SOPHOS
Cybersecurity delivered.

VLCM
Getting IT Right

The State of Ransomware in Education 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 730 respondents from the education sector.

A Sophos Whitepaper. July 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in the education 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 from mid-sized organizations (100-5,000 employees) across 31 countries.

320 respondents were from lower education i.e. organizations that cater to students below 18 years, including primary, secondary, elementary, high school, and K-12 institutions. 410 respondents were from the higher education sector, encompassing organizations catering to students above 18 years such as colleges and universities. Given the many differences between a small school and a larger university, separating education in this way enables us to gain greater insights into the challenges and experiences faced by different types of education organizations.

The survey was conducted during January and February 2022, and respondents were asked to respond based on their experiences over the previous year.

Ransomware attacks on education have increased

56% of lower education organizations and 64% of higher education organizations were hit by ransomware in the last year. This is a considerable increase from the 44% of education respondents that reported an attack in our 2021 survey (based on 499 respondents across lower and higher education).

This jump in the ransomware attack rate was part of a cross-sector trend: across all sectors, 66% of respondents reported being hit by ransomware, up from 37% the year before.

While education has a below-average attack rate, the adversaries' encryption success rate in this sector is considerably higher than average. Higher education has the highest data encryption rate of all sectors surveyed (74% of attacks resulted in data being encrypted) while lower education is only a little behind at 72%. In comparison, the global average encryption rate comes in at 65%. These findings suggest that the education sector is poorly prepared to defend against a ransomware attack, and likely lacks the layered defenses needed to prevent encryption if an adversary does succeed in penetrating the organization.

The high level of successful ransomware attacks is part of an increasingly challenging broader threat environment that has affected organizations across all sectors: globally, 57% of respondents reported an increase in the volume of cyberattacks on their organization last year, and 59% reported an increase in complexity of attacks and 53% reported an increase in attack impact. Overall, 72% of respondents reported an increase in at least one of these areas.

While respondents in both the lower and higher education sectors were affected by this changing threat environment, education had a below-average percentage of respondents reporting increases in all three areas (volume, complexity, impact).

	INCREASE IN VOLUME OF CYBER ATTACKS	INCREASE IN COMPLEXITY OF CYBER ATTACKS	INCREASE IN THE IMPACT OF CYBER ATTACKS
Lower education	47%	50%	49%
Higher education	53%	50%	50%
Global average	57%	59%	53%

Hit by ransomware

56%
lower education

64%
higher education

66%
global average

Data encrypted in the attack

72%
lower education

74%
higher education

65%
global average

Most education 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 lower education (99%) and higher education (98%) organizations hit by ransomware and that had data encrypted got some encrypted data back.

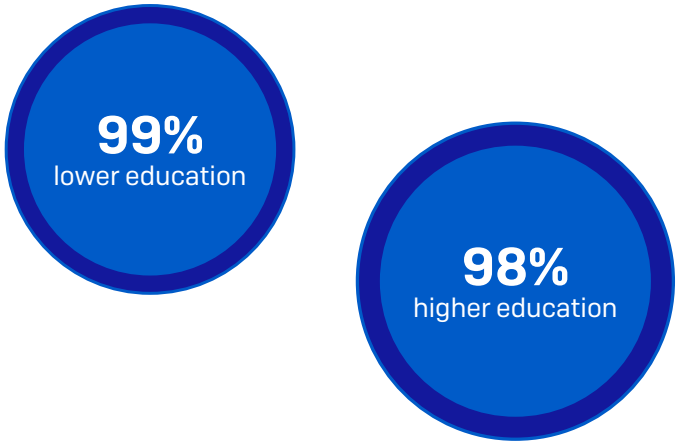
Backups are the #1 method used to restore data, used by 76% of lower education and 70% of higher education organizations whose data was encrypted (global average of 73%).

At the same time, 45% in lower education and 50% in higher education reported that they paid the ransom to restore data, compared with the global average of 46%. Plus, 35% in lower education and 34% in higher education said they used other means to restore data compared to the 30% global average.

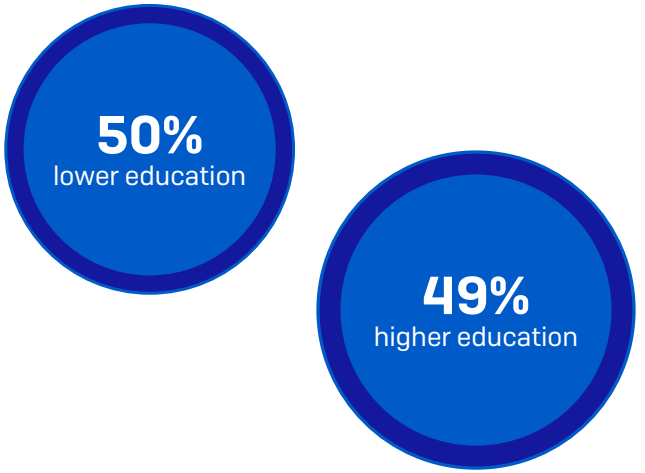
These numbers demonstrate that educational organizations have a high propensity to use multiple restoration approaches in parallel to maximize the speed and efficacy with which they can get back up and running. Overall, half (50%) of lower education respondents and nearly half (49%) of higher education respondents whose organization's data had been encrypted used multiple methods to restore data compared to the global average of 44%.

	PAID THE RANSOM	USED BACKUPS	USED OTHER MEANS
Lower education	45%	76%	35%
Higher education	50%	70%	34%
Global average	46%	73%	30%

Restored some encrypted data



Used multiple restoration methods



Percentage of data recovered by the education sector after paying the ransom

While paying the ransom almost always gets you some data back, the percentage of data restored after paying has dropped over the last year.

On average, in 2021 lower education organizations that paid the ransom got back 62% of their encrypted data and higher education organizations got back 61% of their encrypted data. This is in line with the global average of 61%. However, it represents a drop from the 68% of data restored reported by education organizations in 2020.

Similarly, only 4% of those that paid the ransom in 2021 got ALL their data back, down from 8% in 2020. The 2021 number was even less for lower education (2%) and higher education (2%) organizations.

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%
lower education

61%
higher education

61%
global average

The percentage that got ALL data back after paying the ransom

2%
lower education

2%
higher education

4%
global average

Education made high ransom payments

Although the rate of ransom payment in lower education is slightly below the global average, it is one of the top three sectors for the amount of ransom paid, with the average coming in at a huge US$1.97M.

This is, on the face of it, a surprising finding given that many schools are cash strapped. It may be that attackers are targeting larger school districts that are more likely to be able to pay higher ransom amounts. In addition, as we will see in more detail later, the high frequency of ransom payments by cyber insurance providers in this sector is likely contributing to the high ransom amounts.

Diving into the lower education ransom payments in more detail, 52% of the ransom amounts were US$100K and above. 13% of respondents in lower education paid an exorbitant US$5M or more. Lower education had the highest rate of US$5M or more payments of all sectors surveyed and far exceeded the global average of 4% who paid this level of ransom.

