SOPHOS
Cybersecurity delivered.

The State of Ransomware in Healthcare 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations, including 381 healthcare respondents, across 31 countries.

A Sophos Whitepaper. May 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in healthcare working at the frontline has revealed an ever more challenging attack environment. Together with the growing financial and operational burden ransomware places on its victims, the report 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 381 healthcare respondents, in mid-sized organizations (100-5,000 employees) across 31 countries. The survey was conducted during January and February 2022, and respondents were asked to respond based on their experiences over the previous year.

5,600
respondents

381
Healthcare respondents

31
countries

100-5,000
employees

Jan/Feb 2022
research conducted

Attacks are up and their complexity and impact are increasing

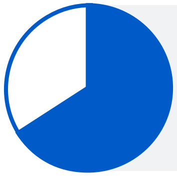
66% of healthcare organizations were hit by ransomware last year, up from 34% in 2020. This is a 94% increase over the course of a year, demonstrating that adversaries have become considerably more capable at executing the most significant attacks at scale. This likely also reflects the growing success of the ransomware-as-a-service model, which significantly extends the reach of ransomware by reducing the skill level required to create and deploy an attack. [Note: hit by ransomware was defined as one or more devices impacted by the attack but not necessarily encrypted.]

If we compare the prevalence of ransomware attacks across all sectors surveyed, the rate of attacks on healthcare was at par with the global average of 66%.

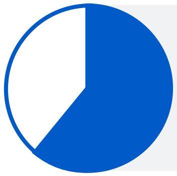
In terms of data encryption rate, healthcare, with a 61% encryption rate, performed better than the global average of 65%, indicating that healthcare was better able to stop data encryption in a ransomware attack. There was also a drop in healthcare's encryption rate over the previous year (65% in 2020).

The percentage of victims who experienced extortion-only attacks, where data was not encrypted but the organization was held to ransom with the threat of exposing data, reduced from 7% in 2020 to 4% in 2021. One reason for this good showing could be that more healthcare organizations are now opting for cyber insurance, which demands higher cybersecurity defense enhancements. We will look at this trend in the later part of this report.

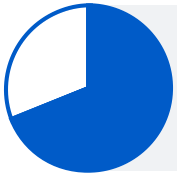
The increase in successful ransomware attacks is part of an increasingly challenging broader threat environment which has affected healthcare more than any other sector. Healthcare saw the highest increase in volume of cyber attacks (69%) as well as the complexity of cyber attacks (67%) compared to the cross-sector average of 57% and 59% respectively. In terms of the impact of these cyber attacks, healthcare was the second most affected sector (59%) compared to the global average of 53%.



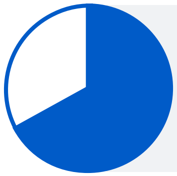
66%
hit by ransomware in the last year



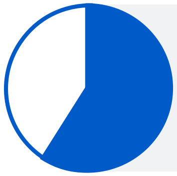
61%
attacks resulted in data encryption



69%
increase in volume of cyber attacks, highest across all sectors



67%
increase in complexity of cyber attacks, highest across all sectors



59%
increase in impact of cyber attacks, second-highest across all sectors

Healthcare is getting better at restoring data after an attack

As ransomware has become more prevalent, organizations have gotten better at dealing with the aftermath of an attack. 99% of healthcare organizations hit by ransomware in the last year now get some encrypted data back, up considerably from 93% last year.

Backups are the number one method used to restore data, used by 72% of healthcare organizations whose data was encrypted. At the same time, 61% reported that they paid the ransom to restore data, and 33% said they used other means to restore data. These numbers reflect the fact that many healthcare organizations use multiple restoration approaches to maximize the speed and efficacy with which they can get back up and running. In fact, overall, a little more than half (52%) of the respondents whose organizations' data had been encrypted used multiple methods to restore data.

Healthcare topped the chart (14%) for using all three methods in parallel to restore encrypted data: backups, ransom payment, and other means, compared with a global average of 7%. Healthcare is heavily dependent on data availability for continuity of its business operations. Lack of timely data can delay patient care, which can prove catastrophic. Healthcare's attempt to restore data using all available means is understandable.

While paying the ransom almost always gets some data back, the percentage of data restored after paying has dropped. On average, in 2021, healthcare organizations that paid the ransom got back only 65% of their data, down from 69% in 2020. Similarly, only 2% of those that paid the ransom in 2021 got ALL their data back, down from 8% in 2020.

99%
got some
encrypted data back

65%
of encrypted data
restored
after paying
the ransom

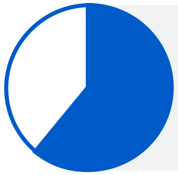
14%
used three
methods in
parallel to restore
data – highest
of all sectors

2%
paid the ransom
and got ALL
the data back

Healthcare is most likely to pay the ransom

Healthcare is the sector most likely to pay the ransom, with 61% of respondents whose data was encrypted admitting to paying the ransom compared to the cross-sector average of 46%. This number is also almost double than the 34% who paid the ransom in 2020. The highest increase in the volume and complexity of attacks on healthcare as compared to all other sectors is a likely reason behind their high propensity to pay and overcome their limited preparedness in dealing with such attacks.

Other reasons, as we will see later in this report, could be the impact of ransomware that affects not only the encrypted databases and devices but also the operations and business revenues of healthcare organizations, leaving them in a rush for normalcy. Finally, the high attack remediation costs for healthcare – which is the second highest across sectors at US$1.85M, as we will see ahead in this report – could be pushing healthcare organizations to pay up rather than spend on remediation costs.



61%
ransom payment rate by healthcare

△ Ransom payment △

61%
2021

34%
2020

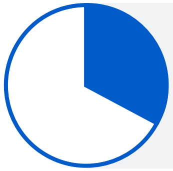
Healthcare paid the least ransom amount

While healthcare is at the top of the list for volume of payments, it's actually at the bottom of the list for the amount paid. Overall, healthcare had the lowest average ransom payment (around US$197K) of all named sectors. So, while there is a high occurrence of healthcare paying the ransom, the ransom amounts are relatively small. These low ransom payments are likely driven by the constrained finances of many healthcare organizations, particularly those in the public sector. They simply don't have more money for the attackers to squeeze out of them.

Interesting to note is that even though healthcare was the sector that paid the lowest ransoms, the overall amount of ransom paid by healthcare in 2021 actually went up by 33% compared to 2020.

