SOPHOS
Cybersecurity delivered.

The State of Ransomware 2022

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

A Sophos Whitepaper. April 2022

Introduction

Sophos' annual study of the real-world ransomware experiences of IT professionals 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. It also shines new light on the relationship between ransomware and cyber insurance, and the role insurance is playing in driving changes to cyber defenses.

About the survey

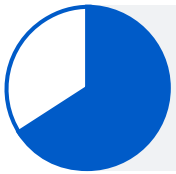
Sophos commissioned research agency Vanson Bourne to conduct an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations (100-5,000 employees) across 31 countries. The survey was conducted during January and February 2022, and respondents were asked to respond based on their experiences over the previous year.

Attacks are up and their complexity and impact are increasing

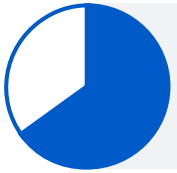
66% of organizations were hit by ransomware in the last year, up from 37% in 2020. This is a 78% increase over the course of a year, demonstrating that adversaries have become considerably more capable at executing the most significant attacks at scale. This likely also reflects the growing success of the Ransomware-as-a-Service model which significantly extends the reach of ransomware by reducing the skill level required to deploy an attack. [Note: hit by ransomware was defined as one or more devices impacted by the attack but not necessarily encrypted.]

Adversaries have also become more successful at encrypting data in their attacks. In 2021 attackers succeeded in encrypting data in 65% of attacks, an increase on the 54% encryption rate reported in 2020. However, there was a reduction from 7% to 4% in the percentage of victims that experienced an extortion-only attack where data was not encrypted but the organization was held to ransom with the threat of exposing data.

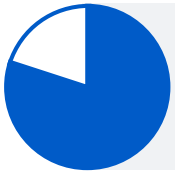
The increase in successful ransomware attacks is part of an increasingly challenging broader threat environment: over the last year 57% experienced an increase in the volume of cyberattacks overall, 59% saw the complexity of attacks increase, and 53% said the impact of attacks had increased. 72% saw an increase in at least one of these areas.



66%
hit by ransomware in the last year



65%
attacks resulted in data encryption



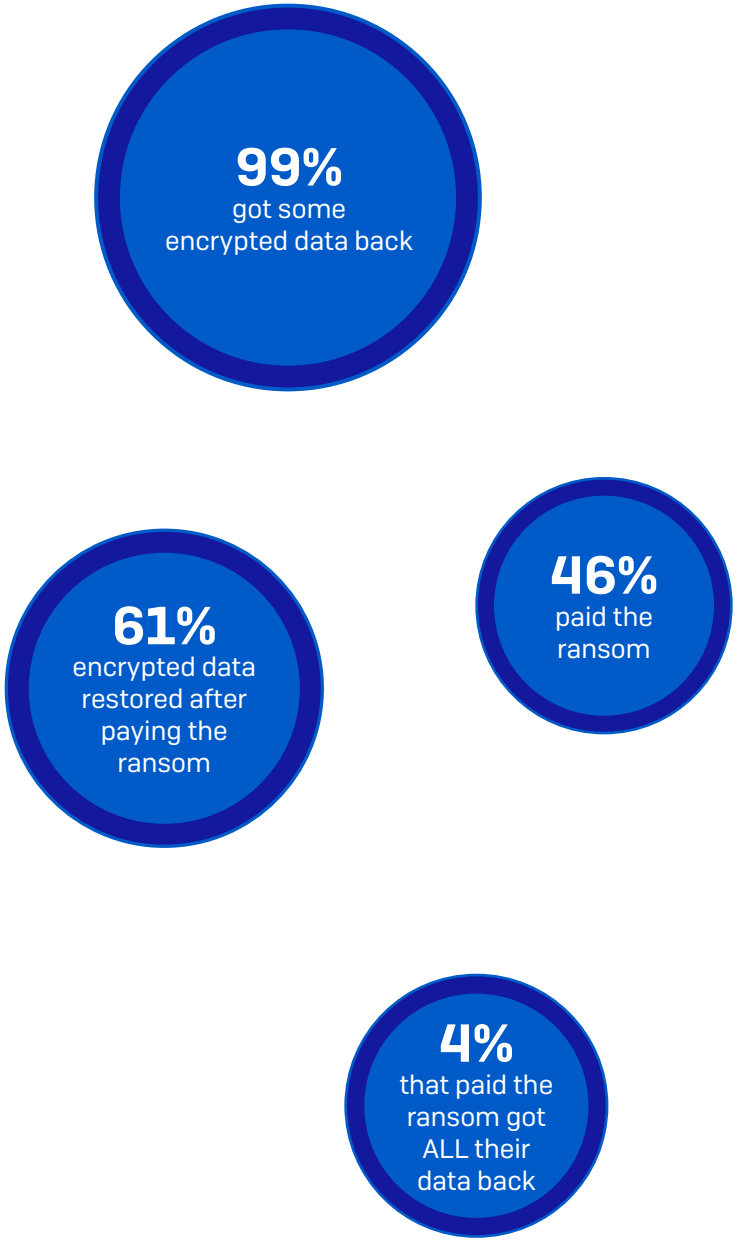
72%
experienced an increase in volume/ complexity/impact of cyber attacks