In the case of higher education, although the average ransom payment (US$905K) was not as high as in lower education, it was still higher than the global average (US$812K). 64% of the ransom amounts by higher education organizations were less than US$100K. At the same time, however, 14% of respondents paid ransom amounts of US$1M or more, pulling up the average ransom payment for this sector to exceed the global average.

US$1.97M ransom paid by lower education, one of the highest of all sectors

US$905K ransom paid by higher education

13% in lower education paid US$5M or more as ransom, the highest of all sectors

14% in higher education paid US$1M or more as ransom

Ransomware has a high commercial and operational impact on the education sector

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

94% of lower education and 97% of higher education respondents hit by ransomware said the attack impacted their ability to operate, while 92% (lower) and 96% (higher) of those working in the private sector said the attack caused their organization to lose business/revenue. The commercial and operational impact on higher education was the highest across all sectors on both fronts. Lower education was second only to higher education in terms of loss of business/revenue.

In terms of the overall cost to remediate the ransomware attack, both lower education (US$1.58M) and higher education (US$1.42M) organizations experienced higher costs than the global average of US$1.4M. Several factors likely contribute to these high bills, including the high commercial and operational impact already reported, and the slower-than-average recovery times for both lower and higher education sectors.

On the topic of recovery time, lower education reported that 40% of organizations hit by ransomware took up to a week to recover from the most significant attack. 26% of respondents took over a month to recover with 21% of respondents taking between 1-3 months and 5% taking 3-6 months to recover.

At the same time, higher education reported the slowest recovery across all sectors with 9% of respondents reporting a recovery period of 3-6 months, more than double the global average of 4%. 31% of higher education respondents took 1-3 months to recover, again almost double the global average of 16%. Overall, 40% in higher education took over a month to recover compared to the global average of 20%.

Ransomware impacted the ability to operate

94%
lower education

97%
higher education*

Ransomware impacted business/revenue

92%
lower education (private sector)

96%
higher education (private sector)*

The average cost to remediate attacks

US$1.58M in lower education

US$1.42M in higher education

Time to recover from attacks

DURATION	LOWER EDUCATION	HIGHER EDUCATION
3-6 months	5%	9%
1-3 months	21%	31%
Over a month	26%	40%

* highest across all sectors

Education has a low rate of cyber insurance coverage for ransomware

Across all sectors, on average 83% of organizations had secured cyber insurance against ransomware. In comparison, only 78% of lower education and higher education organizations have coverage.

For those with cyber insurance, the process for securing coverage has changed over the last year for over 90% of respondents:

- 39% in lower education and 44% in higher education say fewer providers are offering cyber insurance
- 50% in lower education and 49% in higher education say the level of cybersecurity they need to qualify for cyber insurance is now higher
- 46% in lower education and 40% in higher education say policies are now more complex
- 35% in lower education and 41% in higher education say the process takes longer
- 34% in lower education and 31% in higher education say 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. Having strong cyber defenses will significantly improve an organization's ability to secure the coverage they need.

Cyber insurance is driving education to improve cyber defenses

The challenging cyber insurance market is driving education organizations to improve their cyber defenses: over the last year, 95% of lower education and 96% of higher education organizations have made changes to their cyber defenses to secure coverage. While these numbers are very high, they are the lowest of all sectors surveyed, indicating that this is a universal challenge.

Diving into the details, 57% of lower education and 68% of higher education organizations have implemented new technologies/services to improve their insurance position. For comparison, the global average is 64%.

When it comes to increasing cybersecurity training and education of staff, 53% in lower education have invested in this area compared with 48% in higher education (the lowest across all sectors surveyed). 50% in lower education and 49% in higher education have changed processes/behaviors.

Cyber insurance drives improvement in cyber defenses

	HAVE CHANGED CYBER DEFENSES	HAVE IMPLEMENTED NEW TECHNOLOGIES/ SERVICES	HAVE INCREASED STAFF TRAINING/ EDUCATION ACTIVITIES	HAVE CHANGED PROCESSES/ BEHAVIORS
Lower education	95%	57%	53%	50%
Higher education	96%	68%	48%	49%
Global average	97%	64%	56%	52%

Education has high cyber insurance payout rates

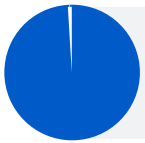
The good news for education organizations with cyber insurance is that in the event of a ransomware attack the cyber insurance almost always pays out towards some costs: lower education reported a 99% payout rate and higher education a 100% payout rate.

There are interesting differences in what the insurance pays out for. Higher education reported the highest (87%) rate of clean-up cost payment of all sectors i.e. the costs to get the organizations back up and running again.

Conversely, lower education reported the highest rate of ransom payment across all sectors with the insurance covering the ransom in over half (53%) of incidents. This is likely a contributing factor to the high average ransom payments in this sector.

However, 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:



99%
lower education

100%
higher education

Clean-up costs payout:

68%
lower education

87%
higher education, highest across sectors

Ransom payout:

53%
lower education, highest across sectors

36%
higher education

Conclusion

The ransomware challenge facing education organizations continues to grow. The proportion of organizations directly impacted by ransomware has increased considerably over the last year. Furthermore, adversaries have an above-average success rate when it comes to encrypting data in an attack.

In the face of the near-normalization of ransomware, education organizations have gotten better at dealing with the aftermath of an attack: virtually everyone now gets some encrypted data back and nearly three-quarters can use backups to restore data.

At the same time, the proportion of encrypted data restored by education after paying the ransom is in line with the global average of 61%: lower education at 62% and higher education at 61%.

The financial impact of ransomware on education is huge. The sector made high average ransom payments – US$1.97M by lower education and US$905K by higher education organizations. Ransomware also severely impacts operations and business/revenue in the education sector.

Many organizations in this sector are choosing to reduce the risk associated with cyber attacks by taking cyber insurance. For them, it is reassuring to know that insurers pay some costs in almost all claims.

