SOPHOS
Cybersecurity delivered.

The State of Ransomware in Financial Services 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries, including 444 respondents from the financial services sector.

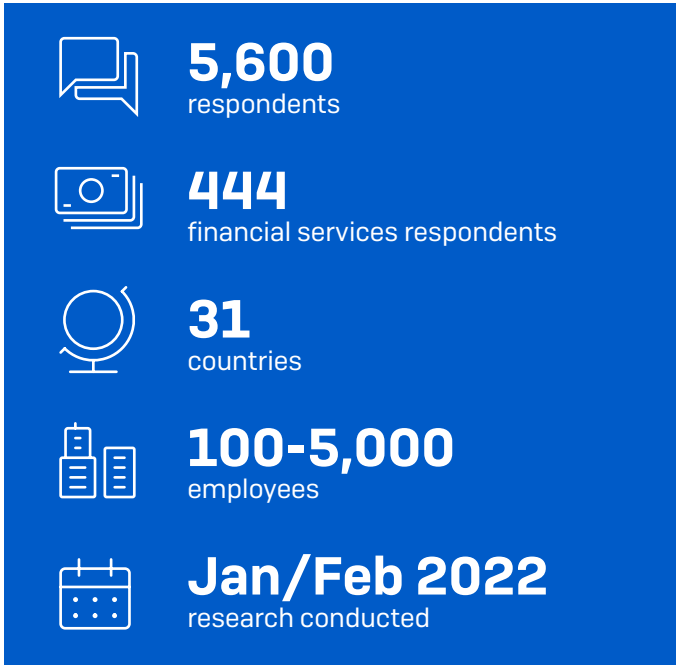
A Sophos Whitepaper. August 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals in the financial services 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 444 from financial services. 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 on financial services have increased

55% of financial services organizations were hit by ransomware in 2021, up from 34% in 2020. This is a 62% rise over the course of a year, demonstrating that adversaries have become considerably more capable of executing attacks at scale. [Note: hit by ransomware was defined as one or more devices being impacted but not necessarily encrypted.]

The increase in propensity to experience a ransomware attack in the financial services sector was part of a broader cross-sector trend in 2021: across all sectors, 66% of respondents reported being hit by ransomware, up from 37% the year before. In fact, despite the jump in the financial services ransomware attack rate, the sector actually reported the lowest rate across all sectors surveyed.

In addition to having the lowest rate of ransomware attacks, financial services organizations also reported the second-lowest rate of data encryption: just over half (54%) of financial services organizations that were hit by ransomware reported that the criminals succeeded in encrypting their data, considerably below the global average of 65%.

Financial services' high success rate in stopping the encryption of data likely indicates strong layered defenses in this sector. It may also be influenced by the increased take-up of cyber insurance in financial services, which often demands higher cyber defenses as a condition of coverage. We will look at this trend later in this report.

The surge in ransomware attacks is part of an increasingly challenging broader threat environment that has affected organizations across all sectors. Over the last year, cyberattacks have increased in volume, complexity, and impact, which in turn increases the challenge for IT teams.

Within the financial services sector 55% of respondents reported an increase in attack volume, 64% reported an increase in attack complexity, and 55% reported an increase in the impact of attacks.

While the increase in volume and impact of attacks is in line with the global average, financial services experienced an above-average increase in the complexity of attacks (64% vs. 59%). It may be that, in response to this sector's strong ability to stop attacks, adversaries are forced to increase the sophistication of their approaches.

Hit by ransomware

55%
financial services – lowest across all sectors

66%
global average

Data encrypted in the attack

54%
financial services – second-lowest across all sectors

65%
global 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
Financial Services	55%	64%	55%
Global average	57%	59%	53%

Most financial services victims get some encrypted data back

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

Backups are the #1 method used to restore data, used by 66% of financial services organizations whose data was encrypted. While it's encouraging that backups are the primary method of recovery, financial services reported one of the lowest levels of backup usage and is considerably below the global average of 73%. The sector should invest in both taking backups and practicing recovering from them as a matter of priority.

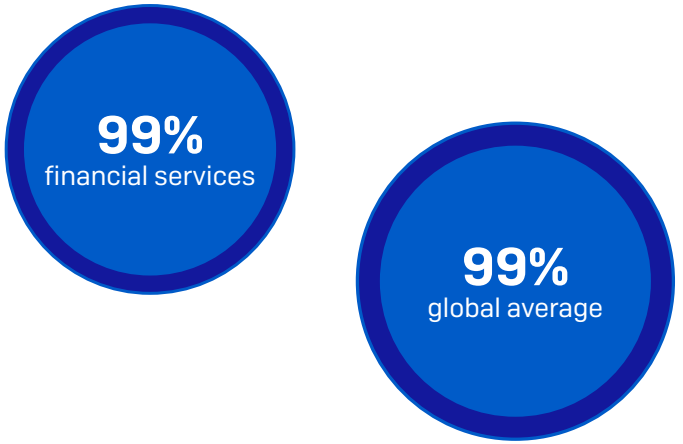
52% of respondents in financial services reported that they paid the ransom to restore data. This is higher than the global average of 46%, likely reflecting the lower rate of backup use. Furthermore, 24% said they used other means to restore encrypted data.

These numbers clearly add up to more than 100%, demonstrating that many organizations use multiple restoration approaches in parallel to maximize the speed and efficacy with which they can get back up and running. While financial services is part of this trend with 31% using multiple methods to restore data, it is the sector least likely to combine approaches in order to accelerate recovery. For comparison, globally 44% use multiple methods to restore data.

Used multiple restoration methods

	PAID THE RANSOM	USED BACKUPS	USED OTHER MEANS	MULTIPLE METHODS USED
Financial services	52%	66%	24%	31%
Global average	46%	73%	30%	44%

Restored some encrypted data



Financial services has above-average data recovery after paying the ransom

Across all sectors, the average amount of data recovered after paying the ransom dropped over the last year, from 65% in 2020 to 61% in 2021.

Financial services respondents that paid the ransom recovered 63% of their data on average in 2021, slightly above the global average of 61%. In fact, the amount of data restored by financial services has remained constant (63%) across 2020 and 2021.

Encouragingly, there has been a considerable increase over the last year in the percentage of financial services organizations that got ALL their encrypted data back, up from 4% in 2020 to 10% in 2021. For comparison, the global average in 2021 was just 4%. This suggests that financial services has an above-average ability to restore encrypted data once the cybercriminals provide the decryption key.

That being said, it's important to note that nine in ten financial services organizations that paid the ransom did not get all their data back. 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

63%
financial services

61%
global average

The percentage that got ALL data back after paying the ransom

10%
financial services

4%
global average

Financial services' ransom payment rate has more than doubled

Financial services is one of the sectors most likely to pay the ransom to get their encrypted data back after a ransomware attack. The sector reported a 52% rate of ransom payment compared to the global average of 46%.