Diving into the healthcare ransom payments in more detail, 60% of the ransom amounts were less than US$50K. Only three respondents said their organization paid US$1M or more. This is contrary to the trend seen for other sectors surveyed where over the last year, there has been an almost threefold increase in the proportion of victims paying ransoms of US$1M or more: up from 4% in 2020 to 11% in 2021. In parallel, the percentage paying less than US$10,000 dropped from one in three (34%) in 2020 to one in five (21%) in 2021.

US$197K average ransom payment by healthcare, lowest across sectors



33% increase in healthcare ransom payment over previous year

60% ransom amounts in healthcare less than US$50,000

Ransomware has a major commercial and operational impact in healthcare

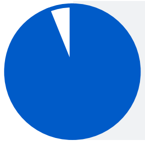
The ransom sums are just part of the story, and the impact of ransomware ranges much more widely than just the encrypted databases and devices. 94% of healthcare organizations hit by ransomware in the last year said the most significant attack impacted their ability to operate. Furthermore, 90% of private sector heathcare organizations said it caused them to lose business or revenue.

Across all sectors, the average cost to an organization to rectify the impact of the most recent ransomware attack was US$1.4M in 2021, down from US$1.85M in 2020. This reduction likely reflects the prevalence and impact of cyber insurance where the insurance providers are better able to guide victims swiftly and effectively through the incident response process, reducing the remediation cost.

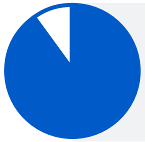
However, in the case of healthcare, the average remediation cost went up from US$1.27M in 2020 to US$1.85M in 2021. In fact, healthcare ranked second in terms of the average cost involved to rectify a ransomware attack compared to the cross-sector average (US$1.85M vs US$1.4M). As we saw earlier in this report, ransomware attacks on healthcare almost doubled in the last year (66% in 2021 versus 34% in 2020). This may be a reason why healthcare organizations rank far behind other sectors in their ability to secure cyber insurance – we cover this in more detail later in the report. Lack of cybersecurity expertise, proliferation of medical IoT devices, vulnerable legacy systems, and the very nature of 24/7 operations (which leads to an inability to quickly remediate vulnerable systems) continue to affect the healthcare sector, driving up overall remediation costs.

44% of healthcare organizations that suffered an attack in the last year took up to a week to recover from the most significant attack, whereas 25% of them took upto one month – a long time for most organizations. The slowest recovery was reported by higher education and central/federal government where around two in five took over one month to recover.

Furthermore, some organizations continue to put their faith in ineffective defenses. Of the healthcare respondents whose organizations weren't hit by ransomware in the last year and don't expect to be hit in the future, 77% are basing this on approaches that don't stop organizations from being attacked: 50% cited backups and 43% cited cyber insurance as reasons why they don't anticipate an attack, with some selecting both options. While these elements help recover from an attack, they don't prevent it in the first place.



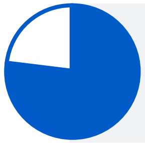
94%
ransomware attack impacted the ability to operate



90%
ransomware attack caused loss of business/revenue

US$1.85M average cost to remediate attack in healthcare, second highest across sectors

ONE WEEK average time to recover from an attack



77%
put faith in approaches that don't prevent an attack

Healthcare organizations are finding it harder to get cyber insurance

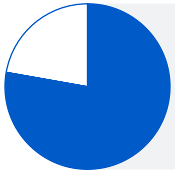
Across all sectors, 83% of organizations have secured cyber insurance against ransomware. Comparatively, only 78% of healthcare organizations are covered, and 46% of them say there are exclusions or exceptions in their policies. Given the high rate of ransomware incidents in healthcare, this insurance coverage gap leaves many organizations exposed to the full cost of an attack.

Energy, oil/gas, and utilities are most likely to have coverage (89%) closely followed by retail (88%). Manufacturing and production stands last with only 75% having insurance coverage.

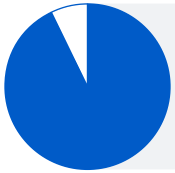
93% of those with cyber insurance in healthcare said the process for securing cover had changed over the last year with cyber insurance getting harder to secure. 51% reported that the level of cybersecurity they need to qualify is now higher, 45% said policies are now more complex, 48% said fewer companies offer cyber insurance, 46% stated that the process takes longer, and 34% 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. Those that remain are looking to reduce risk and exposure. They're also pushing up prices considerably.

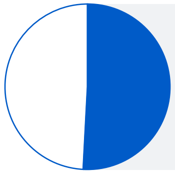
With fewer organizations providing cyber cover, it's a sellers' market. They call the shots and they can be selective about which clients they cover. Having strong cyber defenses will significantly improve an organization's ability to secure the cover they need.



78%
cyber insurance against ransomware in healthcare



93%
process for securing cover has changed over the last year



51%
level of cybersecurity needed to qualify for cyber insurance is now higher

Cyber insurance is driving improvements to cyber defenses

As the cyber insurance market hardens and it becomes more challenging to secure coverage, 97% of healthcare organizations that have cyber insurance have made changes to their cyber defenses in order to improve their cyber insurance positions. 66% have implemented new technologies and services, 52% have increased staff training and education activities, and 49% have changed processes and behaviors.

The hardening of the cyber insurance market is driven in large part by the increase in ransomware payouts and is becoming a forcing function for cyber defense enhancements.

97%
have changed cyber defenses to improve insurance position

66%
have implemented new technologies/ services

52%
have increased staff training/education activities

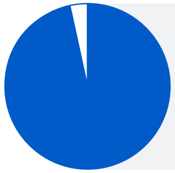
49%
have changed processes/ behaviors

Cyber insurance pays out in almost all ransomware claims

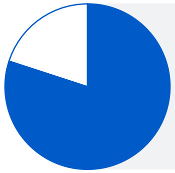
Reassuringly for healthcare organizations with cyber insurance cover, 97% that were hit by ransomware and had cyber insurance that covered ransomware said the policy paid out in the most significant attack. 81% of respondents reported that their insurer paid cleanup costs i.e., costs incurred to get the organization up and running again. Conversely, 47% reported that the insurer paid the ransom. Looking at what cyber insurance coverage paid for across all sectors, the survey reveals an increase in the payment of cleanup costs and a decrease in ransom payments by insurers compared with the findings of our 2020 survey.

However, the rate of ransom payouts varied considerably by sector. The highest rates were reported in lower education (K-12/primary/secondary) at 53%, state/local government at 49%, and healthcare at 47%. The lowest payouts came from manufacturing and production at 30% and financial services at 32%. It's interesting to note that the sectors with the lowest rate of ransom payments are also the ones able to recover fastest from incidents, emphasizing the importance of disaster recovery preparation.