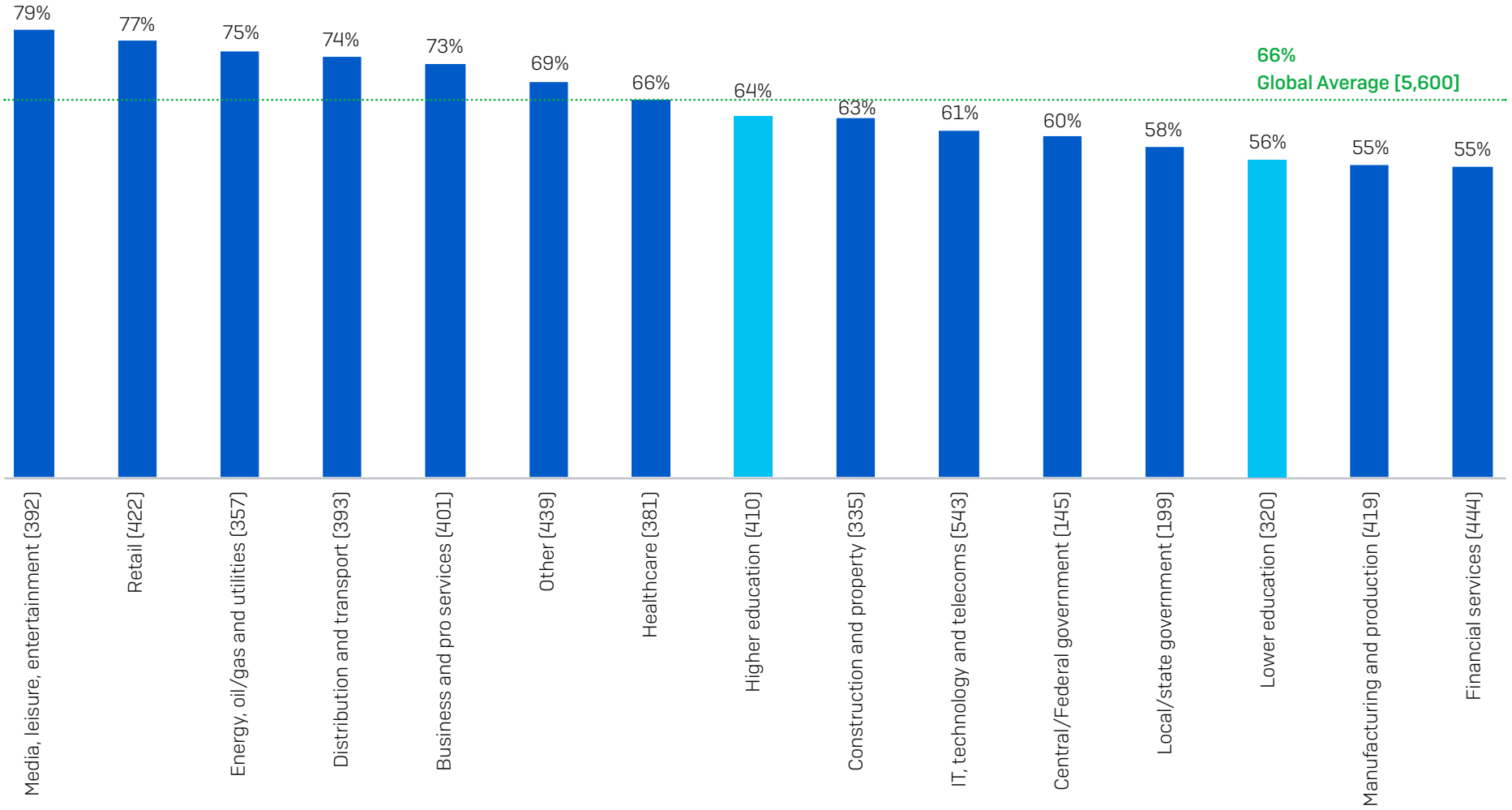
However, it's getting harder for organizations especially in the education sector to secure coverage. While many education organizations have made changes to their cyber defenses to improve their cyber insurance position, the survey shows that education organizations lag behind other sectors when it comes to improving their defenses.

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.

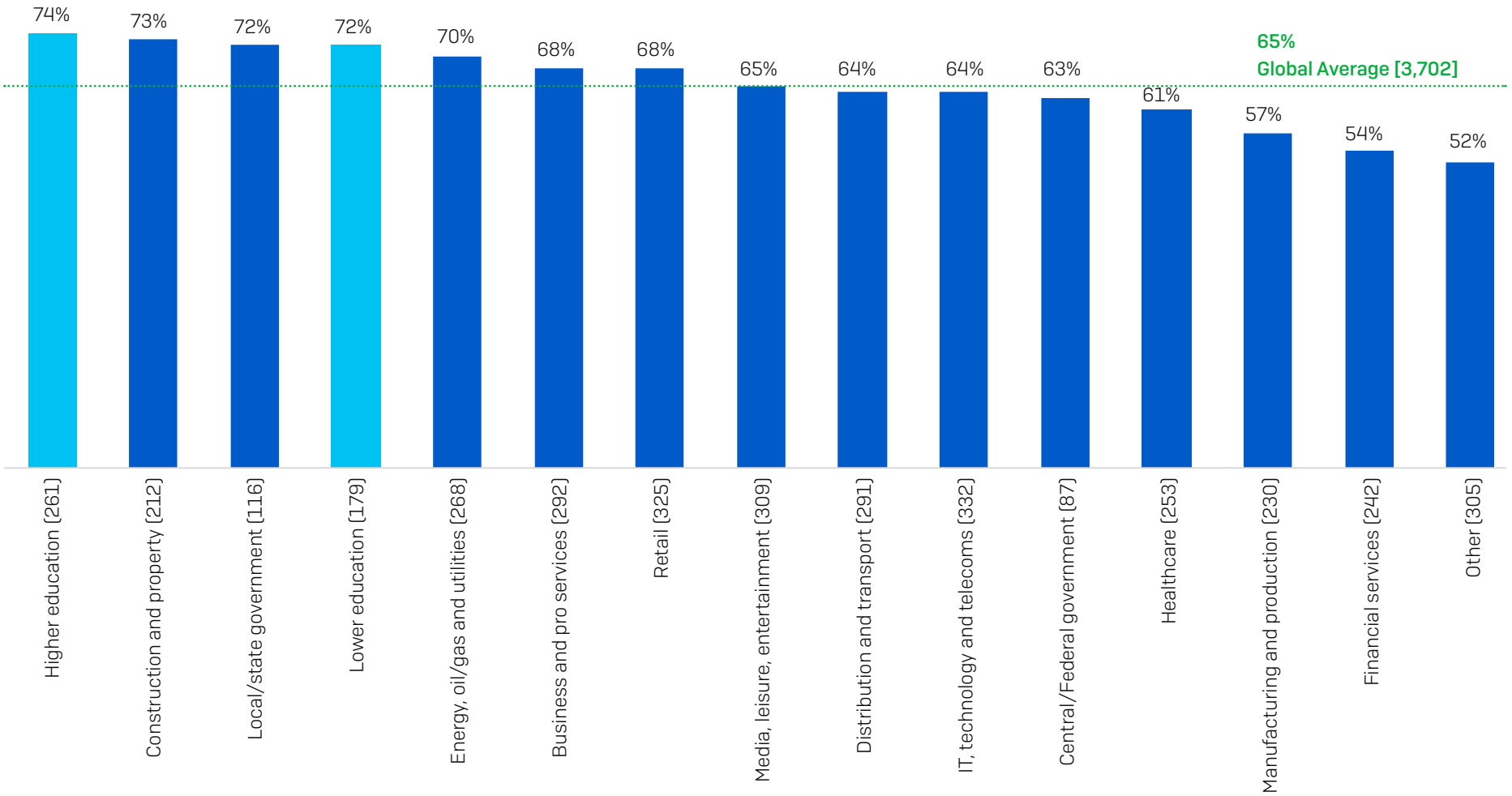
For detailed information on individual ransomware groups, see the Sophos ransomware threat intelligence center.