What's particularly notable is that the rate of ransom payment by the financial services sector has more than doubled in the last year: up from 25% in 2020 to 52% in 2021. At the same time, the ability to restore encrypted data using backups increased only slightly, up from 62% in 2020 to 66% in 2021.

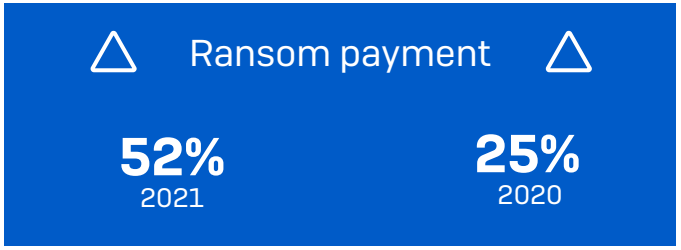
The slow progress in backup use together with the above-average increase in the complexity of cyberattacks in this sector in 2021 may have contributed to the increased propensity of financial services organizations to pay the ransom to get their data back.

Ransom payment rate

52%
financial services

46%
global average

Ransom payment rate doubled in the last year



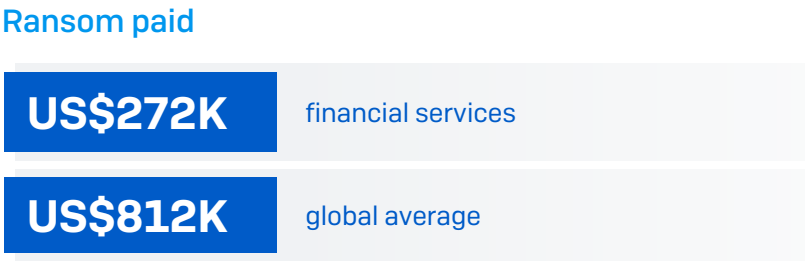
Financial services made below-average ransom payments

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).

59 respondents from financial services shared the exact ransom payment made, revealing that the average payment for the sector was just one-third of the global average, coming in at $272,655.

While it is encouraging to note that the ransom payments are considerably below average, $272,655 is a considerable sum of money for a small/mid-sized financial services organization and can have a major impact on their cash flow and commercial success.

Furthermore, $272,655 is more than double the average ransom payment of $128,066 reported last year by the 13 financial services respondents who shared the exact ransom amount. While last year's figure is not statistically significant due to the low response base, it indicates that financial services has been impacted by the global trend of increased ransom sums.



Ransomware has considerable financial, commercial and operational impact on financial services

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

91% of financial services organizations hit by ransomware said the attack impacted their ability to operate, while 85% said the attack cause their organization to lose business/revenue. These data points are in line with the global average.

In terms of the overall cost to remediate the ransomware attack, financial services organizations reported a drop of almost a quarter over the last year, down from US$2.1M in 2020 to US$1.59 in 2021. While a welcome reduction, the average remediation cost in this sector remains above the global average of US$1.4M.

The high level of regulation in this sector coupled with severe penalties for data loss and non-compliance with critical regulations likely contribute to this high bill for the sector. Also, as we will see later, the financial services sector reported one of the lowest cyber insurance payout rates for clean-up costs and ransom, increasing the financial burden on the victim. The above-average increase in the complexity of ransomware attacks on financial services may also have had a commensurate impact on recovery costs.

Turning to the time taken to recover from a ransomware attack, financial services has a strong ability to recover quickly with over six in ten (62% with rounding) recovering within a week from the most significant attack, compared to 53% on average across all sectors. Similarly, just 12% (with rounding) said it took them between one and six months to recover, compared to the global average of 20%.

The fast response capabilities reported indicate strong resilience and disaster recovery preparation in this sector, likely driven in part by regulatory compliance requirements. Financial services organizations should continue to maintain focus in this area as it will help lower the impact and cost of an attack on their organization.

Impact on the ability to operate

91%
financial services

90%
global average

Impact on business/revenue

85%
financial services

86%
global average

The average cost to remediate attacks

US$1.59M financial services

US$1.40M global average

Time to recover from ransomware attacks

DURATION	FINANCIAL SERVICES	GLOBAL AVERAGE
Within a week	62%	53%
1-6 months	12%	20%

Process for securing cyber insurance coverage has changed considerably

83% of respondents from the financial services sector said their organization had cyber insurance coverage against ransomware, in line with the global average.

For 92% of those with cyber insurance in financial services, the process for securing coverage changed over the last year:

- 36% said fewer insurance providers are offering cyber insurance
- 52% said the level of cybersecurity they need to qualify for cyber insurance is now higher
- 50% said policies are now more complex
- 39% 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. Having strong cyber defenses will significantly improve an organization's ability to secure the coverage they need.

Cyber insurance is driving financial services to improve cyber defenses

The challenging cyber insurance market is driving financial services organizations to improve their cyber defenses: over the last year, 98% of financial services organizations have made changes to their cyber defenses to secure coverage.

Diving into the details, 66% of financial services 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, 59% in financial services have invested in this area. 51% have changed processes/ behaviors.

Cyber insurance drives improvement in cyber defenses

	HAVE CHANGED CYBER DEFENSES TO IMPROVE INSURANCE POSITION	HAVE IMPLEMENTED NEW TECHNOLOGIES/ SERVICES	HAVE INCREASED STAFF TRAINING/ EDUCATION ACTIVITIES	HAVE CHANGED PROCESSES/ BEHAVIORS
Financial services	98%	66%	59%	51%
Global average	97%	64%	56%	52%

Financial services has one of the lowest ransom payout rates

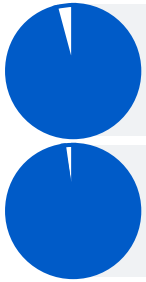
Across all sectors, cyber insurance almost always pays out towards some costs in the event of a ransomware attack. Financial services organizations with cyber insurance reported a 96% payout rate, slightly below the global average of 98%.

Notably, financial services reported a ransom payment rate that is one-fifth lower than the global average, with 32% saying the insurance paid the ransom compared to 40% across all sectors. This is a surprising finding given that financial services reported an above-average ransom payment rate and suggests that the victims are often paying the ransoms out of their own funds.

Financial services organizations that invest in cyber insurance should take the time to review the details of their policy to ensure that their coverage aligns with their requirements and will support them in the event of a major incident.

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:



96%
financial services

98%
global average

Clean-up costs payout:

73%
financial services

77%
global average

Ransom payout:

32%
financial services

40%
global average

Conclusion

The ransomware challenge facing financial services organizations continues to grow. The proportion of organizations hit by ransomware has increased considerable 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, financial services 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, however financial services reported the lowest level of backup use of all sectors.