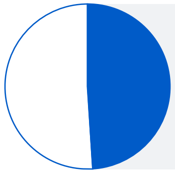
It's worth noting that while cyber insurance can help an organization get to its previous state, it doesn't cover "betterment" i.e., investing in better technologies and services to address weaknesses that led to the attack.



97%
cyber insurance payout
rate in healthcare



81%
insurer paid clean-up costs in healthcare



47%
insurer paid the ransom

Conclusion

The ransomware challenge facing organizations continues to grow. The proportion of healthcare organizations directly impacted by ransomware has almost doubled in 12 months: from just over a third in 2020 to two thirds in 2021.

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

At the same time, the proportion of encrypted healthcare data being restored after paying the ransom has dropped, down to 65% on average.

Healthcare made the lowest average ransom payment (US$197K).

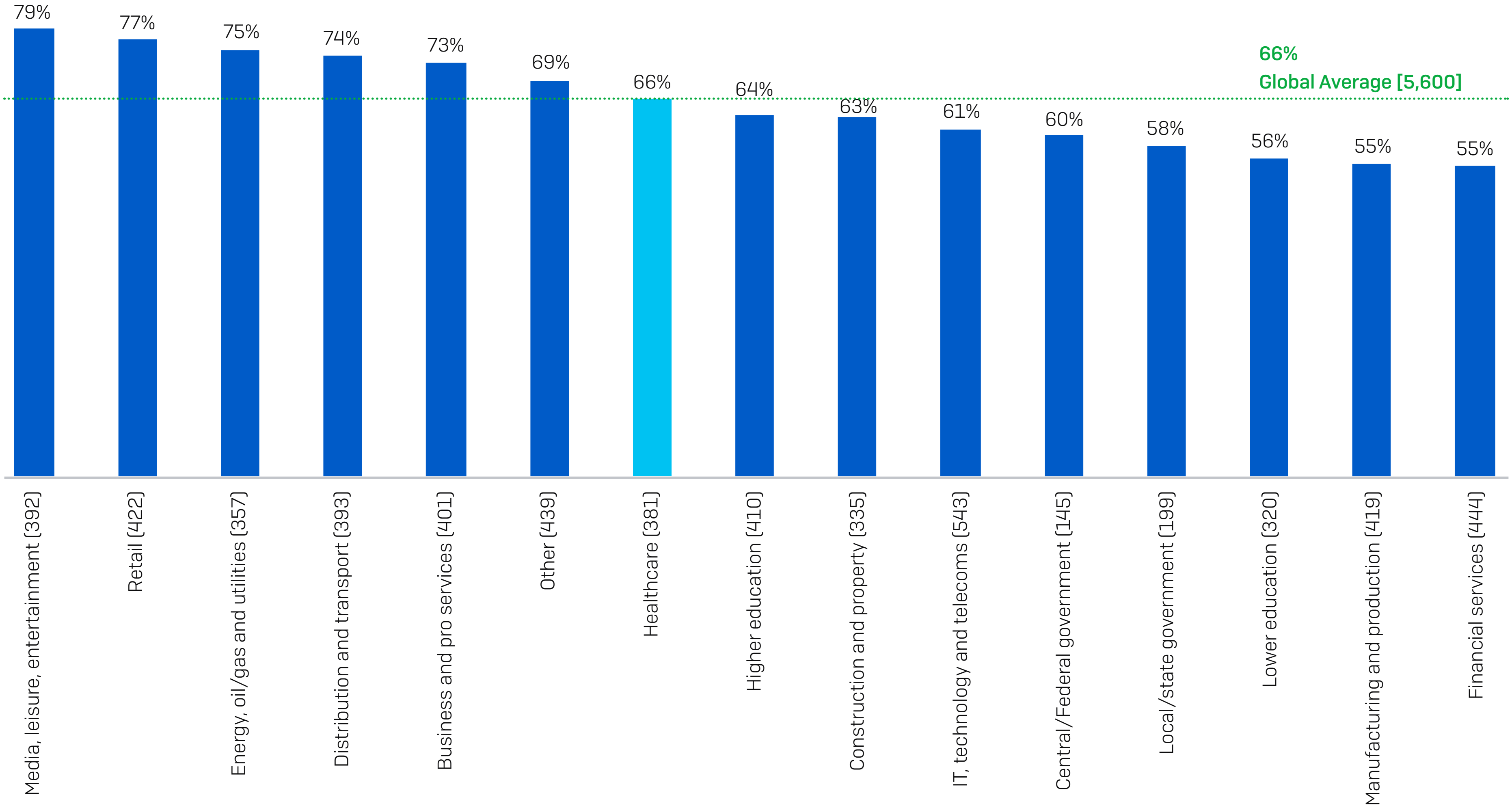
Ransomware impacts healthcare operations, business, and revenue. Most healthcare organizations are choosing to reduce the financial risk associated with such attacks by taking cyber insurance. For them, it is reassuring to know that insurers pay some costs in almost all claims. However, it's getting harder for organizations to secure coverage. This has driven almost all healthcare organizations to make changes to their cyber defenses to improve their cyber insurance position.

Whether you are looking to secure insurance cover or not, optimizing your cybersecurity is imperative for all organizations. 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 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 minimum disruption.