How Education Stacks: Ransomware Attacks by Sector



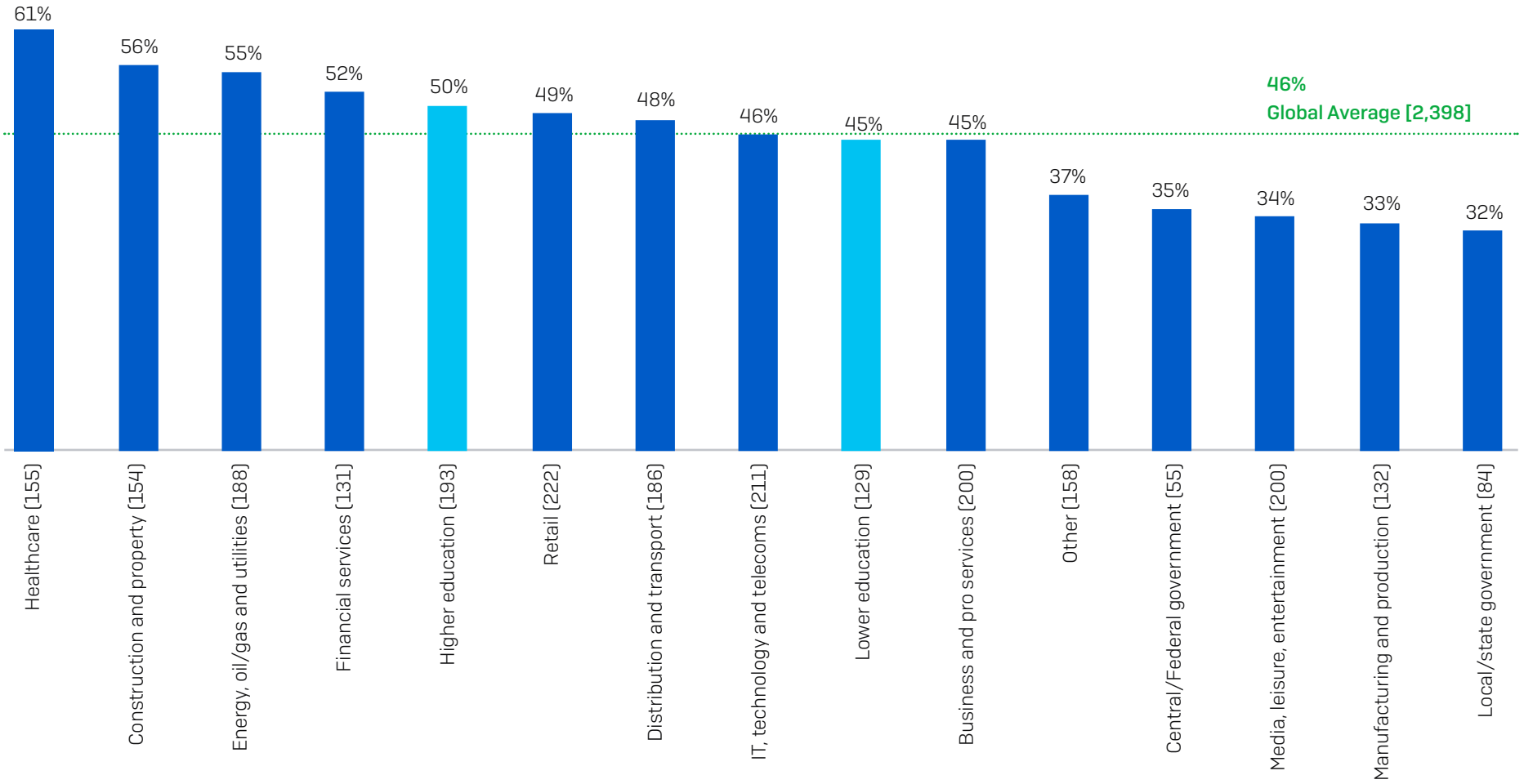
In the last year, has your organization been hit by ransomware? [n=5,600]

Data Encryption Rate in Education is Above the Global Average



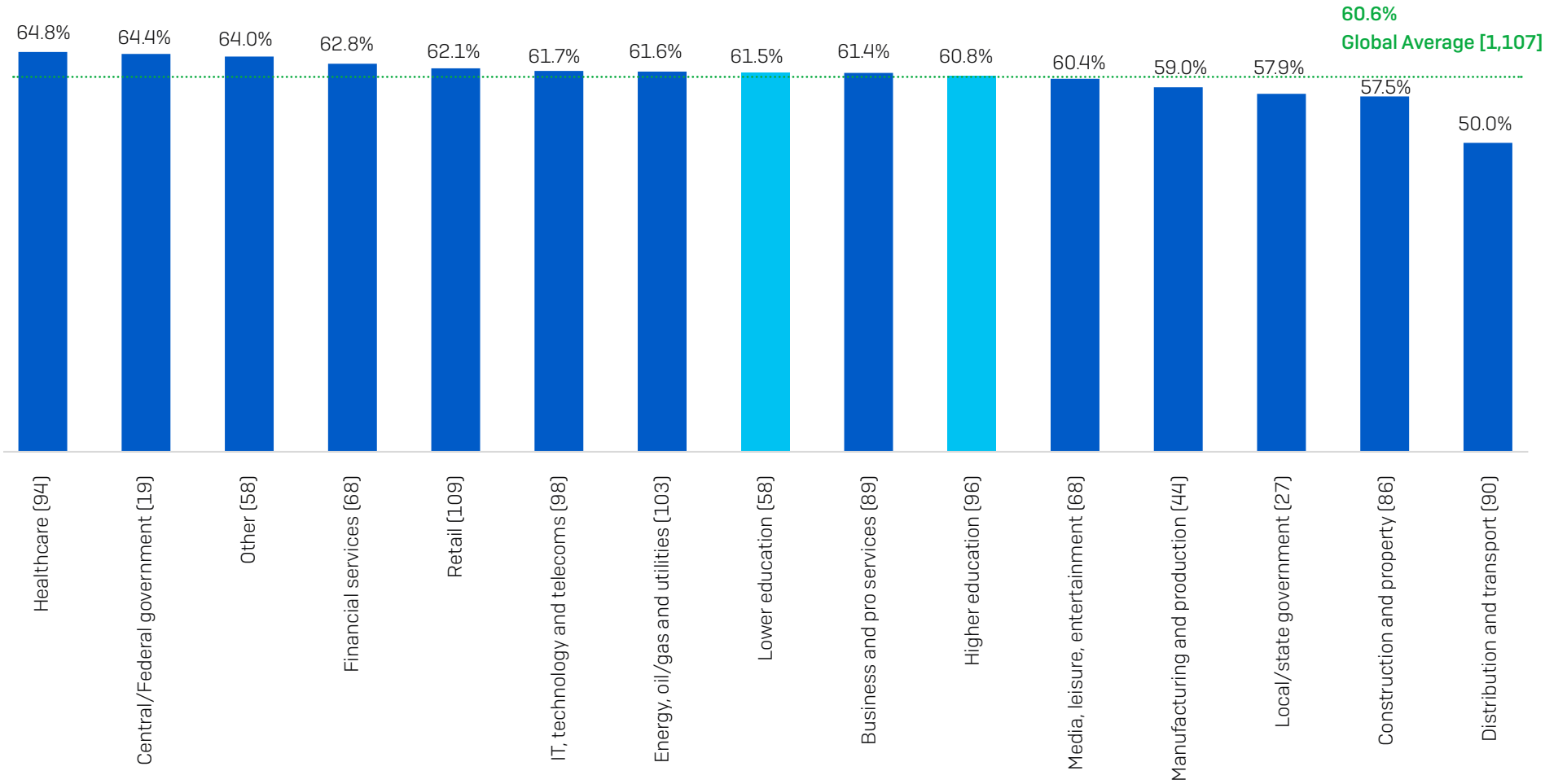
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