Organizations are getting better at restoring data after an attack

As ransomware has become more prevalent, organizations have got better at getting at dealing with the aftermath of an attack. Almost all organizations hit by ransomware in the last year (99%) now get some encrypted data back, up slightly from 96% last year.

Backups are the #1 method used to restore data, used by 73% of organizations whose data was encrypted. At the same time, 46% reported that they paid the ransom to restore data. These numbers reflect the fact that many organizations use multiple restoration approaches to maximize the speed and efficacy with which they can get back up and running. Overall, almost half (44%) of the respondents whose organization's data had been encrypted used multiple methods to restore data.

While paying the ransom almost always gets you some data back, the percentage of data restored after paying has dropped. On average, organizations that paid got back only 61% of their data, down from 65% in 2020. Similarly, only 4% of those that paid the ransom got ALL their data back in 2021, down from 8% in 2020.



Ransom payments have increased

965 respondents whose organization paid the ransom shared the exact amount, revealing that average ransom payments have increased considerably over the last year.

Over the last year there has been an almost threefold increase in the proportion of victims paying ransoms of US$1 million 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.

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). While this headline sum is influenced by 15 eight-digit payments, it's clear from the data that ransoms are trending upwards across the board. There is considerable industry variation, with adversaries extracting the highest sums from those they consider most able to pay:

- HIGHEST average ransom payments were US$2.04M in manufacturing and production (n=38) and US$2.03M in energy, oil/gas and utilities (n=91)
- LOWEST average ransom payments were US$197K in healthcare (n=83) and US$214K in local/state government (n=20)

In Italy, where extortion payments are illegal, meaning organizations are not allowed by law to pay the ransom, 43% of those whose data was encrypted admit that their organization paid up (n=76). The research demonstrates that legislative barriers alone are not effective at stopping ransom payments.

3x
increase in proportion that paid ransoms of US$ 1M or more

21%
paid ransoms of less than $10,000

$812,360
average ransom payment (excluding outliers)

MANUFACTURING, UTILITIES
highest average ransom payment ($2M)

HEALTHCARE
lowest average ransom payment ($197K)

Ransomware has a major commercial and operational impact

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. 90% of those hit by ransomware in the last year said the most significant attack impacted their ability to operate. Furthermore, among private sector organizations, 86% said it caused them to lose business/revenue.

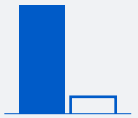
Overall, the average cost to an organization to rectify the impact of the most recent ransomware attack in 2021 was US$1.4M. This welcome drop from US$1.85M in 2020 likely reflects that, as ransomware has become more prevalent, the reputational damage of an attack has lessened. In parallel, insurance providers are better able to guide victims swiftly and effectively through the incident response process, reducing the remediation cost.