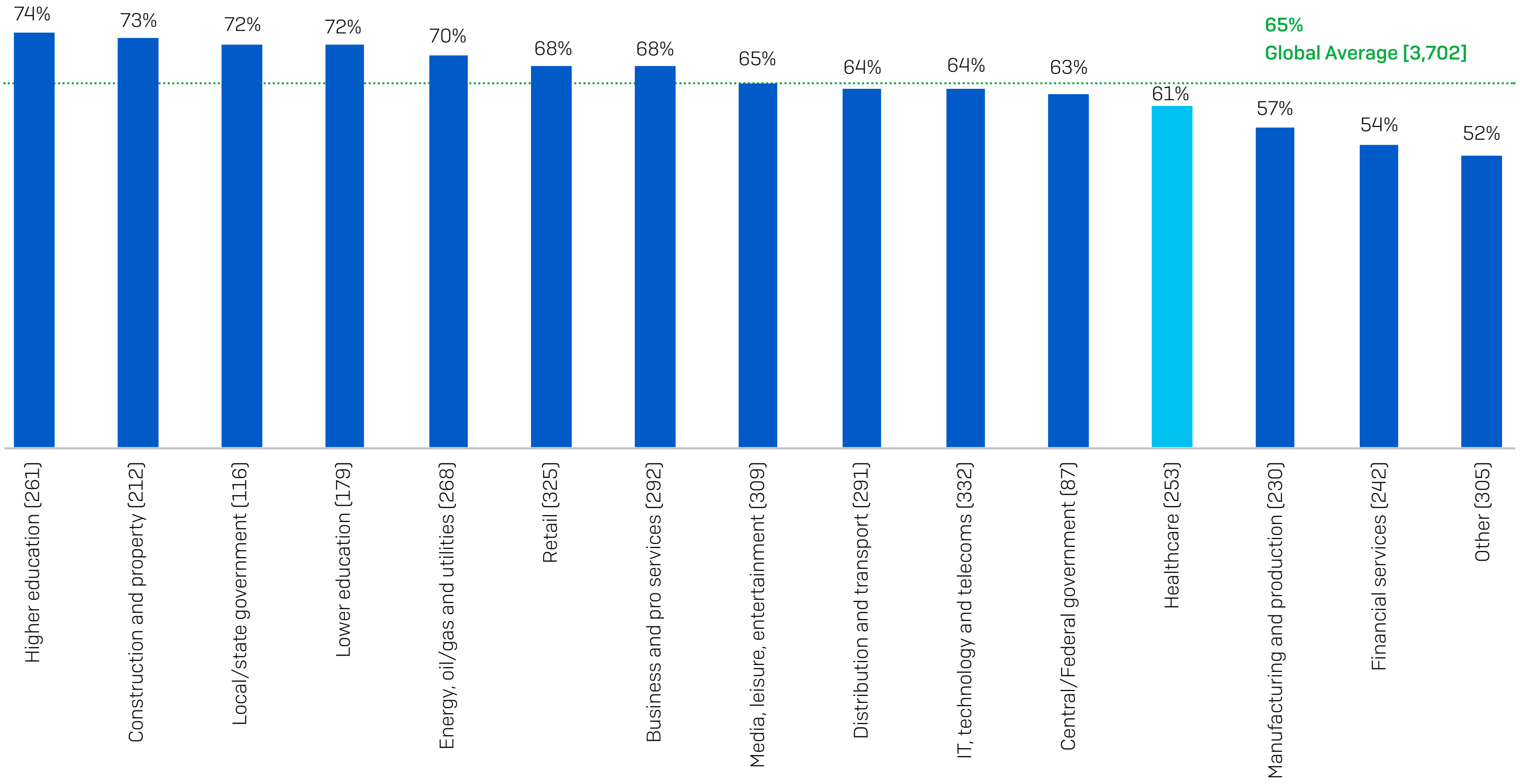
For detailed information on individual ransomware groups, see the Sophos ransomware threat intelligence center.

How Healthcare Stacks: Ransomware Attacks by Sector



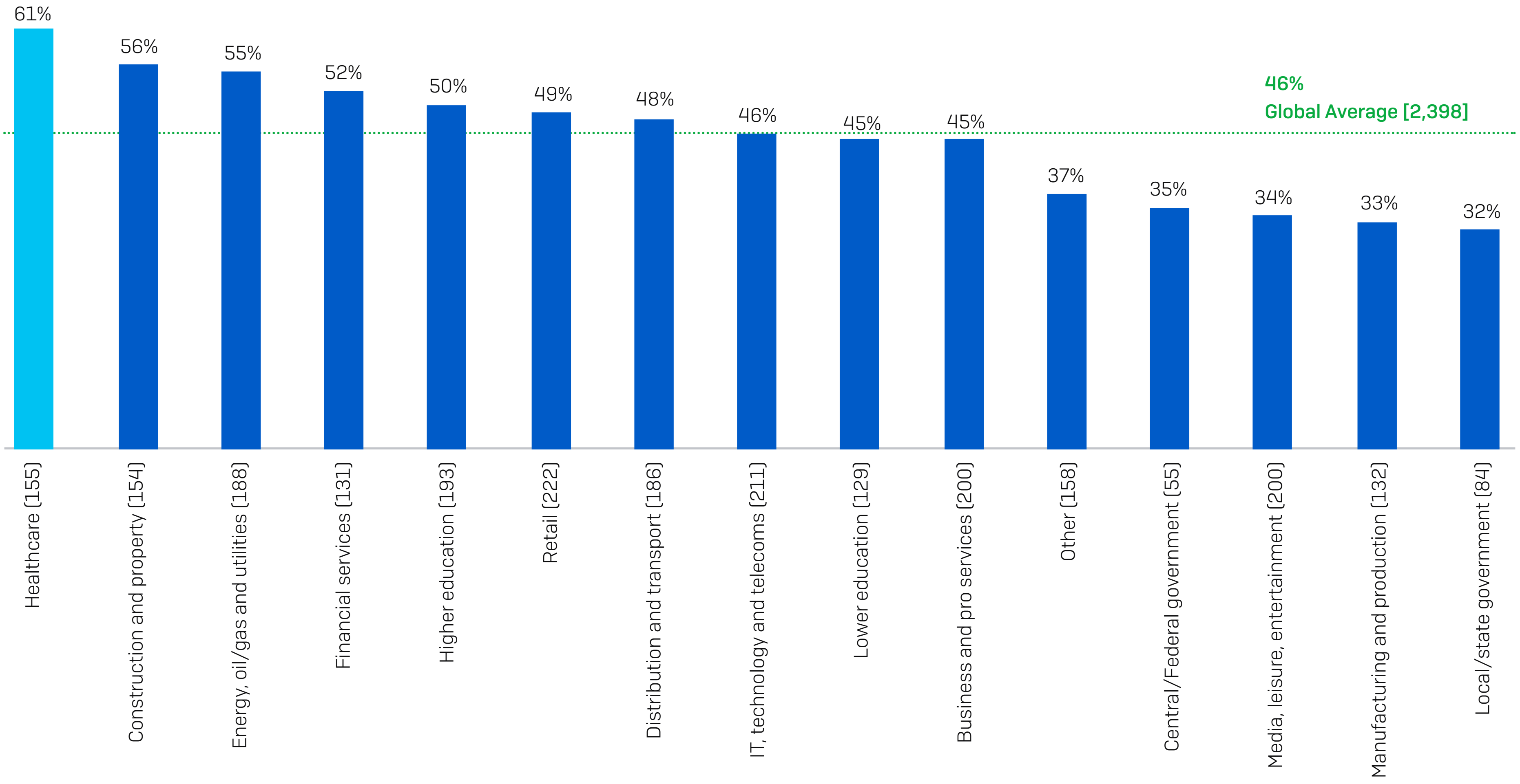
In the last year, has your organization been hit by ransomware? [n=5,600]