Financial services has an above-average rate of ransom payment, with 52% paying compared to the global average of 46%. At the same time, the average ransom paid in this sector was just one-third of the global average. The proportion of encrypted data restored by financial services after paying the ransom is slightly above the global average: 63% vs 61%.

While the overall cost to remediate a ransomware attack in financial services fell by almost a quarter over the last year (down from US$2.1M in 2020 to US$1.59 in 2021), it remains considerably higher than the global average of US$1.4M.

Many financial services organizations are choosing 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, the sector has one of the lowest ransom payout rates.

It is getting harder for organizations especially in the financial services sector to secure coverage. This has driven almost all financial services organizations to make changes to their cyber defenses to improve their cyber insurance position.

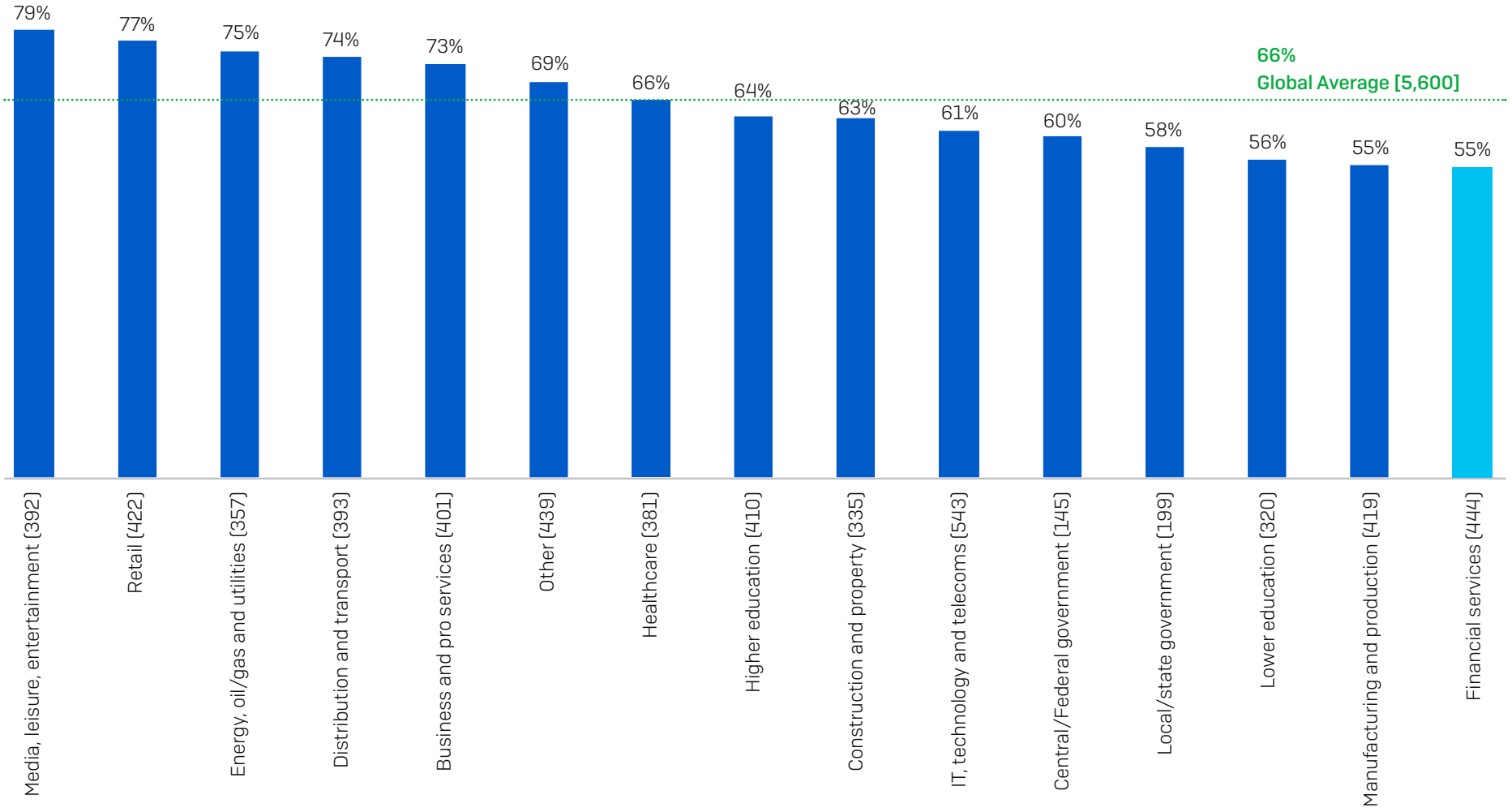
Recommendations

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.

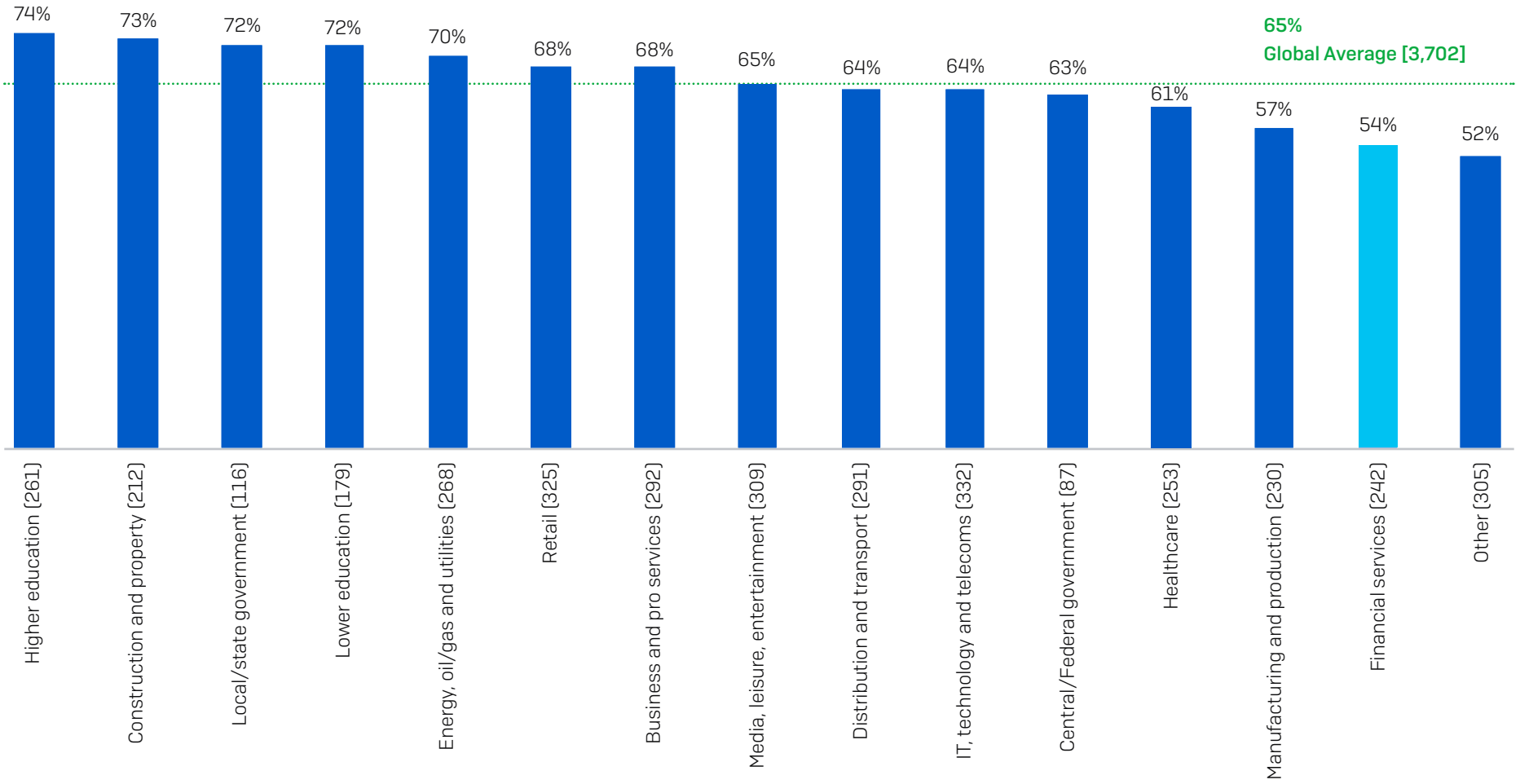
For detailed information on individual ransomware groups, see the Sophos ransomware threat intelligence center.