It's worth noting that in many cases the where the ransom is paid, the insurance provider, rather than the victim, foots the bill. We cover this in more detail later in the report.

On average, organizations that suffered attacks in the last year took one month to recover from the most significant attack – a long time for most companies. The slowest recovery was reported by higher education and central/federal government where around two in five took over one month to recover. In contrast, the fastest sectors were manufacturing and production (10% took over one month) and financial services (12% took over one month), likely a result of the high levels of recovery planning and preparation.

Furthermore, some organizations continue to put their faith in ineffective defenses. Of the respondents whose organizations weren't hit be ransomware in the last year and don't expect to be hit in the future, 72% are basing this on approaches that don't stop organizations from being attacked: 57% cited backups and 37% cited cyber insurance as reasons why they don't anticipate an attack, with some selecting both options. While these elements help you recover from an attack, they don't prevent it in the first place.

90%
ransomware attack impacted their ability to operate



86%
ransomware attack caused loss of business/revenue

$1.4M
average cost to remediate an attack

ONE MONTH
average time to recover from an attack

72%
putting faith in approaches that don't prevent an attack

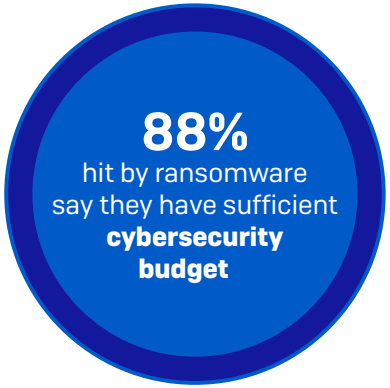
Organizations are unable to use their budgets and resources effectively to stop ransomware

The survey revealed that simply throwing people and money at the problem is not the solution; rather you need to invest in the right technology and have the skills and know-how to use it effectively. Without this, your return on investment is low.

64% of those hit by ransomware in the last year say that they have more cybersecurity budget than they need, while a further 24% say they have the right amount of budget. Similarly, 65% of ransomware victims say they have more cybersecurity headcount than they need and 23% believe they have the right level of staffing. These findings suggest that many organizations are struggling to deploy their resources effectively in face of the accelerating volume and complexity of attacks.

Similarly, the results also indicate that organizations may not realize they do not have the right skills to stop the latest attack techniques: 58% that were hit by ransomware describe their organization as mostly/completely on top of reviewing logs to identify suspicious signals or activities, and 56% say they are mostly/completely on top of the latest attack tools/methodologies.

Conversely, among the organizations that were not hit by ransomware in the previous year and do not anticipate a future attack, the #1 reason behind this confidence is having trained IT security staff or an internal security operations center (SOC) that is able to stop attacks.

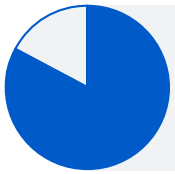


Ransomware drives cyber insurance cover

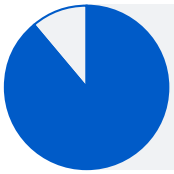
Over four in five mid-sized organizations have cyber insurance against ransomware. However, while 83% of respondents say their organization has cyber insurance that covers them if hit by ransomware, 34% say there are exclusions/exceptions in their policy. Energy, oil/gas, and utilities are most likely to have coverage (89%) closely followed by retail (88%). Cyber insurance adoption increases with organization size, with 88% of 3,001-5,000 employee organizations having cover compared to 73% those with 100-250 employees.

Organizations hit by ransomware in the last year are much more likely to have cyber insurance than those that avoided falling victim to an attack. Among those that were hit, 89% have cyber insurance compared with 70% of those not hit. The cause and effect is not clear here. It may be that direct experience of a ransomware incident has driven many organizations to take insurance to help mitigate the impact of future attacks. Alternatively, adversaries may target their attacks on organizations that they know have insurance cover to increase their chances of a ransom pay out. Another option is that some organizations took cover to balance known weaknesses in their defenses. The reality is likely a combination of all three.