How Healthcare Stacks: Data Encryption Rate by Sector



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

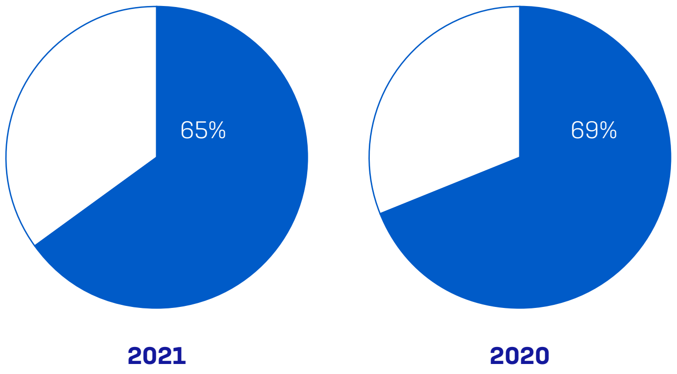
Healthcare Is Most Likely to Pay the Ransom



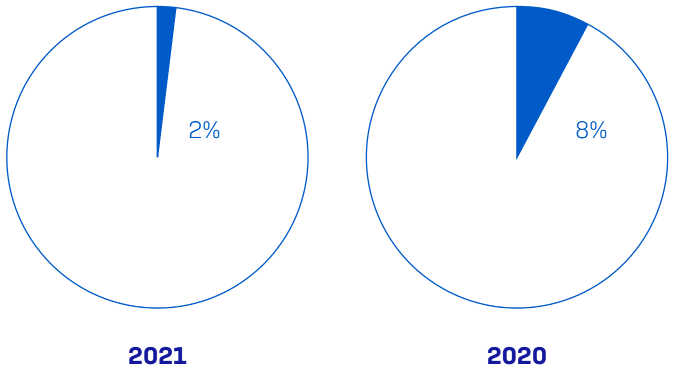
Did your organization get any data back in the most significant ransomware attack?
(n=2,398 organizations that had data encrypted): Yes, we paid the ransom and got data back

Less Data Is Recovered by Healthcare Than In the Previous Year After Paying the Ransom

Percentage of data restored after paying the ransom

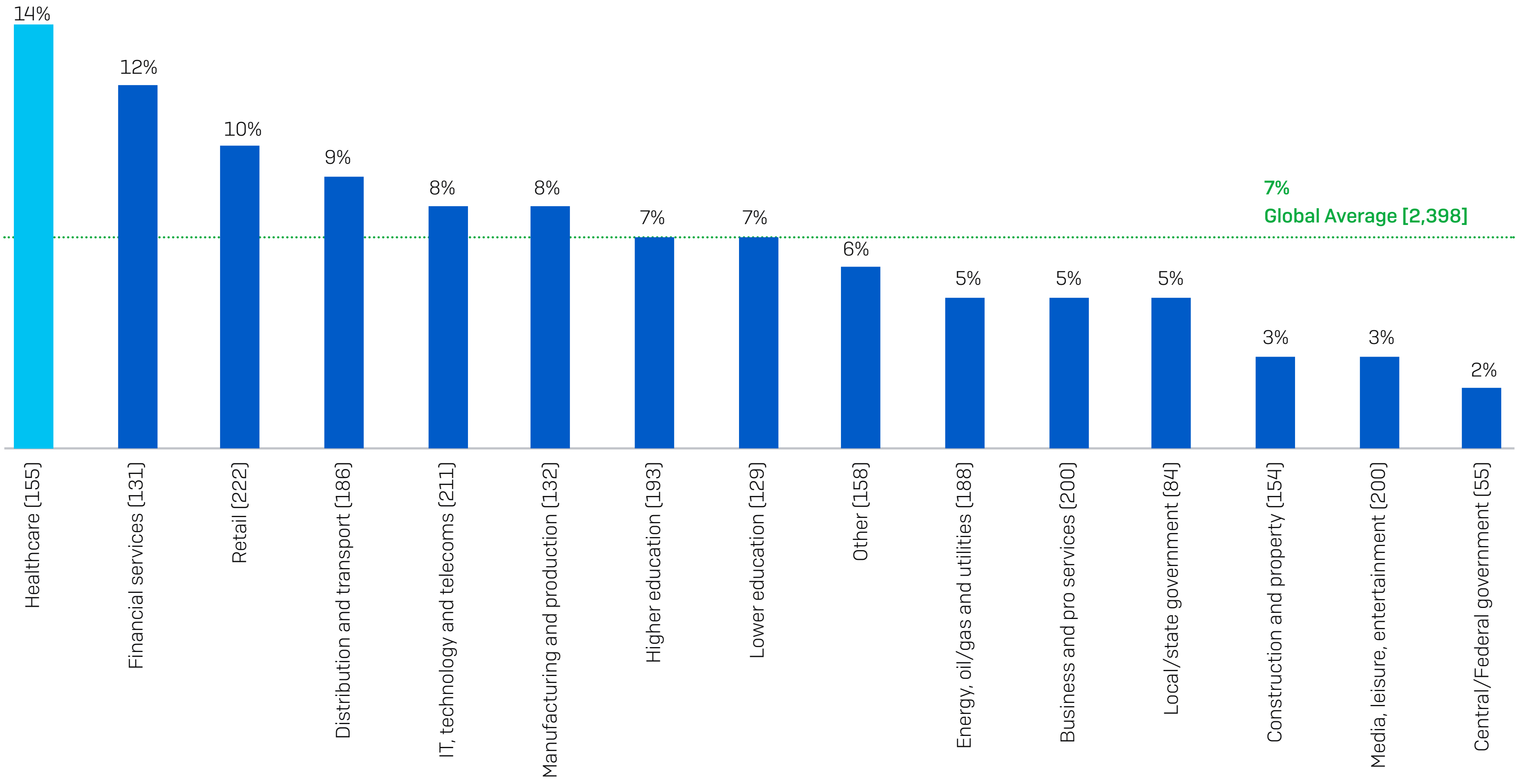


Percentage that got ALL their data back after paying the ransom



How much of your organization's data did you get back in the most significant ransomware attack?
(94/25 healthcare organizations that paid the ransom and got data back)