Financial Services Has Lowest Rate of Ransomware Attacks



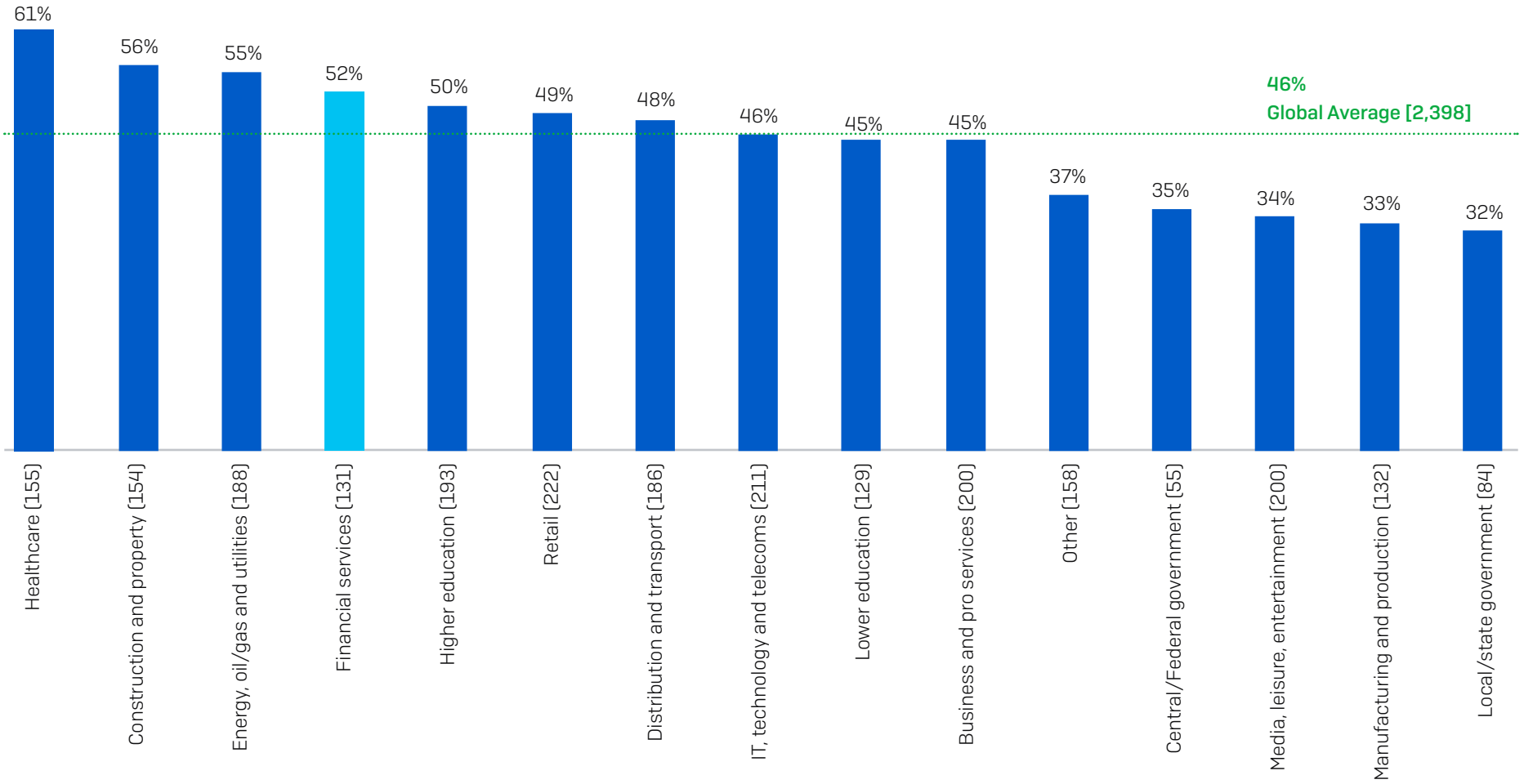
In the last year, has your organization been hit by ransomware? [n=5,600]