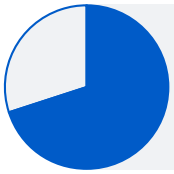
Cyber insurance cover drops to 61% among those that were not hit and don't expect to experience an attack. Given that many in this group are putting faith in approaches that don't stop ransomware, lack of cover leaves them fully exposed to the costs of an incident.



83%
have cyber insurance against ransomware



89%
hit by ransomware have cyber insurance



70%
not hit by ransomware have cyber insurance

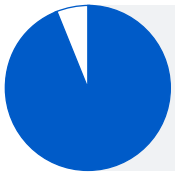
Cyber insurance is driving improvements to cyber defenses

94% of those with cyber insurance said the process for securing coverage had changed over the last year.

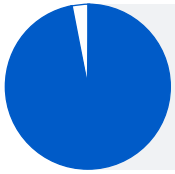
- 54% say the level of cybersecurity they need to qualify is now higher
- 47% say policies are now more complex
- 40% say fewer companies offer cyber insurance
- 37% say the process takes longer
- 34% say it is more expensive

Given that the major cyber insurance price rises began in the second and third quarters of 2021, it's likely that many of the respondents hadn't experienced the impact of this change at the time of the research.

As the cyber insurance market hardens and it becomes more challenging to secure cover, 97% of organizations that have cyber insurance have made changes to their cyber defense to improve their cyber insurance position. 64% have implemented new technologies/services, 56% have increased staff training/education activities, and 52% have changed processes/behaviors.



94%
have found it harder to secure cyber insurance cover over the last year



97%
that have cyber insurance have made changes to their defenses to improve their cyber insurance position

Cyber insurance pays out in almost all ransomware claims

Reassuringly for those with cyber insurance cover, 98% that were hit by ransomware and had cyber insurance that covered ransomware said the policy paid out in the most significant attack – up from 95% in 2019. In a number of countries this rose to a full 100% pay out rate: Switzerland (n=52), Mexico (n=131), Sweden (n=68), Belgium (n=66), Poland (n=75), Turkey (n=51), UAE (n=49), India (n=218) and Singapore (n=91).

Looking at what the cyber insurance cover paid for, the survey reveals an increase in the payment of cleanup costs and a decrease in ransom payments by insurers. 77% of respondents reported that their insurer paid cleanup costs i.e., costs incurred to get the organization up and running again – up from 67% in 2019. Conversely, 40% reported that the insurer paid the ransom, down from 44% in 2019.

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

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

98%
pay-out rate on ransomware claims

△ Clean-up Cost Payout △

67%	77%
2019	2021

▽ Ransom Payout ▽

44%	40%
2019	2021

Conclusion

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

In the face of this near-normalization, organizations have got 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 data restored after paying the ransom has dropped, down to 61%, on average. Despite this, there was a near threefold increase in the percentage victims paying ransoms of $1 million or more.

The survey revealed that simply throwing people and money at the problem is not the solution; rather you need to invest in the right technology and have the skills and know-how to use it effectively. Organizations should look to partner with experts that can help them improve the return on their cybersecurity investments and elevate their defenses.

