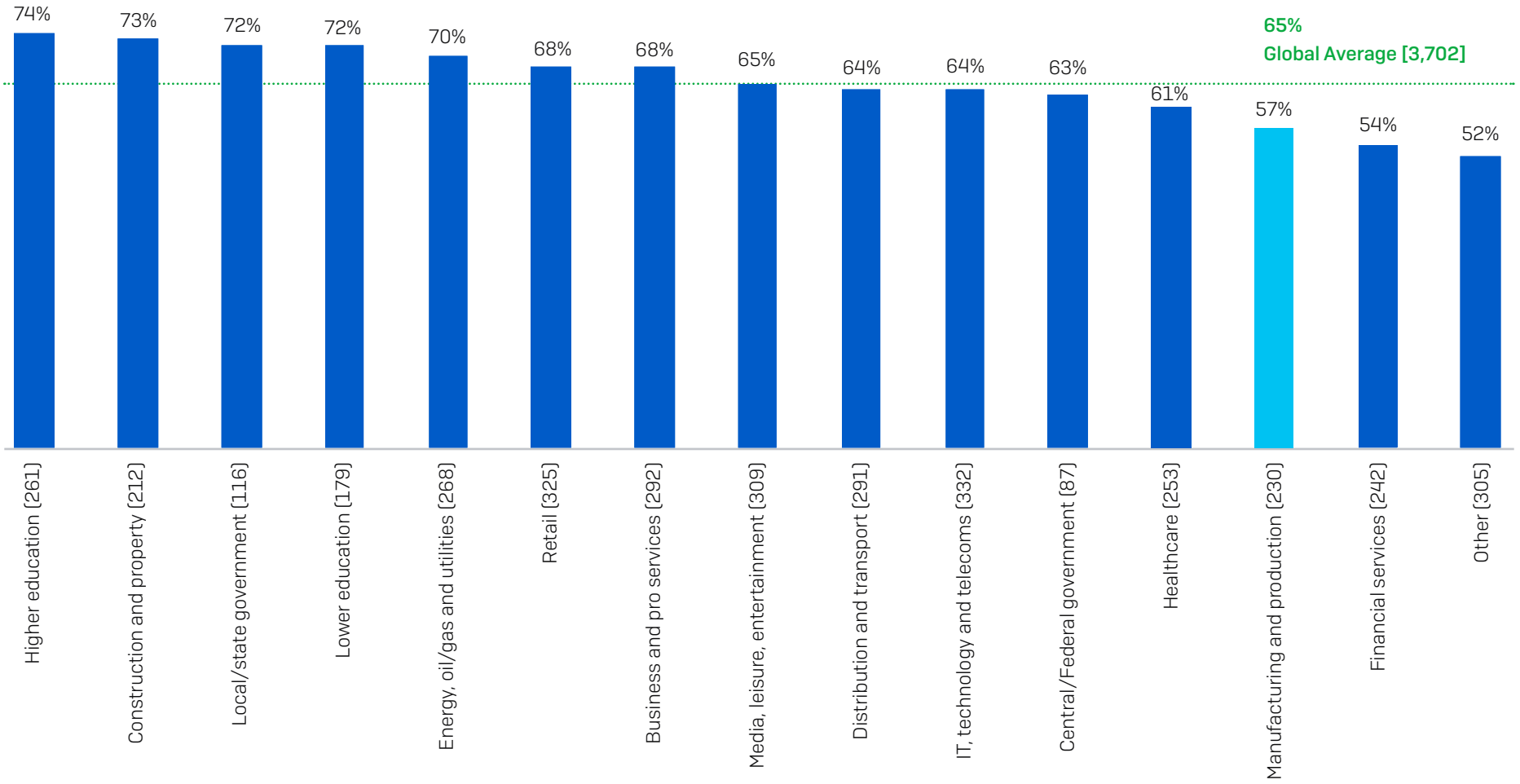
See the Sophos ransomware threat intelligence center for detailed information about individual ransomware groups.