Financial Services Has Low Data Encryption Rate



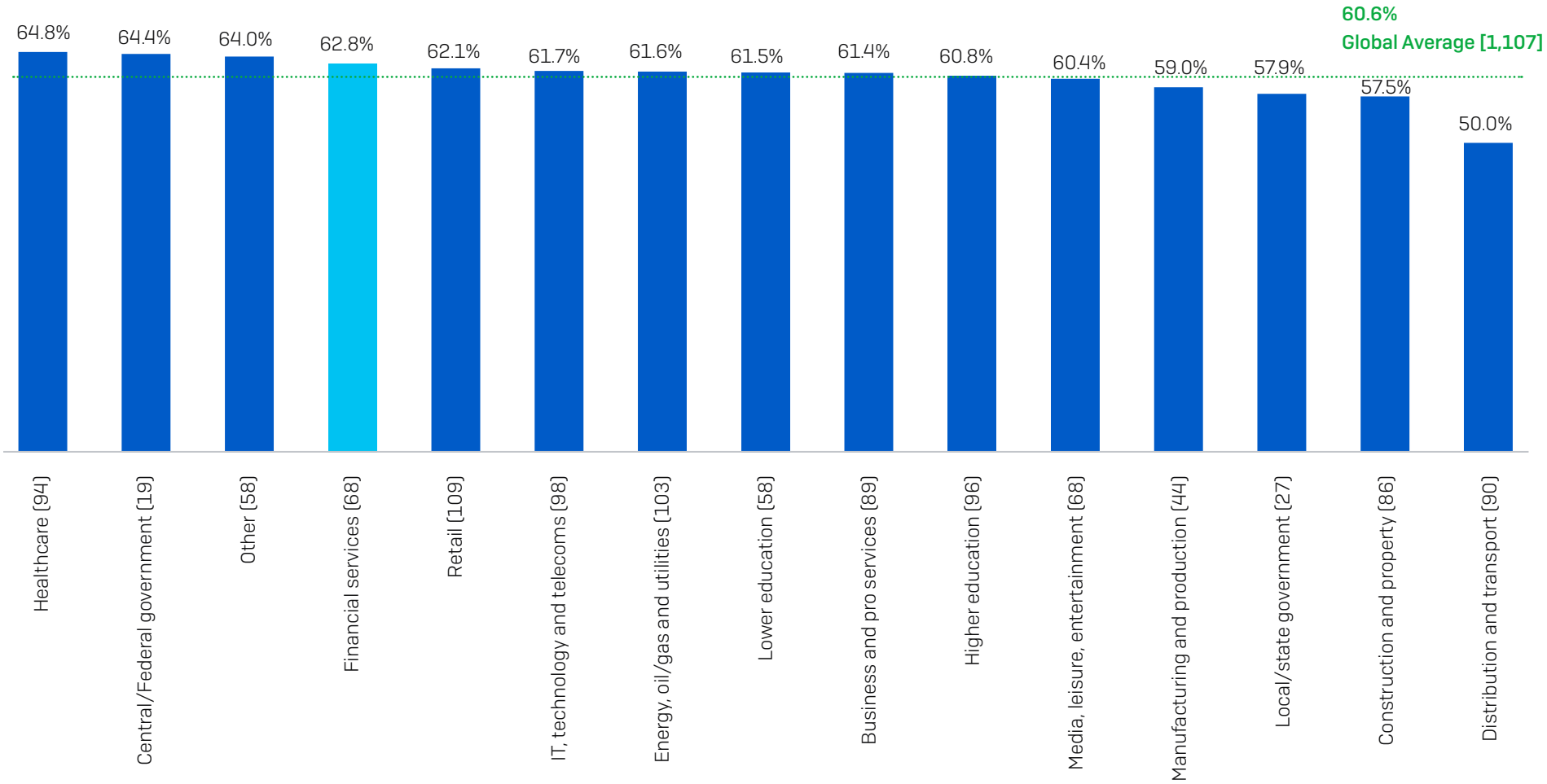
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

Financial Services 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

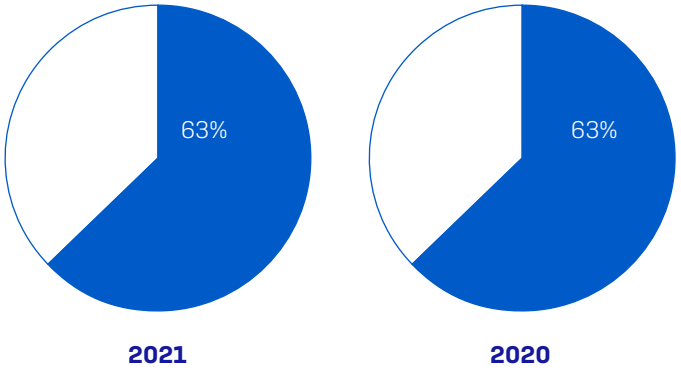
Financial Services Got More Data Back Than Average After Paying the Ransom



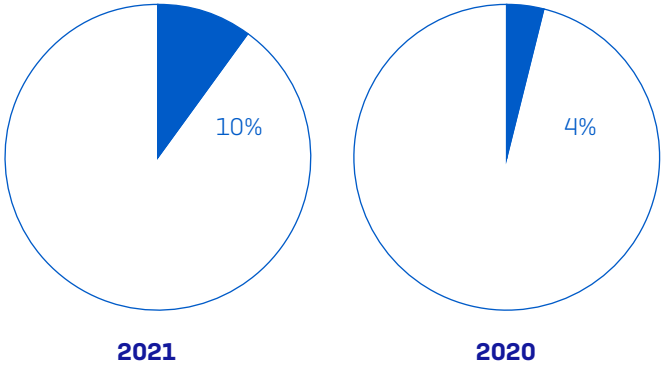
How much of your organization's data did you get back in the most significant ransomware attack? (1,107 organizations that paid the ransom and got data back)