How Education Stacks: Rate of Ransom Payment



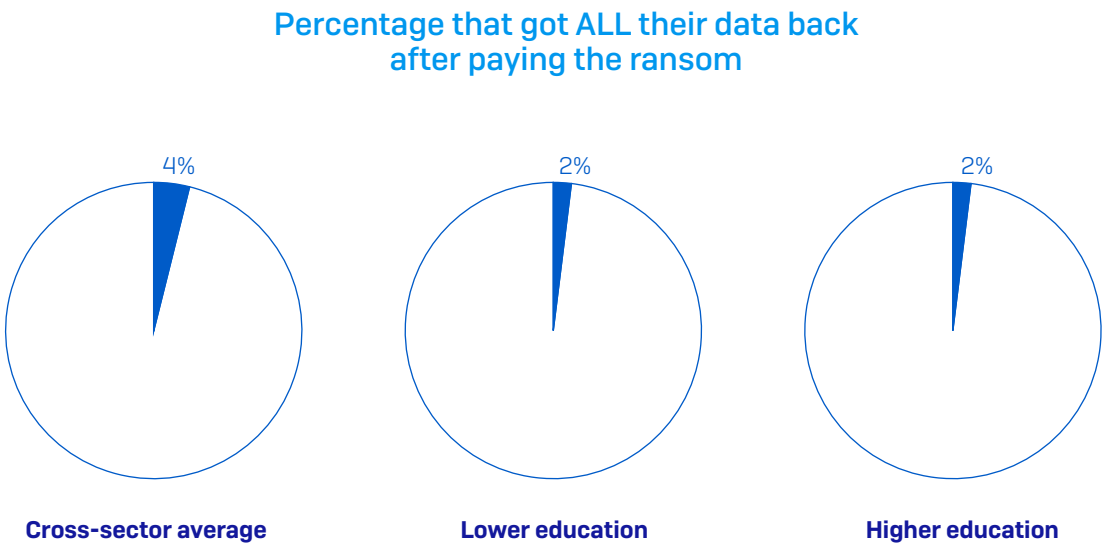
Did your organization get any data back in the most significant ransomware attack?
[n=2,398 organizations that had data encrypted]: Yes, we paid the ransom and got data back

How Education Stacks: Data Recovered After Paying the Ransom



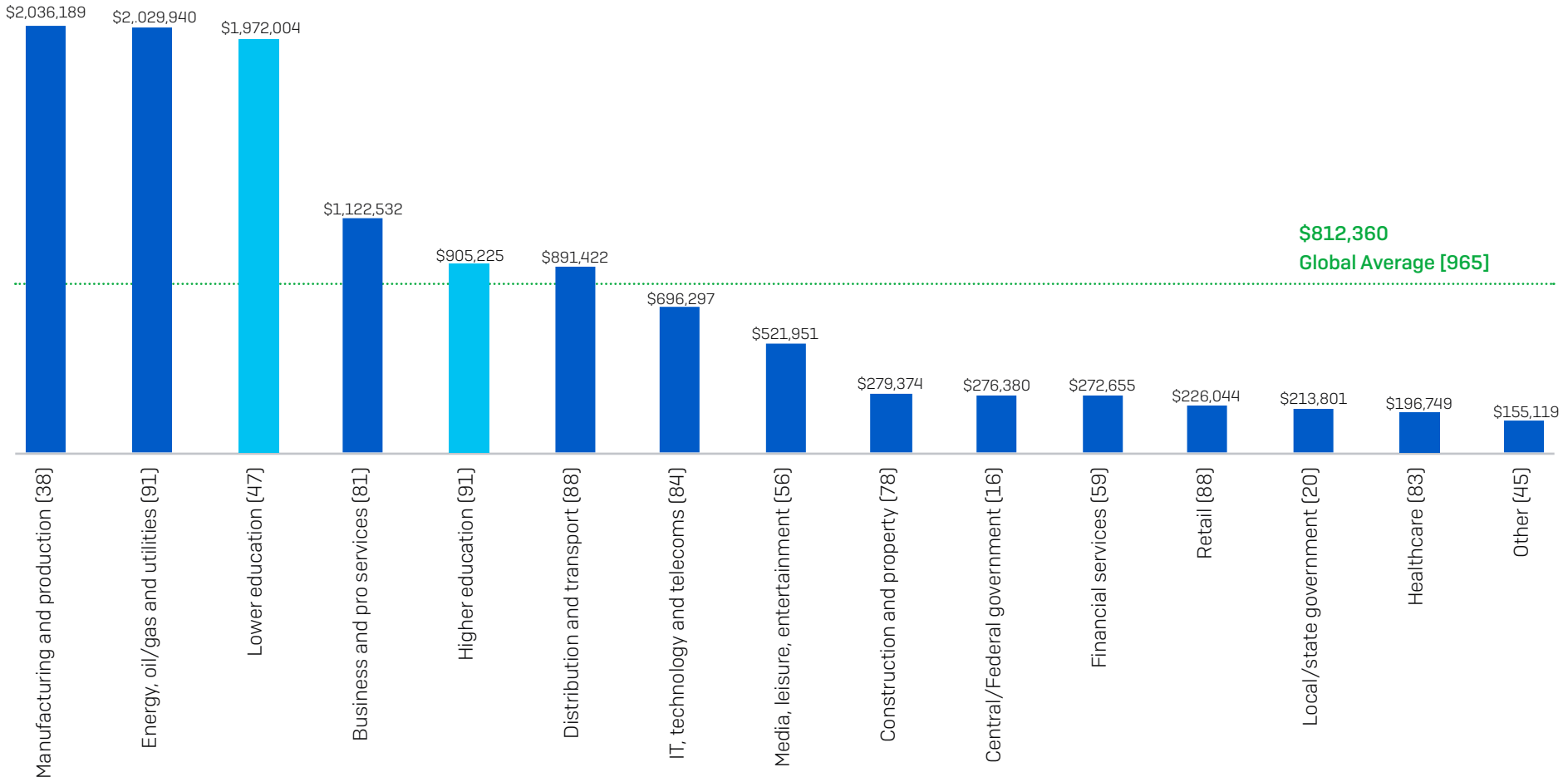
How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)