Manufacturing and Production Has the Lowest Attack Rate



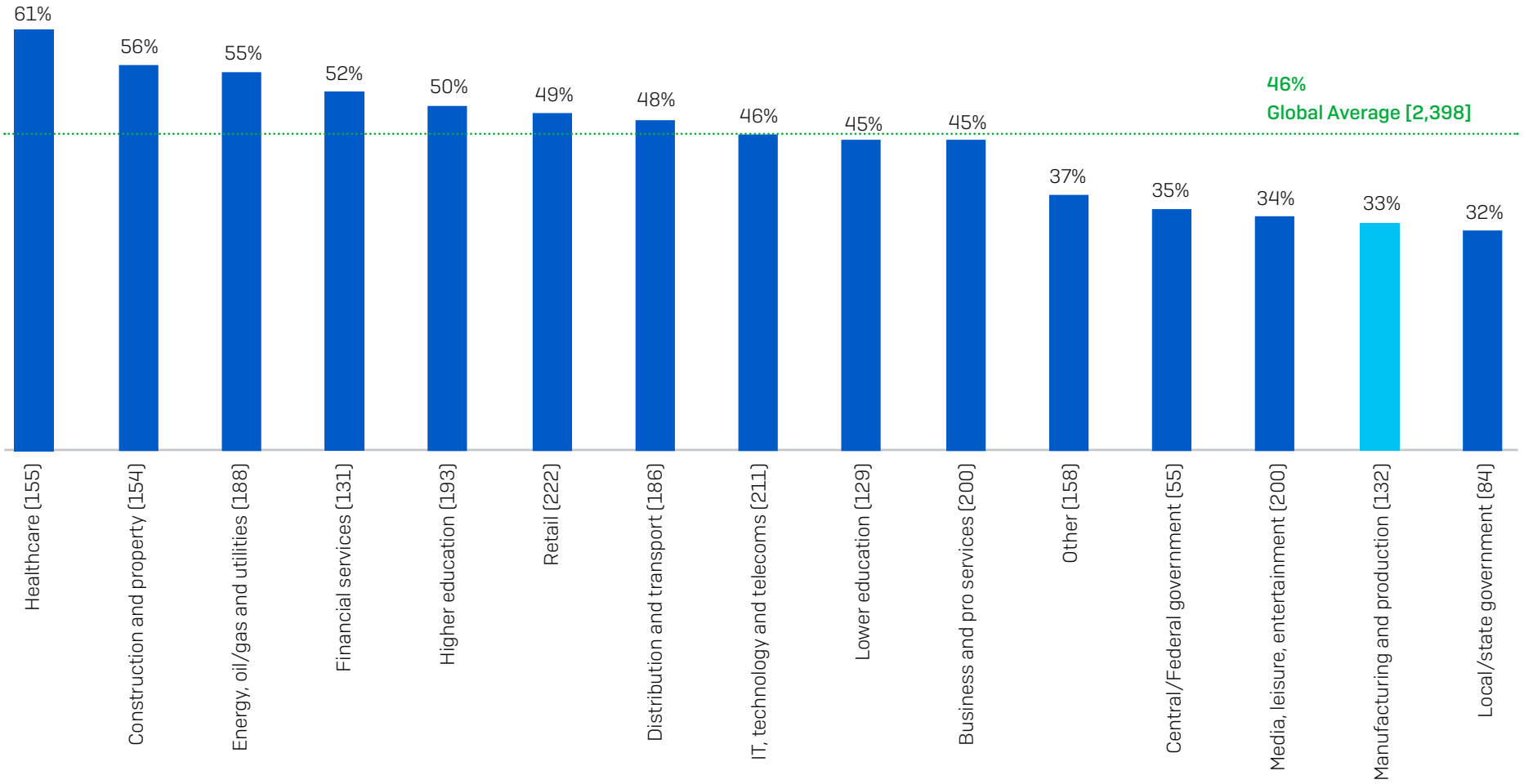
In the last year, has your organization been hit by ransomware? [n=5,600]