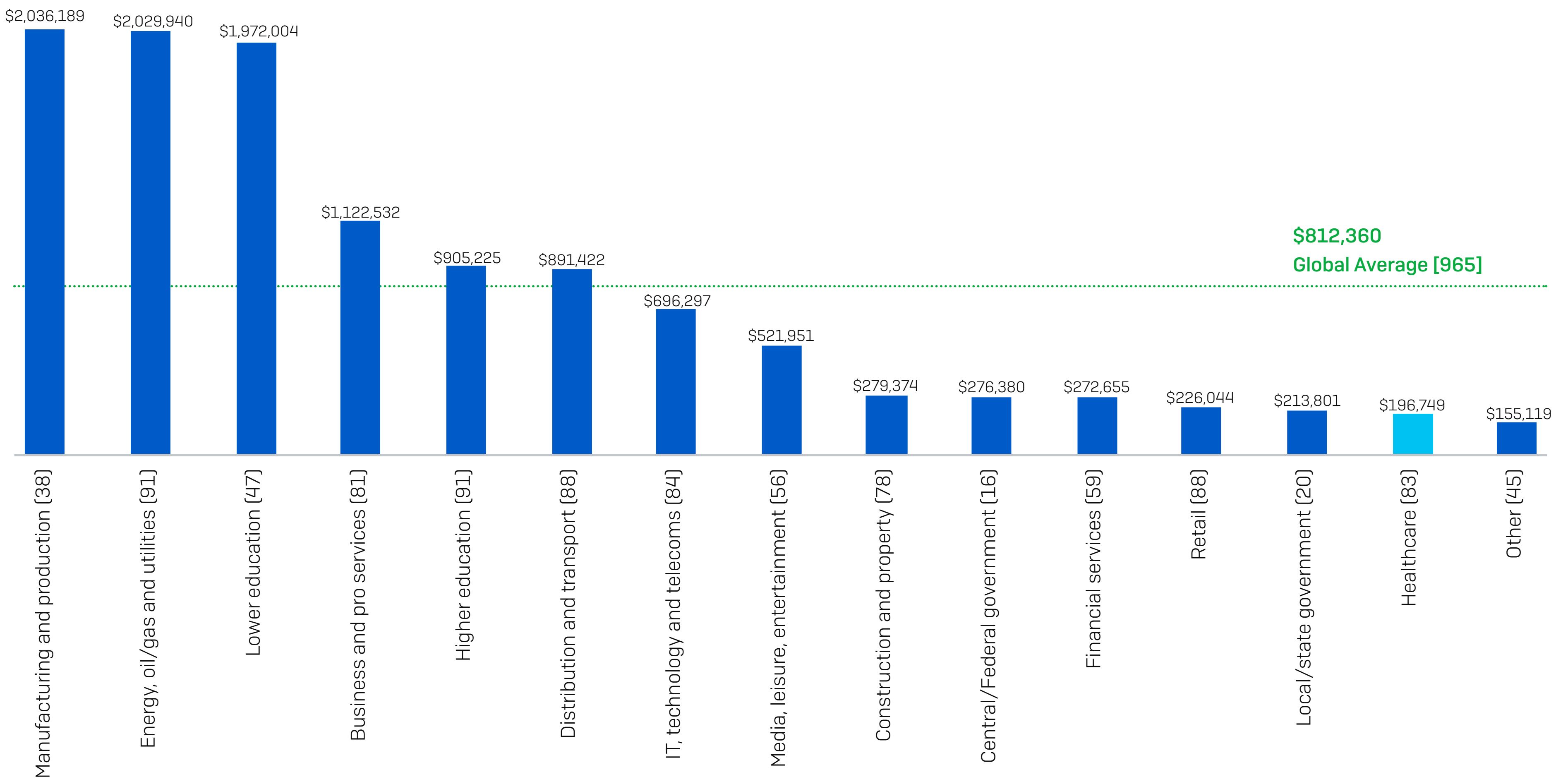
Healthcare Is Most Likely to Use All Three Methods to Restore Data



Did your organization get any data back in the most significant ransomware attack?

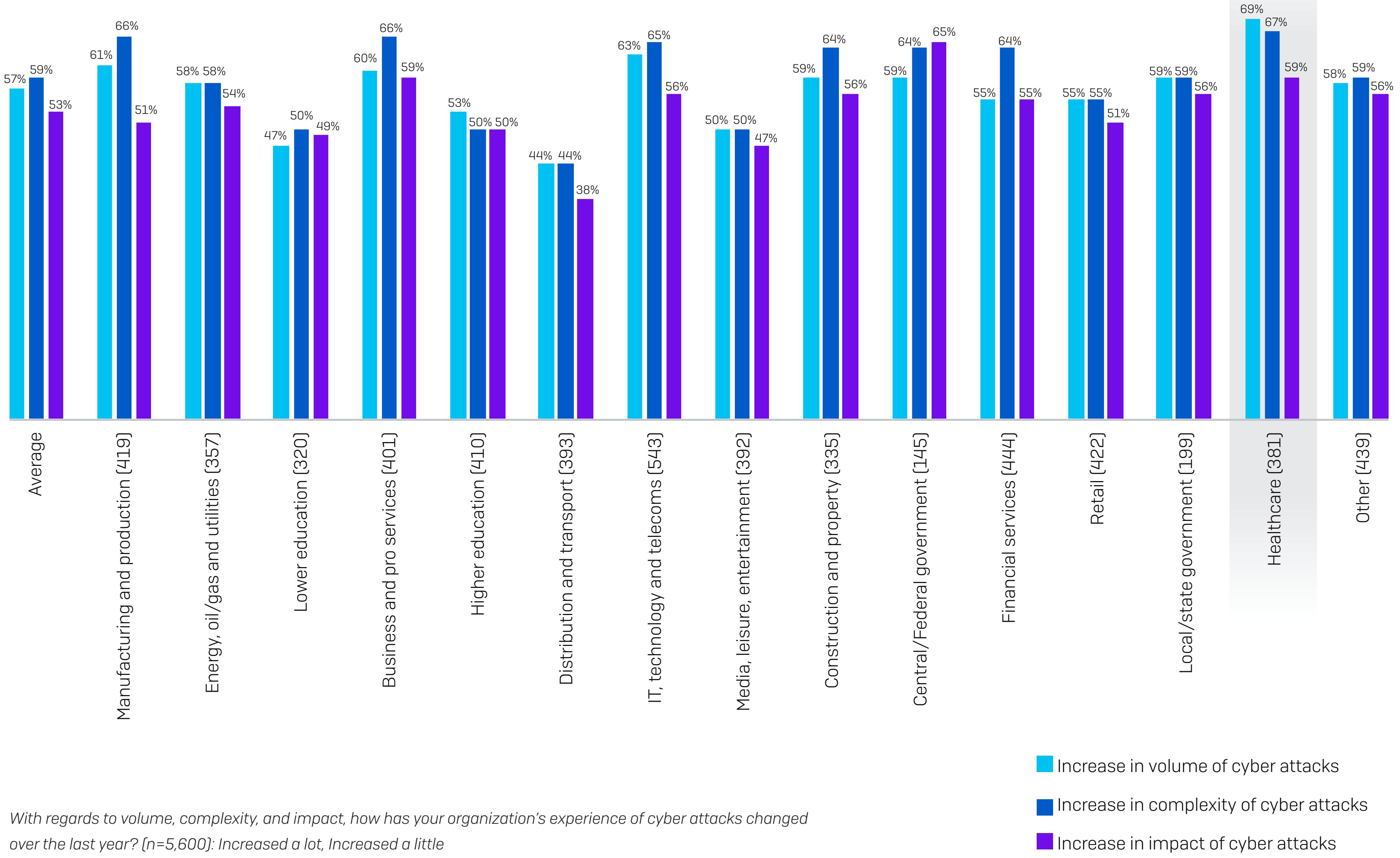
[2,398 organizations that had data encrypted]: Yes, we used all three methods [backups, ransom payment, and other means] of getting the data back