One in Ten Financial Services Victims Got All Their Data Back

Percentage of data restored after paying the ransom

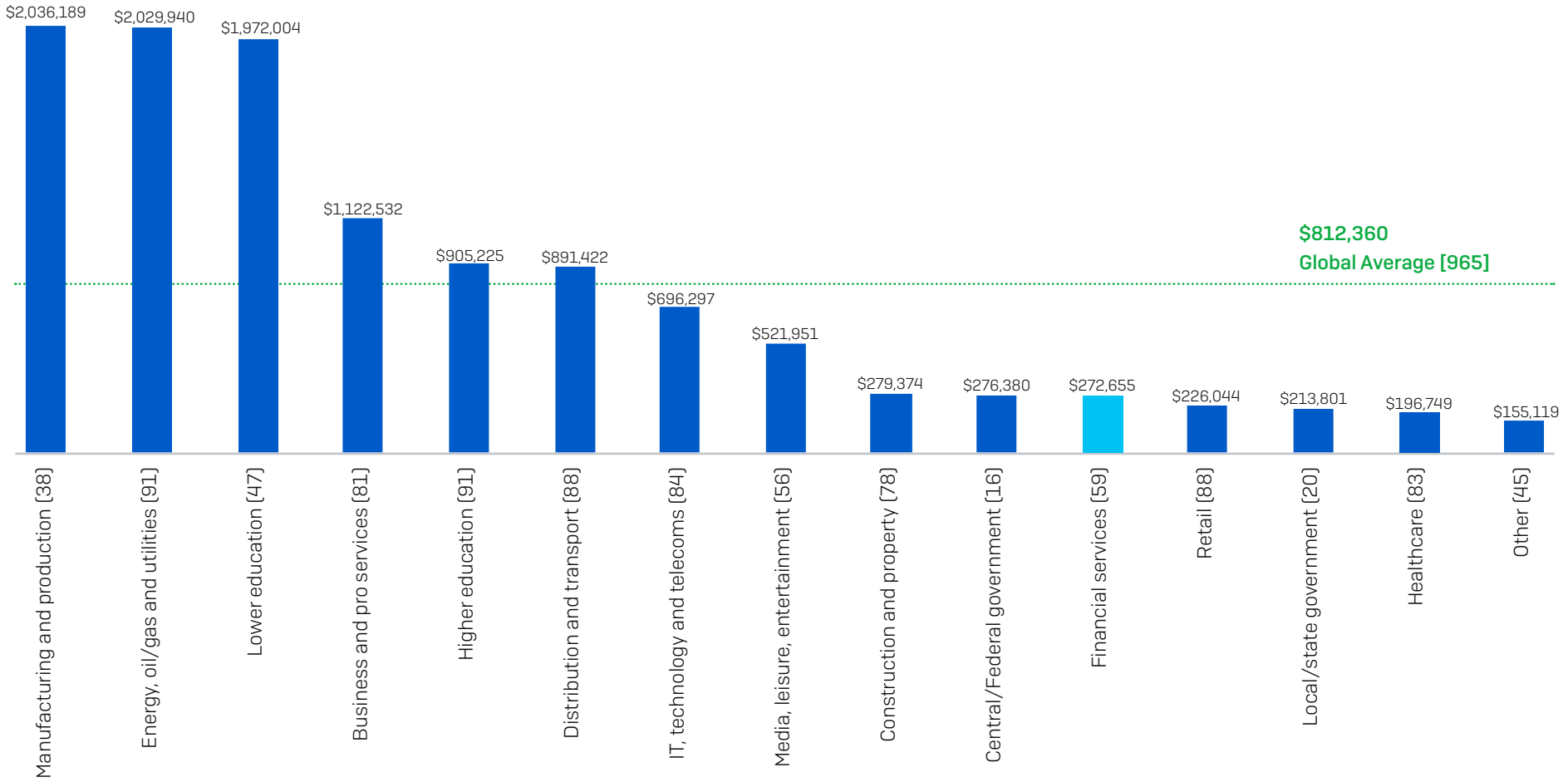


Percentage that got ALL their data back after paying the ransom



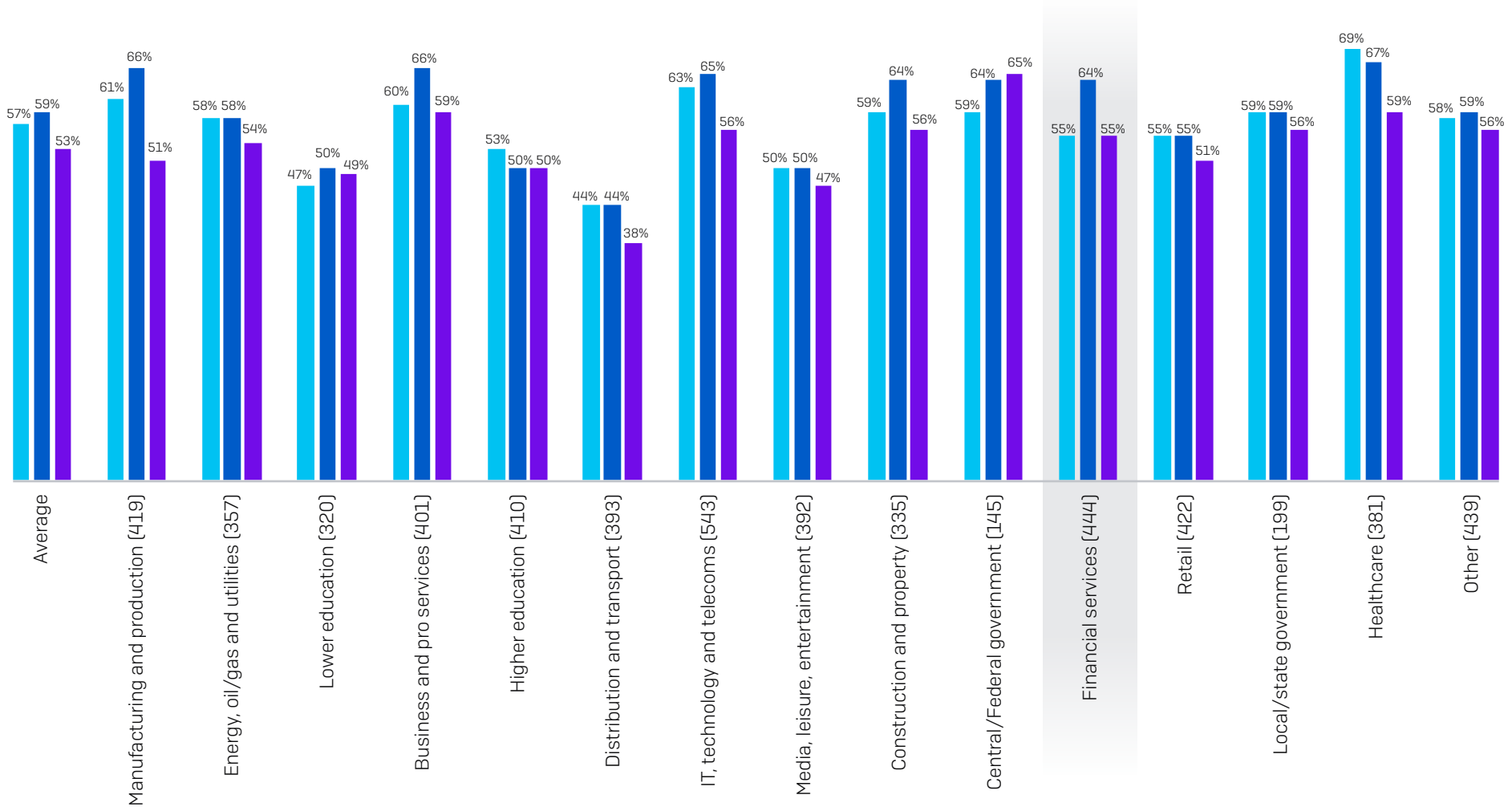
How much of your organization's data did you get back in the most significant ransomware attack? (68/ 24 financial services organizations that paid the ransom and got data back)