Manufacturing and Production Has Low Encryption Rate



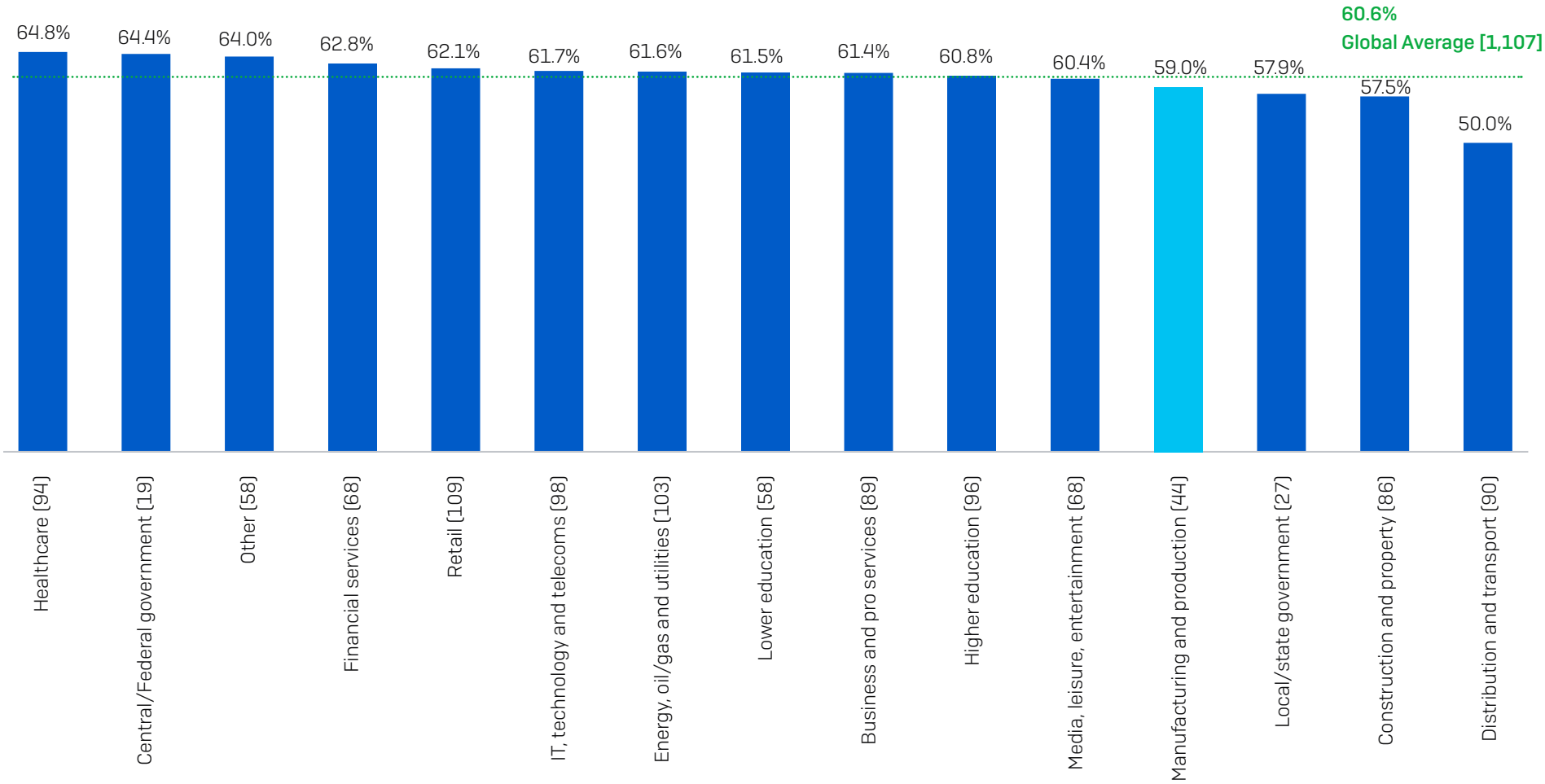
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

Manufacturing and Production Has One of the 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

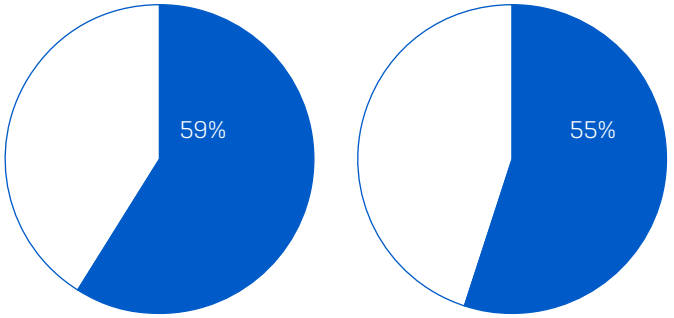
Data Restored After Paying the Ransom



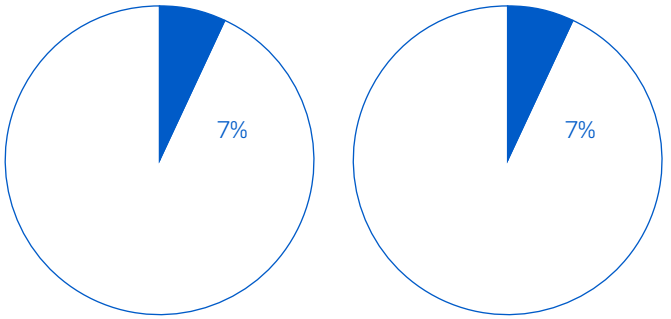
How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)