Healthcare Made The Lowest Ransom Payments



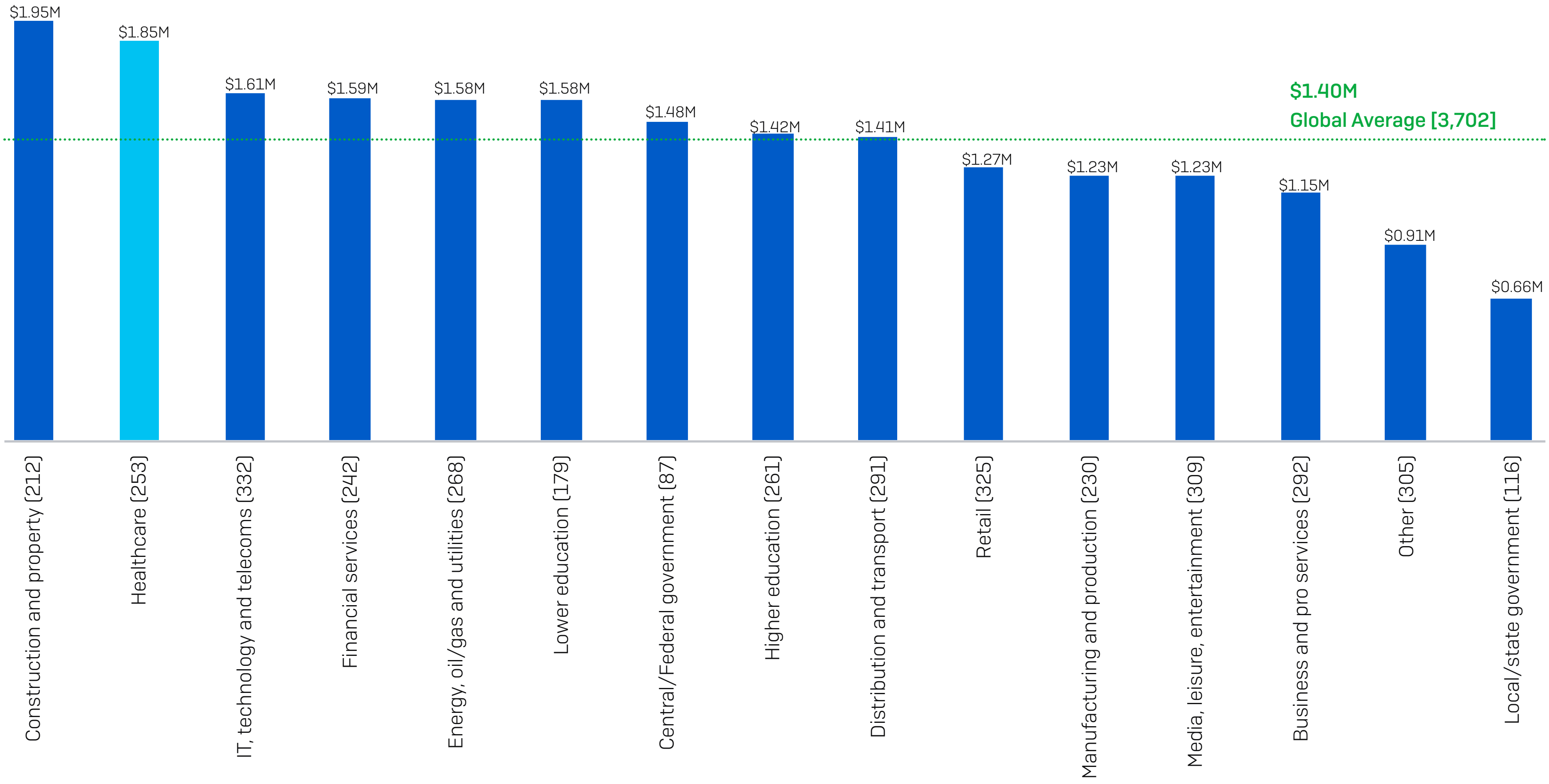
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses.N.B. For sectors with low base numbers, findings should be considered indicative.