Financial Services Made Low Ransom Payments



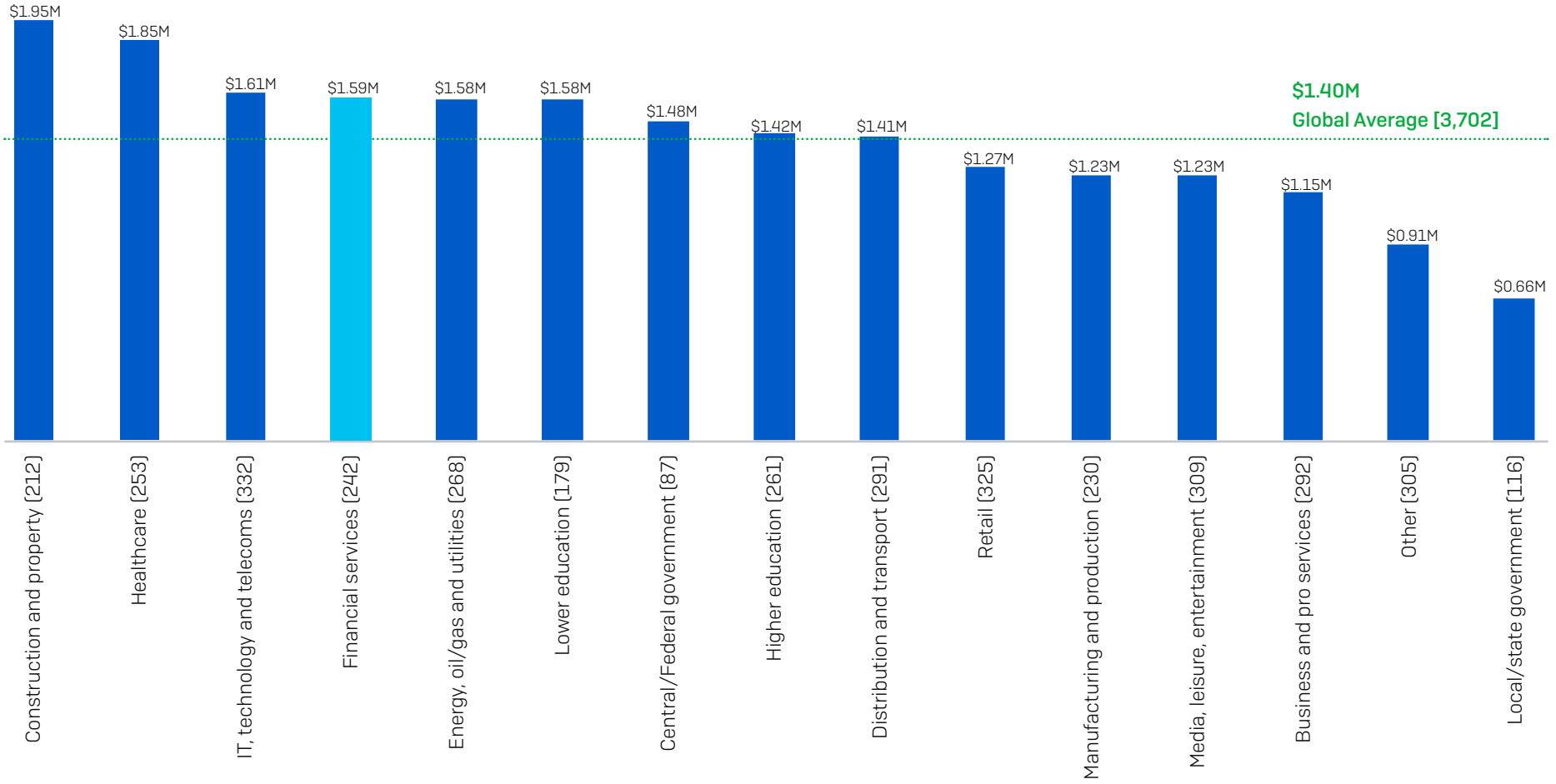
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Base number in chart. Excluding "Don't know" responses.N.B. For sectors with low base numbers, findings should be considered indicative.

How Financial Services Stacks: Changing Experience of Attacks



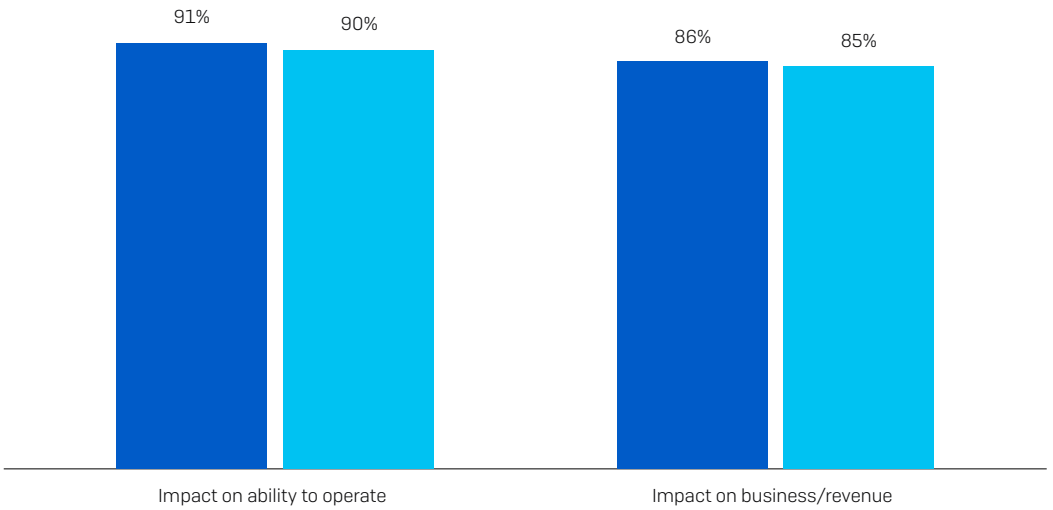
With regards to volume, complexity, and impact, how has your organization's experience of cyber attacks changed over the last year? (n=5,600): Increased a lot, Increased a little