Data Recovered in the Last Year By Manufacturing and Production

Percentage of data restored after paying the ransom

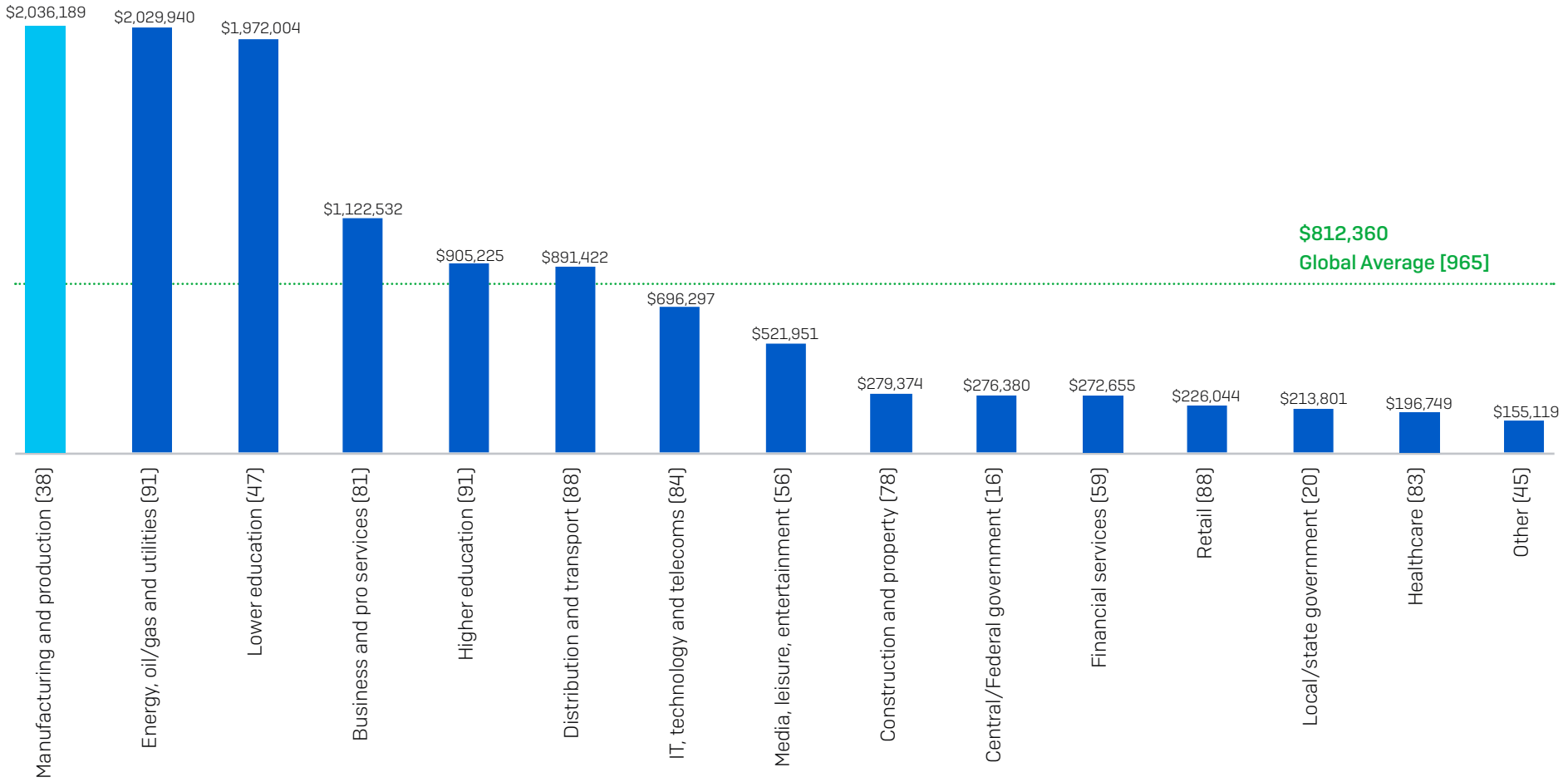


Percentage that got ALL their data back after paying the ransom



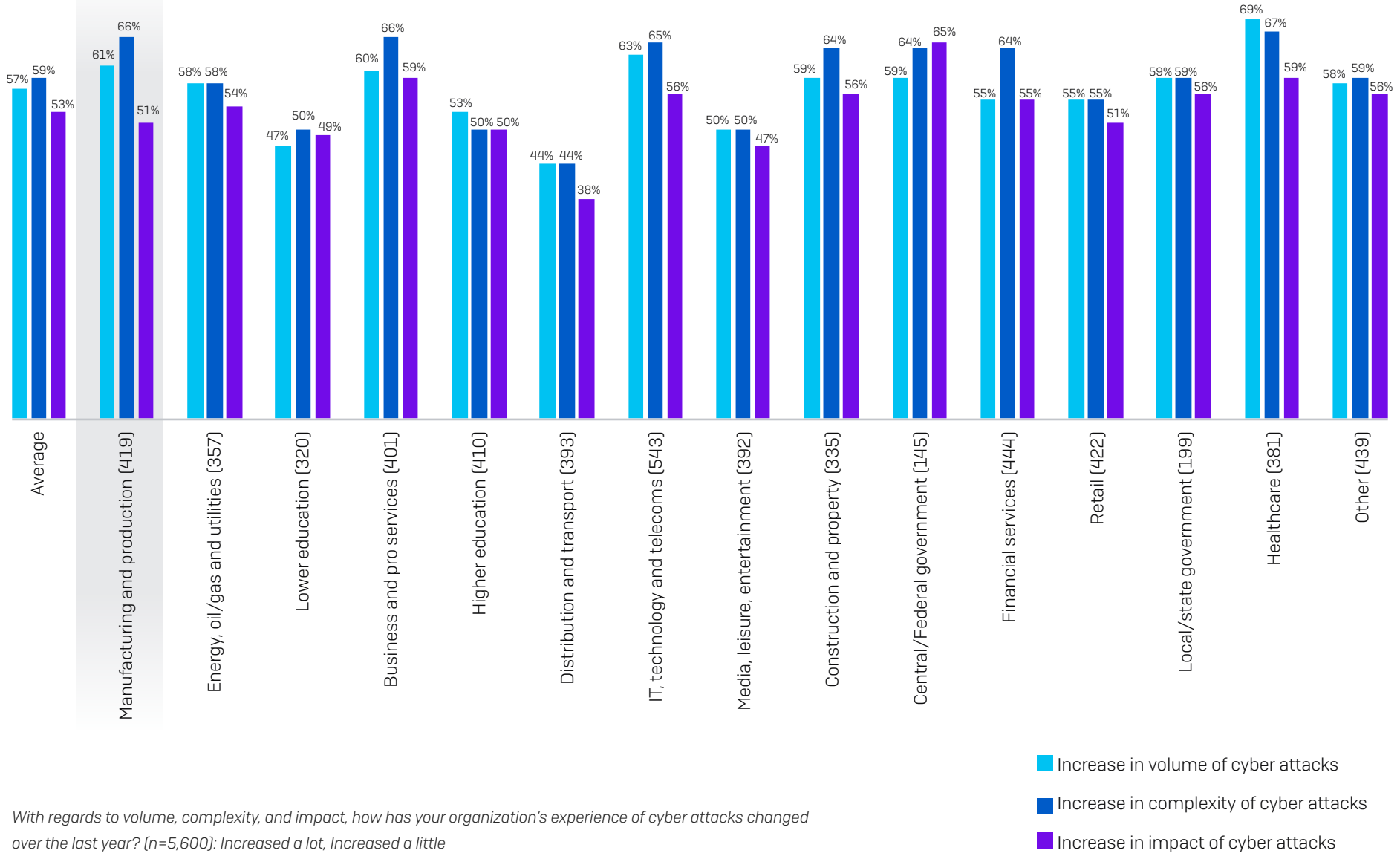
How much of your organization's data did you get back in the most significant ransomware attack?