Paying the Ransom Rarely Gets ALL Data Back



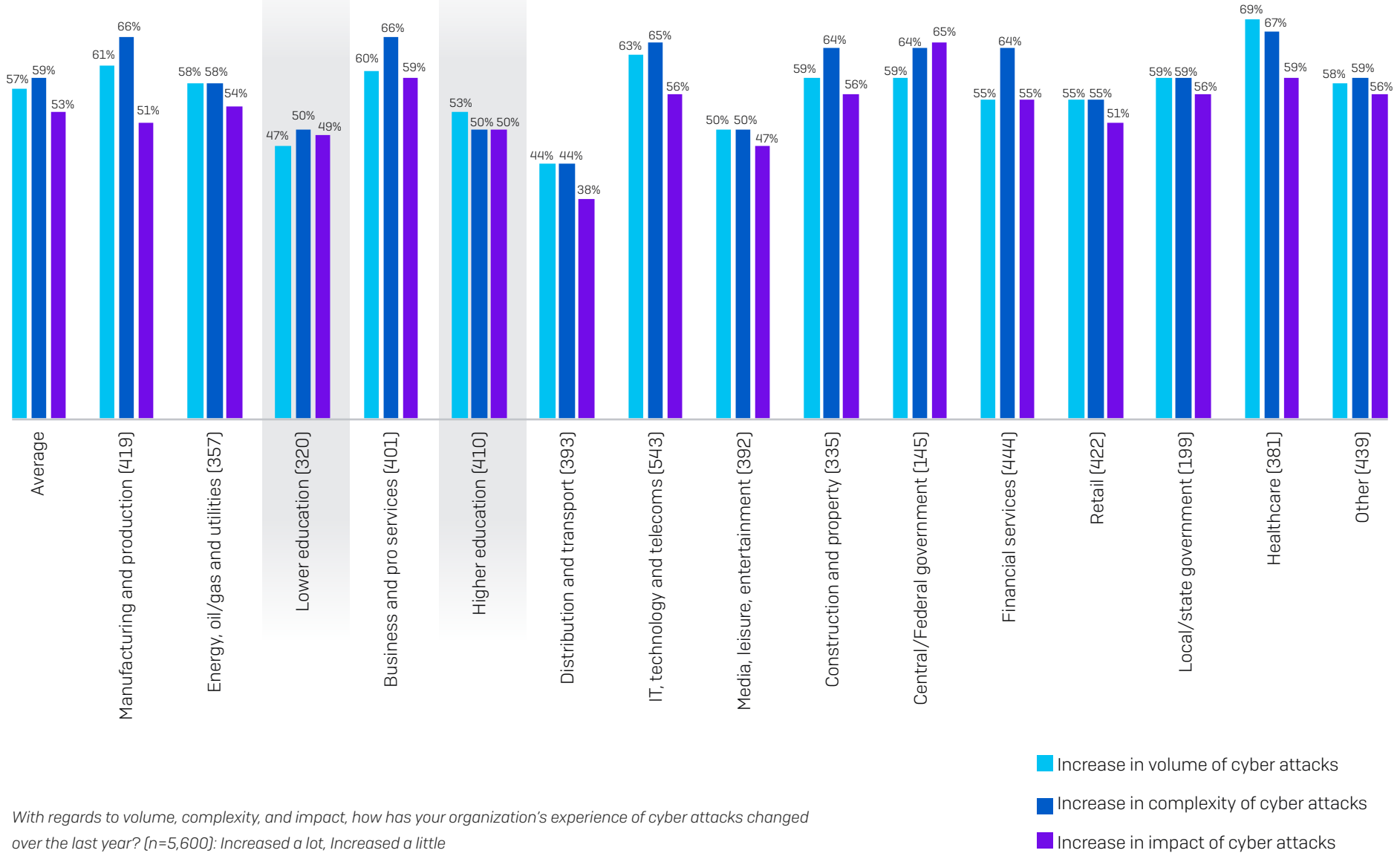
How much of your organization's data did you get back in the most significant ransomware attack? (n=1,107/59 lower education and 96 higher education organizations that paid the ransom and got data back)

Education Made High Ransom Payments



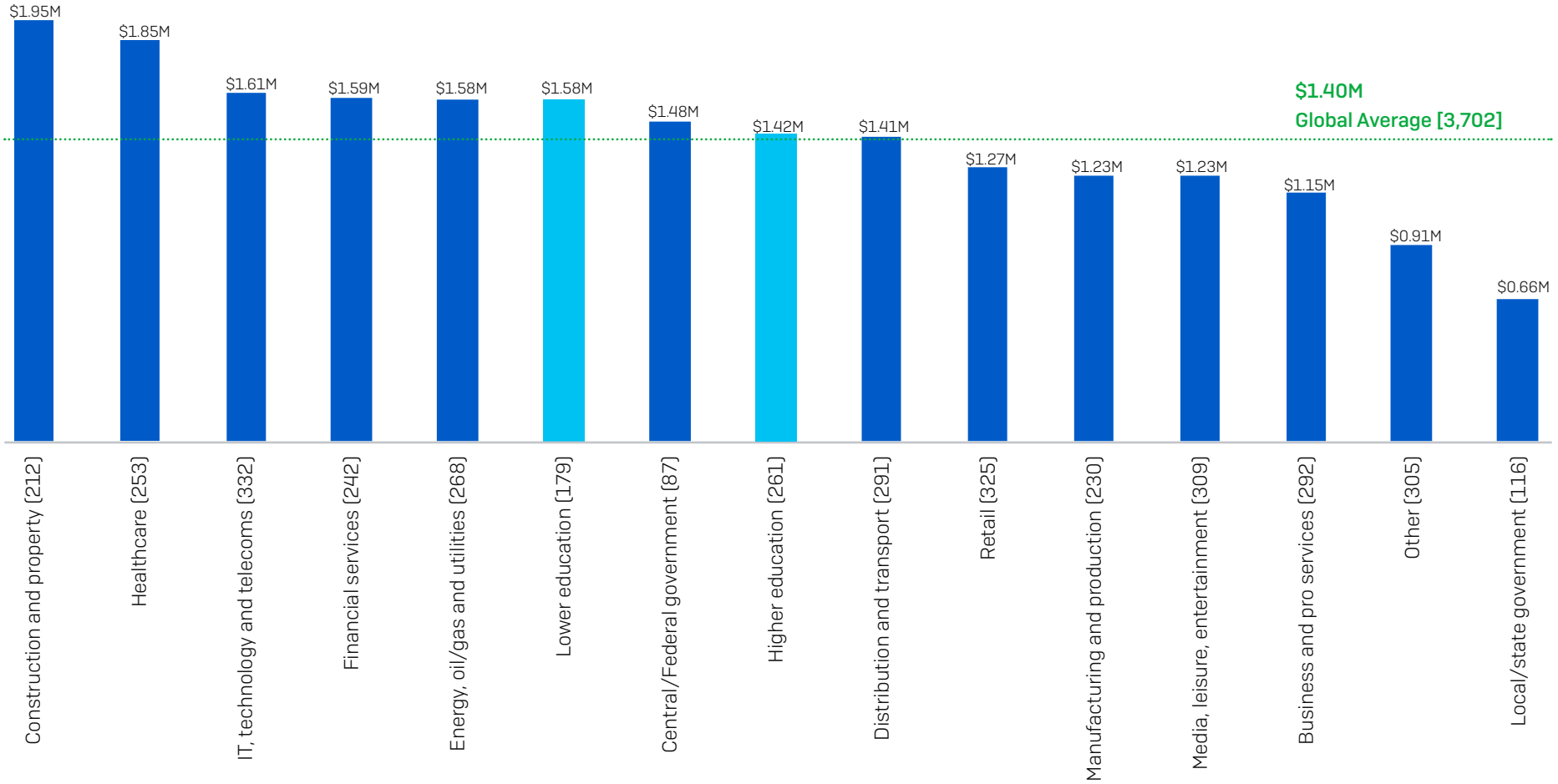
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses.N.B. For sectors with low base numbers, findings should be considered indicative.