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

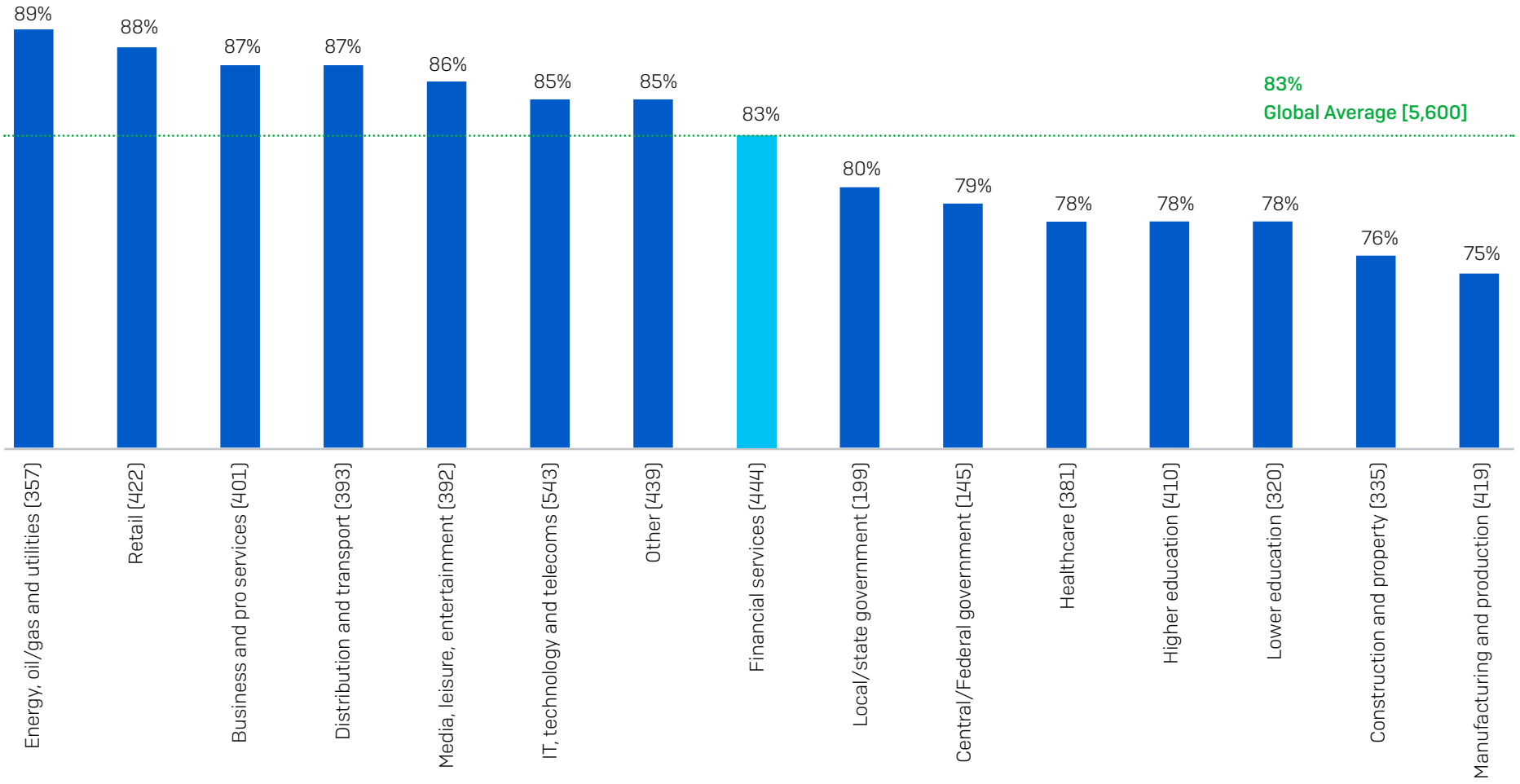
Operational/Commercial Impact of Ransomware on Financial Services



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; 242 financial services organizations that where hit by ransomware in the previous year) Excluding some answer options.

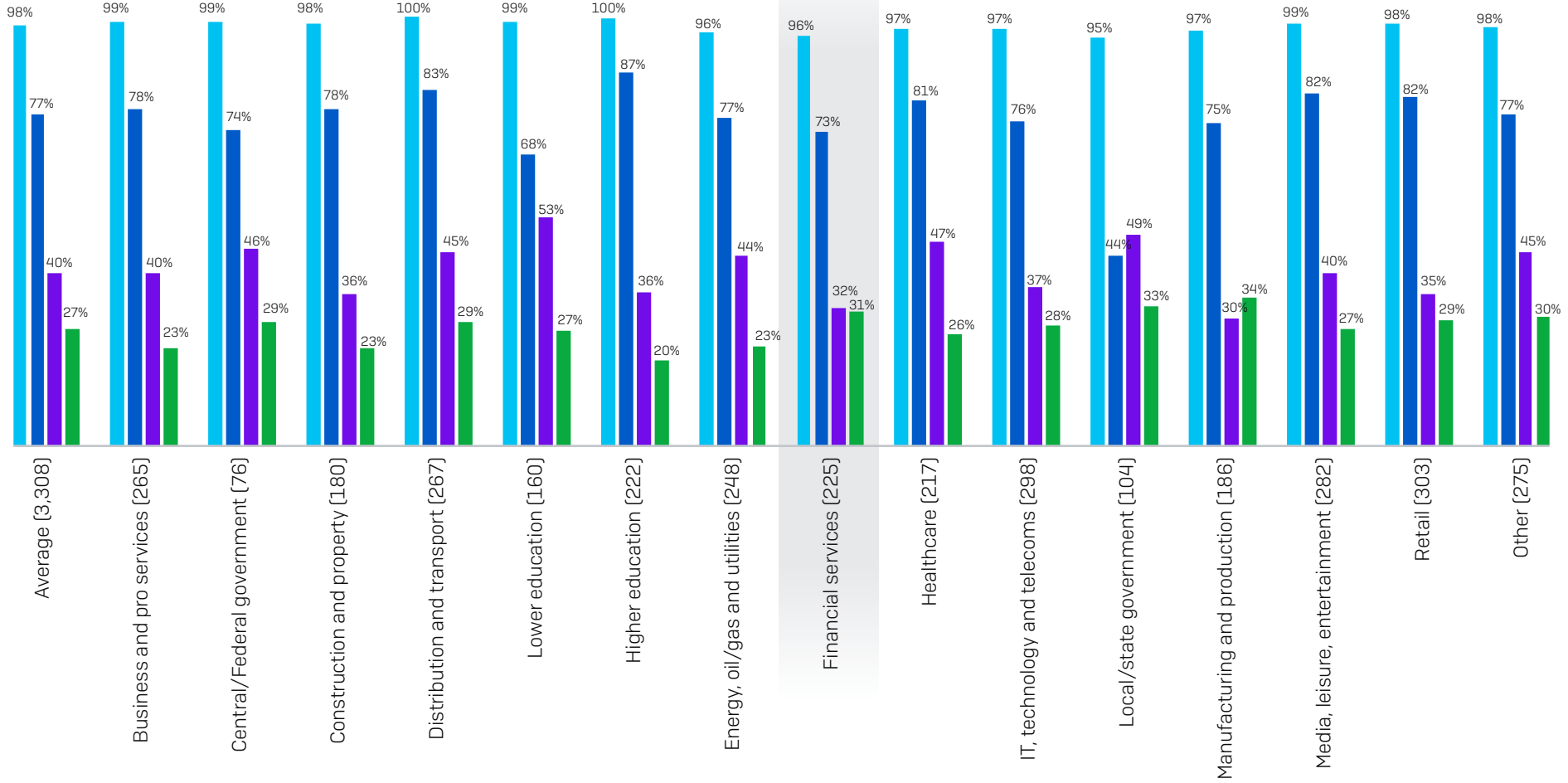
Financial Services Has Average Rate of Cyber Insurance Coverage for Ransomware



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 Financial Services 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.

© Copyright 2022. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

2022-07-20 (WP-NP)

SOPHOS