44/ 15 manufacturing and production organizations that paid the ransom and got data back

Manufacturing and Production Made Highest Ransom Payments



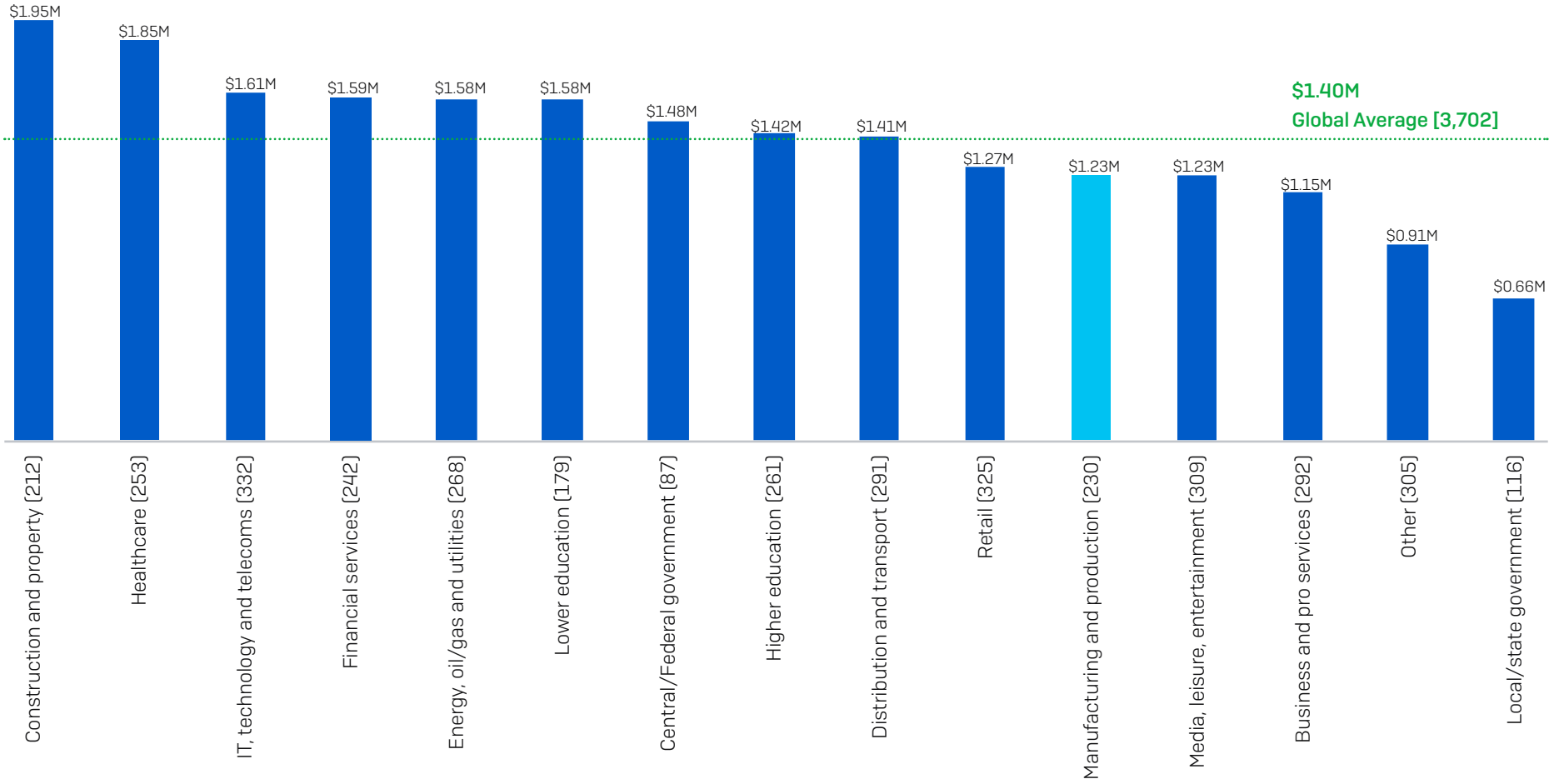
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses. N.B. For sectors with low base numbers, findings should be considered indicative.