How Education Stacks: Change In Experience of Cyber Attacks Over the Last Year



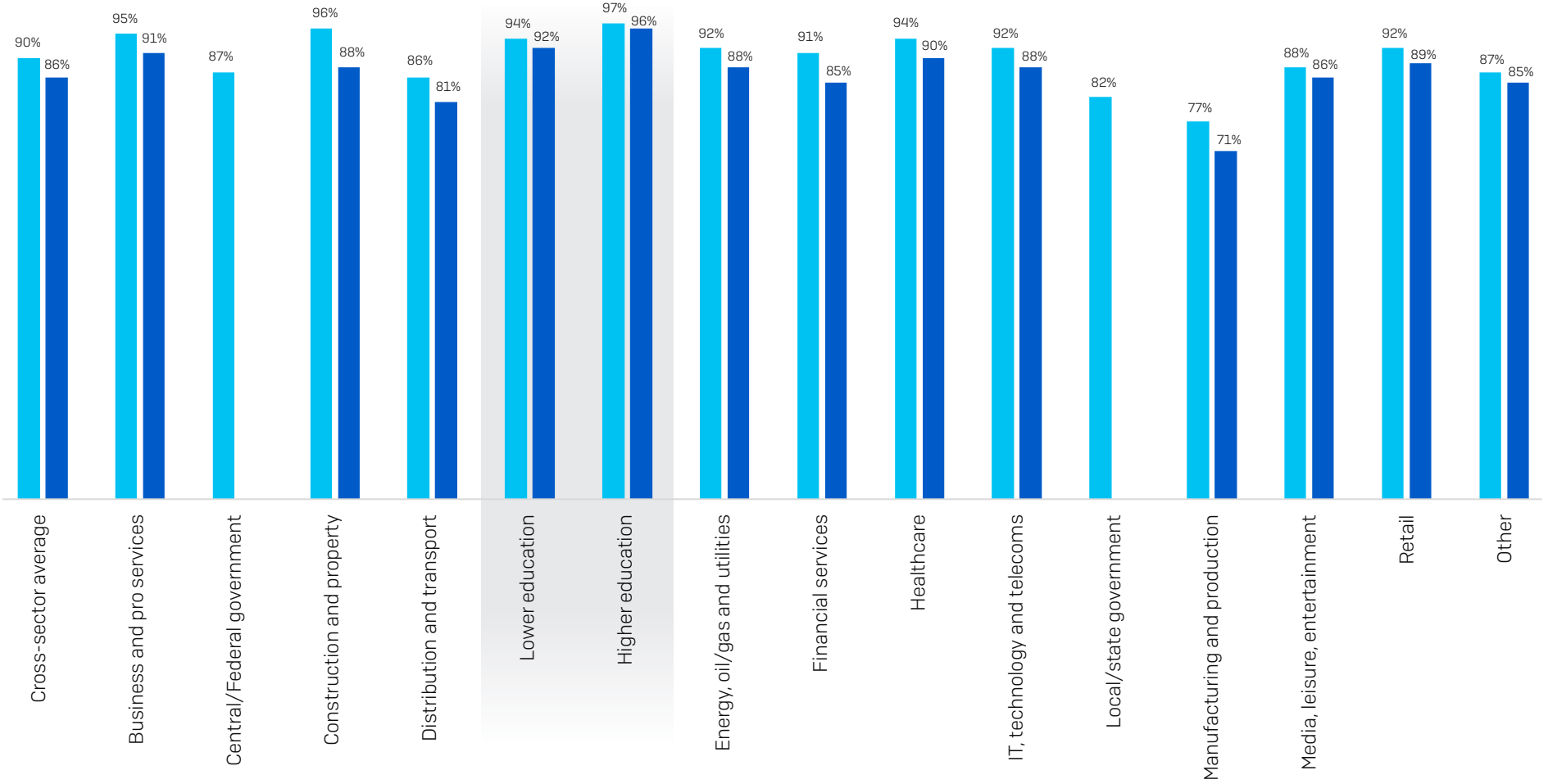
With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600): Increased a lot, Increased a little

Education Experiences Above-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)