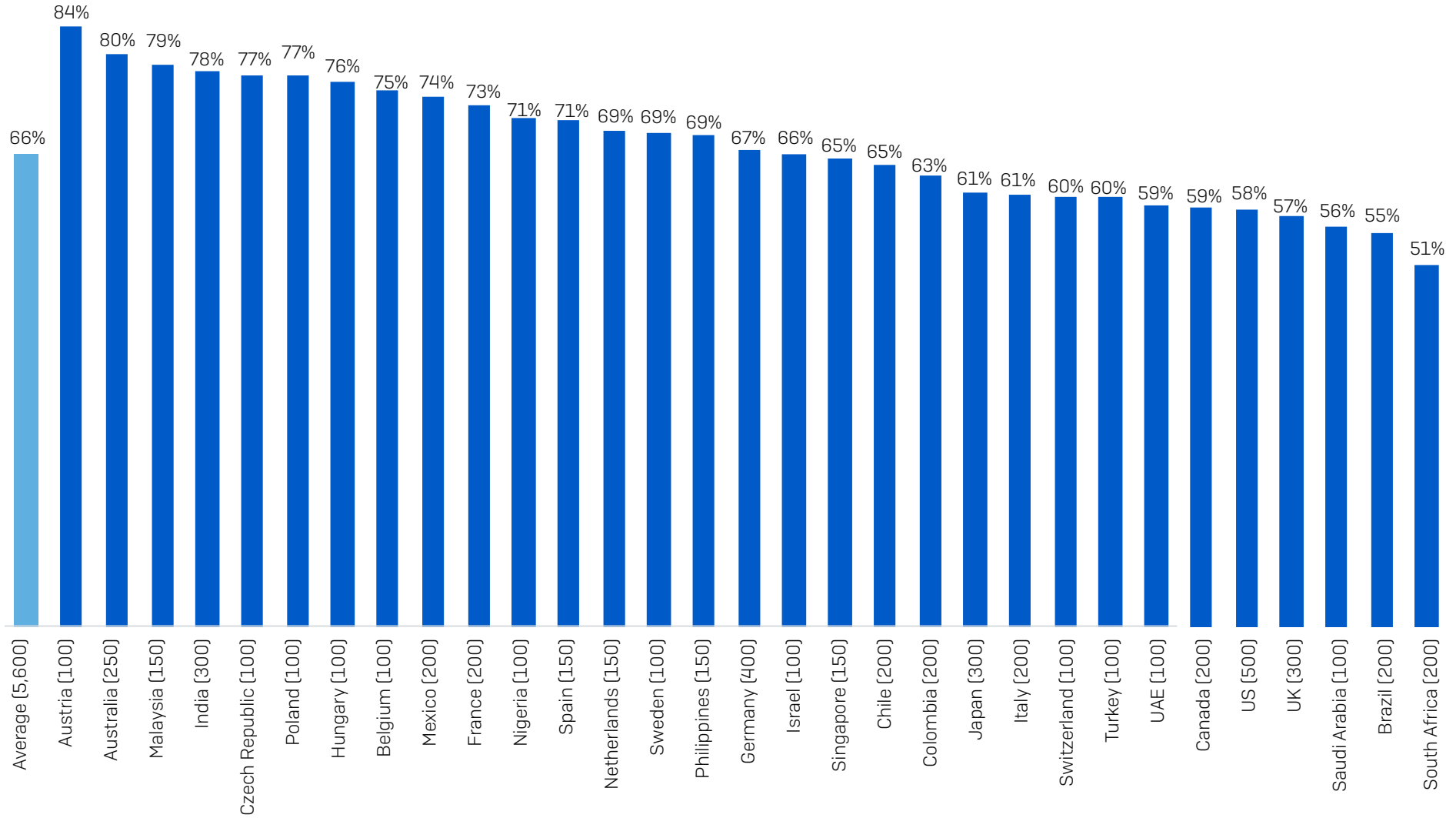
Most organizations are choosing to reduce the financial risk associated with an attack by taking cyber insurance. For them, it is reassuring to know that insurers pay some costs in almost all claims. However, it's getting harder for organizations to secure cover, which has driven almost all to make changes to their cyber defenses to improve their cyber insurance position.

Whether you are looking to secure insurance cover or not, optimizing your cybersecurity is an 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, outsource to a MDR specialist.
- 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.