How Sectors Stack: Changing Experience of Attacks



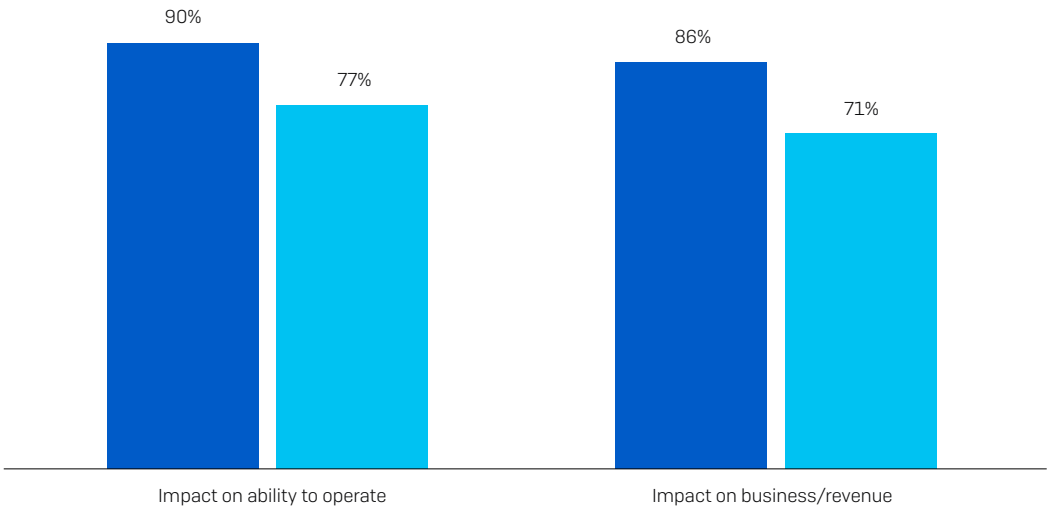
With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600): Increased a lot, Increased a little

Cost to Recover From Attacks Has Dropped



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, ransomware paid etc.)? (3,702 organizations that were hit by ransomware)