Impact Of Ransomware On Education Is Highest Across Sectors

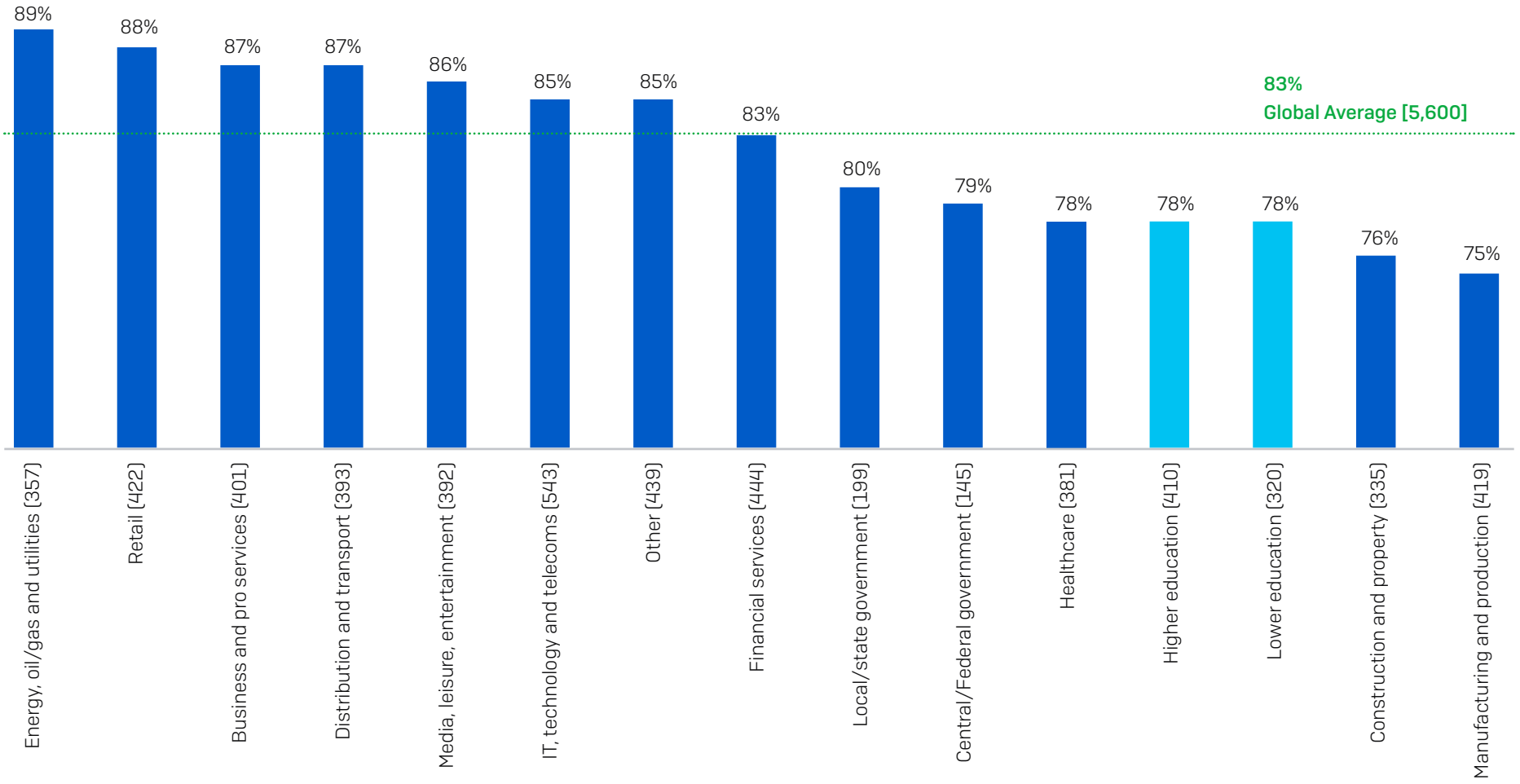


Did the most significant ransomware attack impact your organization's ability to operate? (n=3702 organizations that were hit by ransomware in the previous year)/Did the most significant ransomware attack cause your organization to lose business/revenue? (n=3162 private sector organizations that were hit by ransomware in the previous year.) Excluding some answer options.

Ransomware impacted ability to operate

Ransomware impacted business/revenue

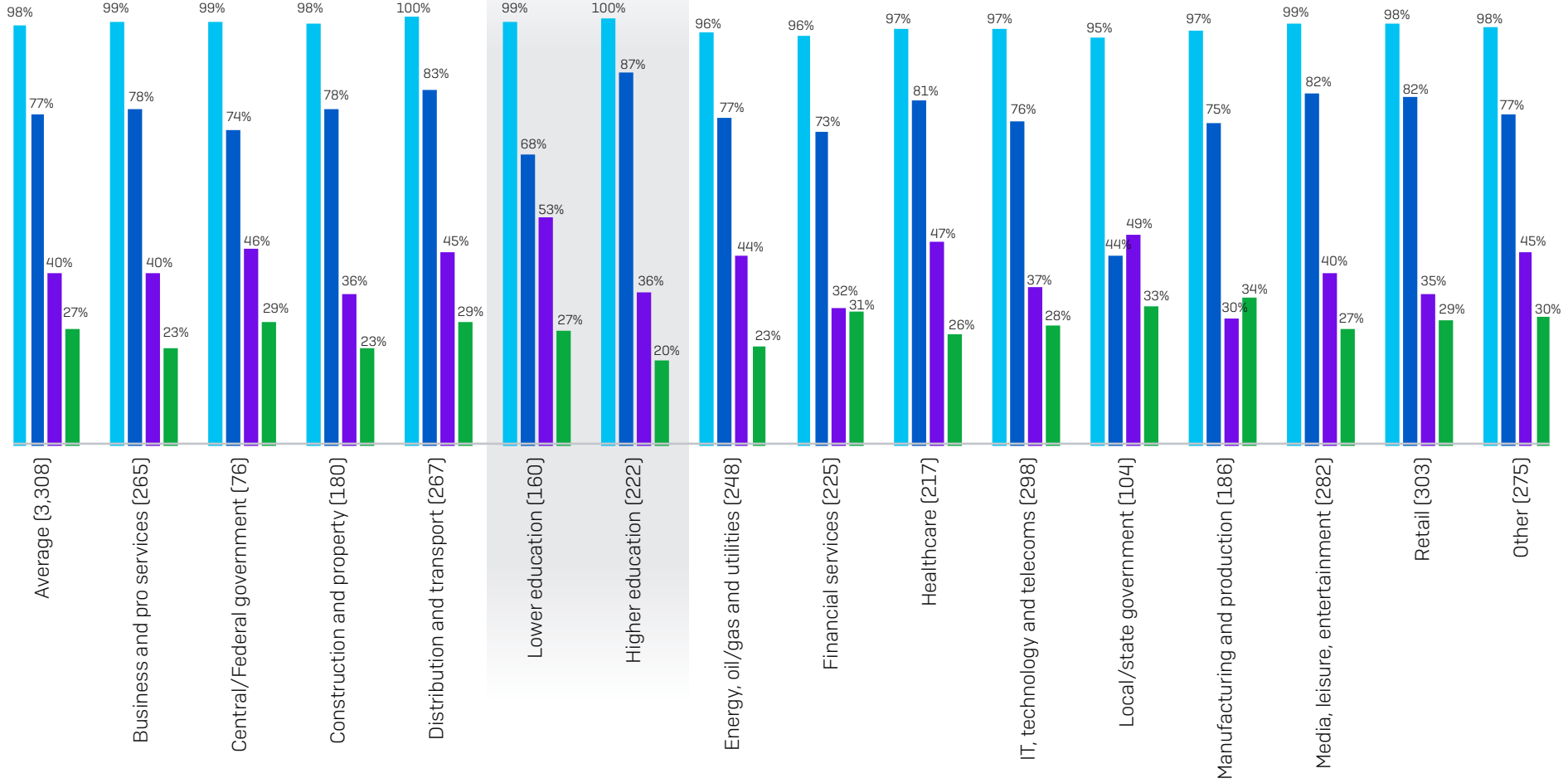
Education Has a Low Rate of Cyber Insurance Coverage for Ransomware



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

How Education Stacks: 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.

2022-06-24 (WP-NP)

VLCM Getting IT Right

SOPHOS