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



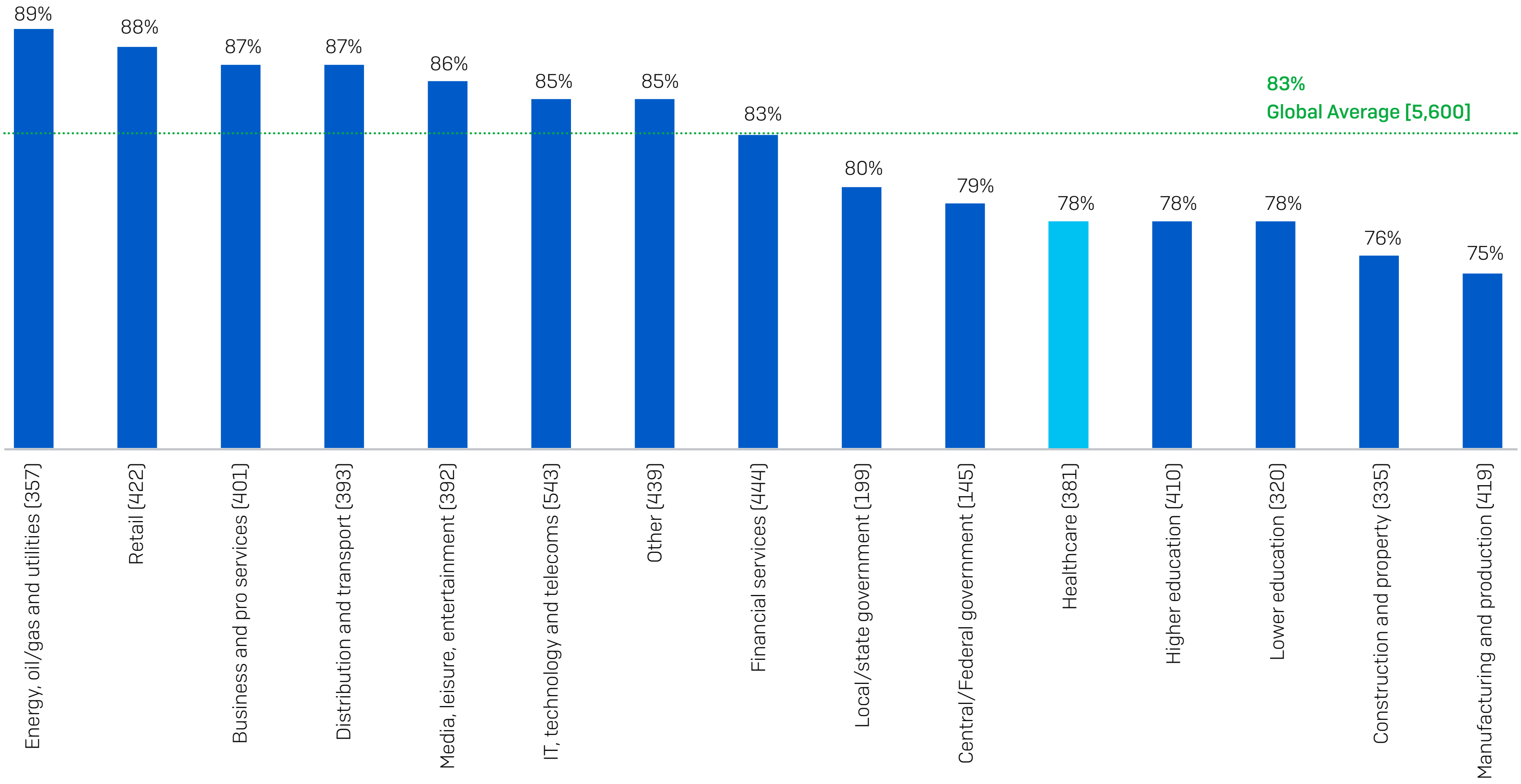
With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600): Increased a lot, Increased a little

Ransomware Remediation Costs in Healthcare Are Above the Global Average



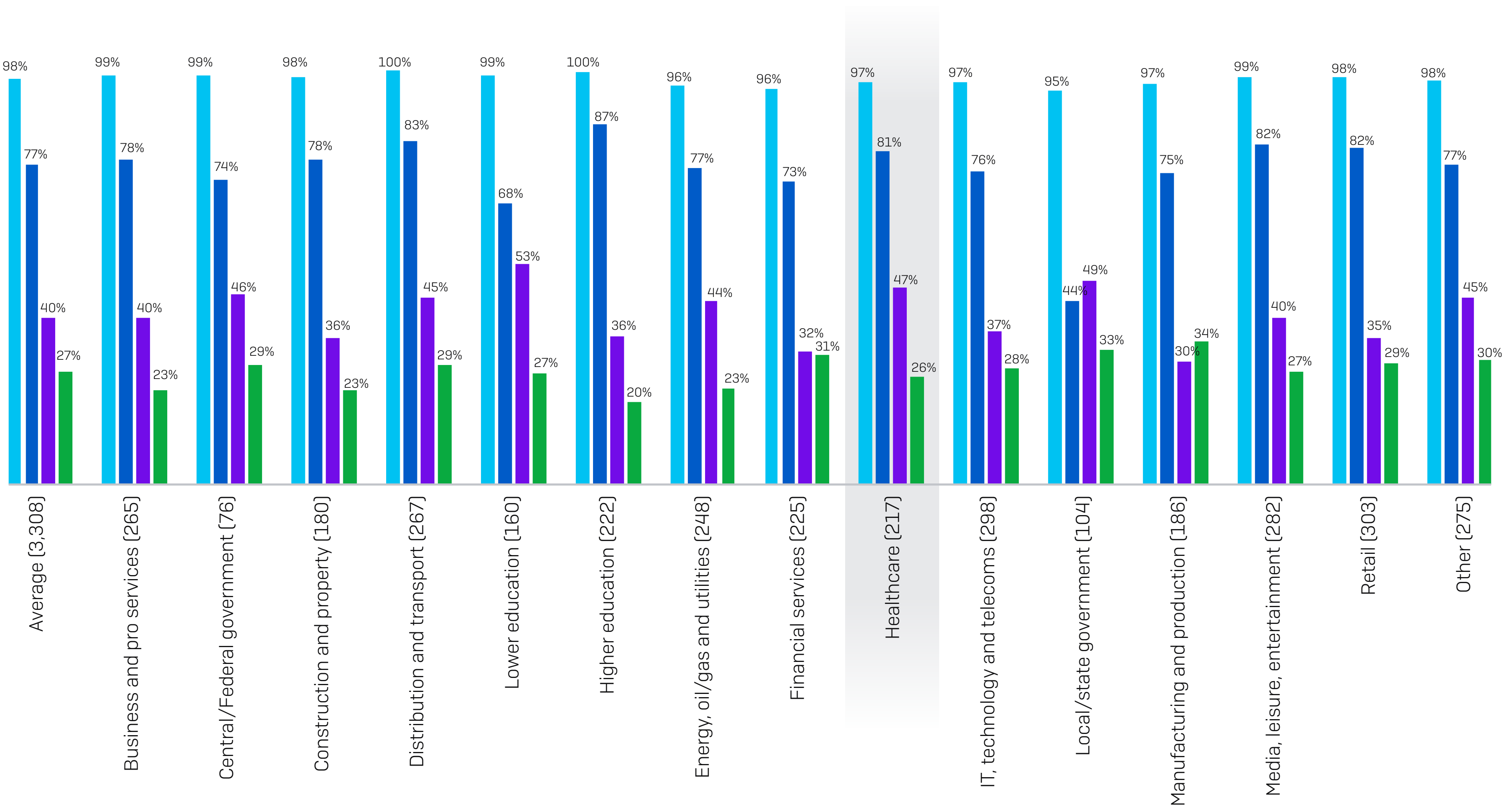
What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time device cost, network cost, lost opportunity, ransomware paid etc.)? (3,702 organizations that were hit by ransomware)

Healthcare Has Below Average Rate of Cyber Insurance Coverage



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 Healthcare 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.]

🟦 Insurance paid out

🟦 Insurance paid clean-up cost

🟪 Insurance paid the ransom

🟩 Insurance paid other costs

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.

2022-05-31 (WP-NP)

SOPHOS