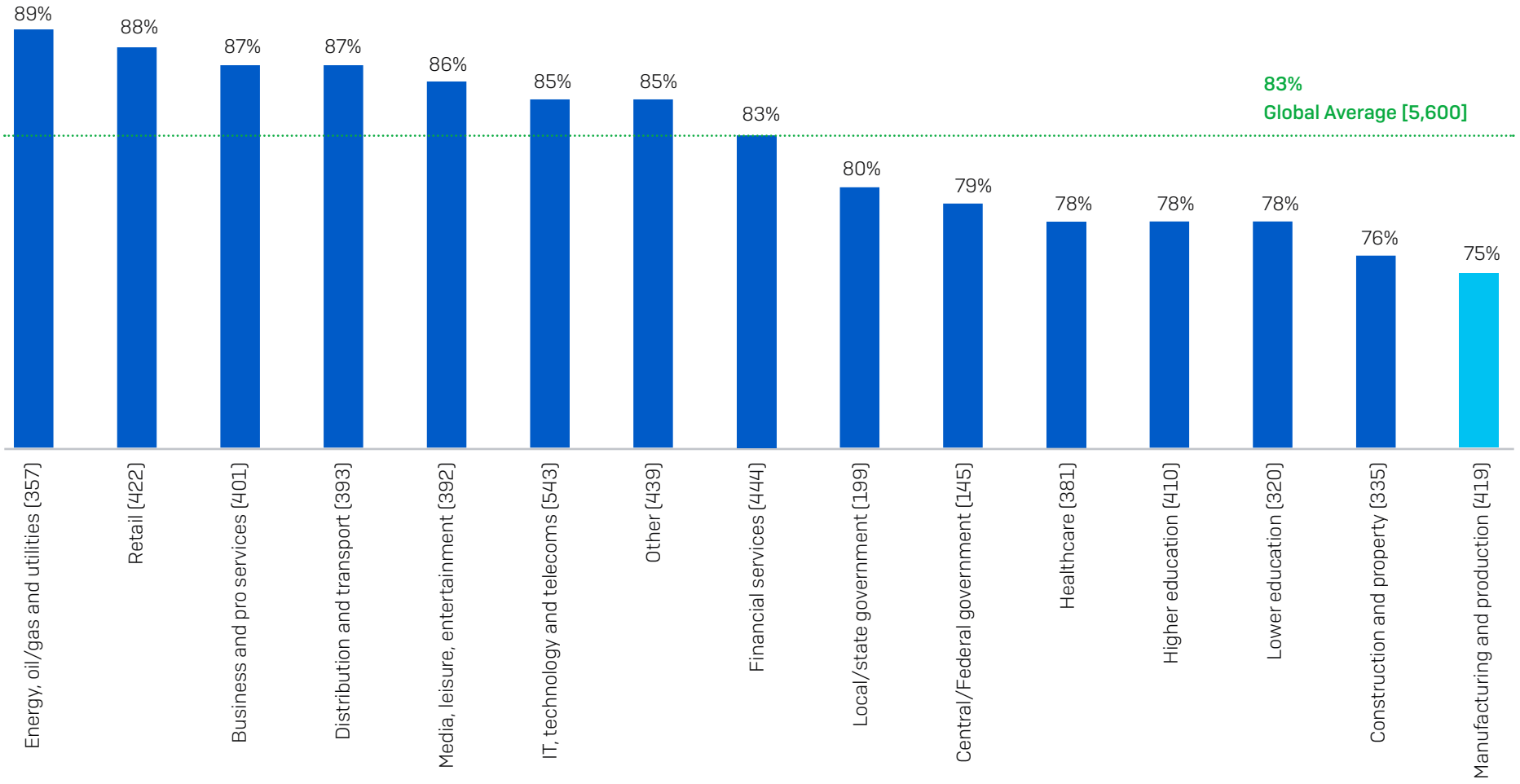
Wider Impact of Ransomware on Manufacturing and Production



Note: Only private sector organizations were asked about loss of business/revenue. The data here excludes public sector respondents.

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; 230 manufacturing and production organizations that where hit by ransomware in the previous year) Excluding some answer options.

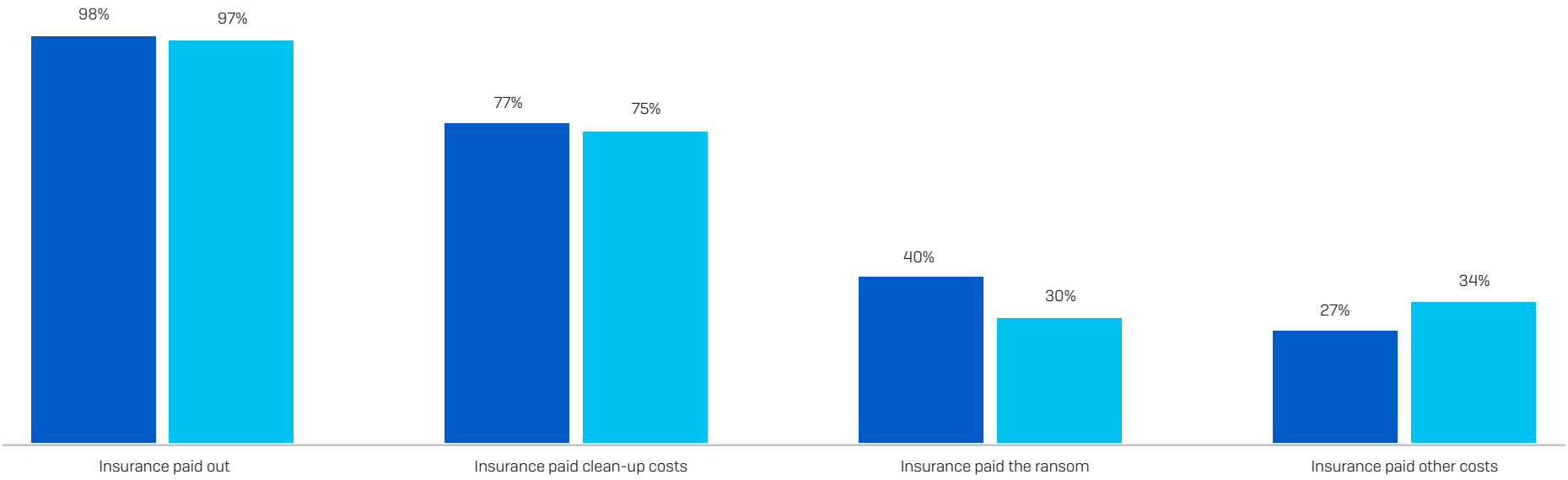
Manufacturing and Production Has the Lowest Rate of Cyber Insurance Coverage for Ransomware



Does your organization have cyber insurance that covers it if it is hit by ransomware? (base numbers in chart).

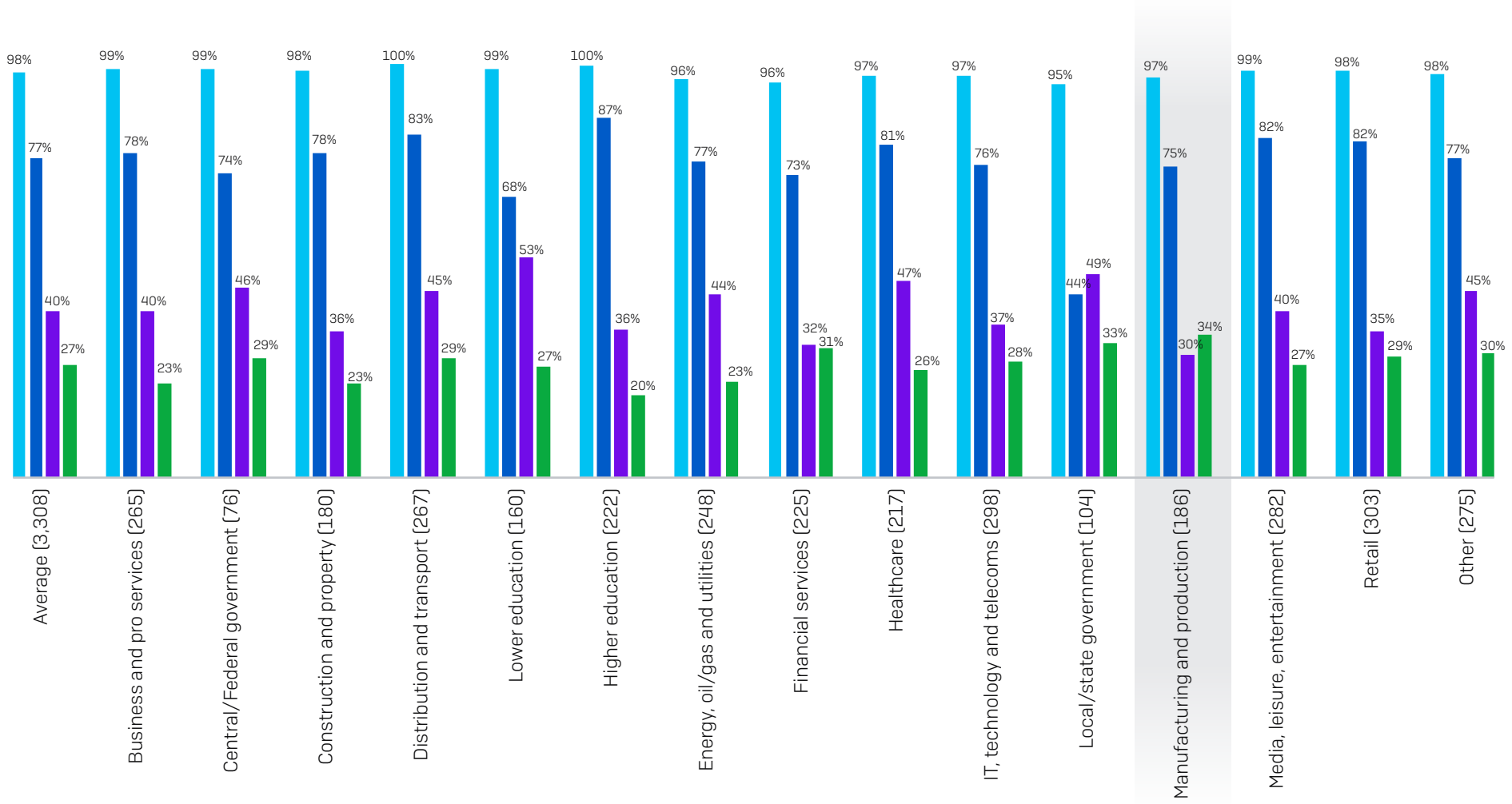
Yes; Yes, but there are exceptions/exclusions in our policy

Manufacturing and Production Has Below-Average Ransom Payout Rates



Did the cyber insurance pay out to address the costs associated with the most significant ransomware attack that your organization suffered? (3,308/ 186 manufacturing and production 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.)

Cyber Insurance Pay-out 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.

2022-10-06 (WP-NP)

SOPHOS