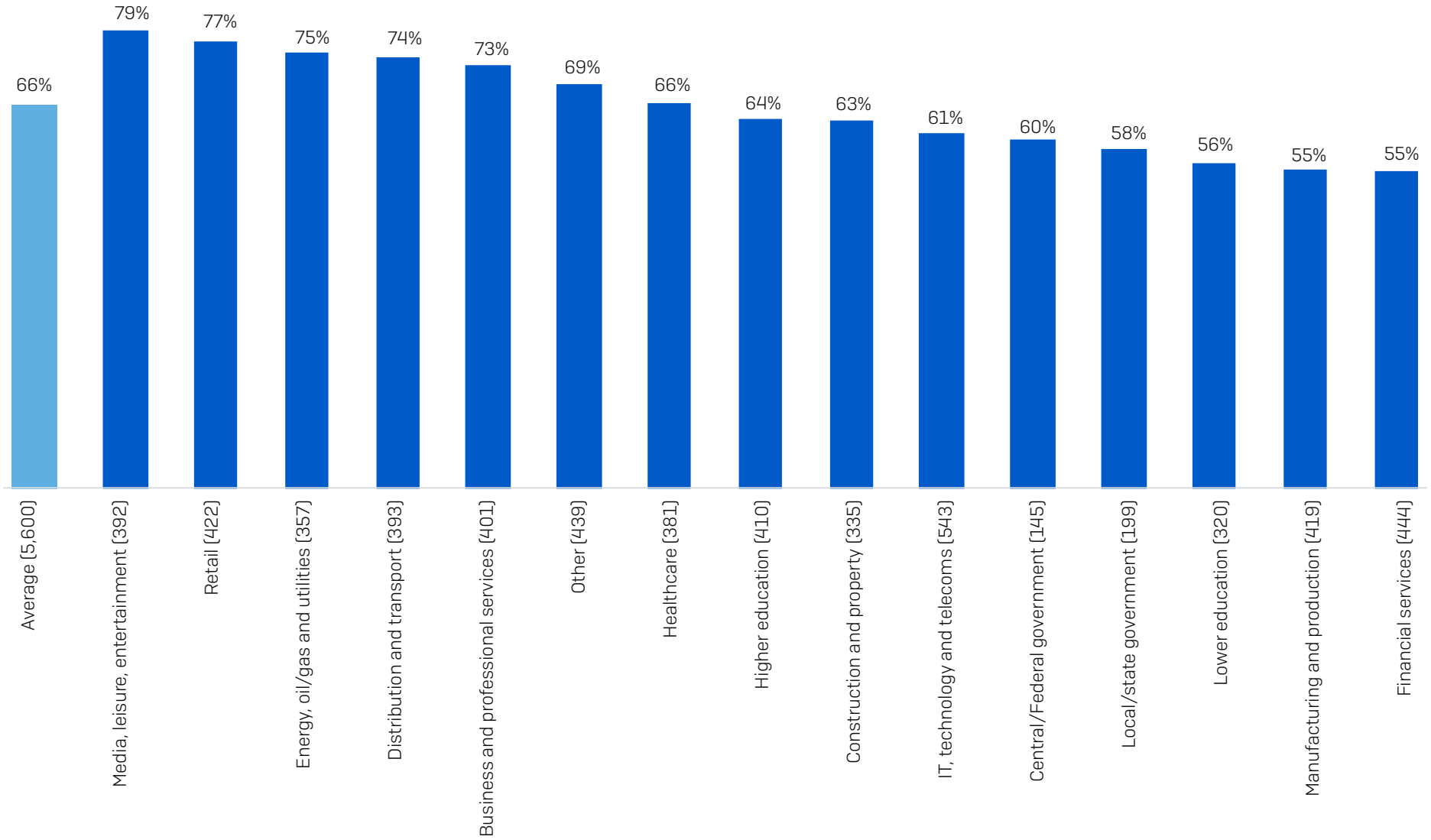
For detailed information on individual ransomware groups, see the Sophos ransomware threat intelligence center.

Percentage of Organizations Hit by Ransomware In the Last Year



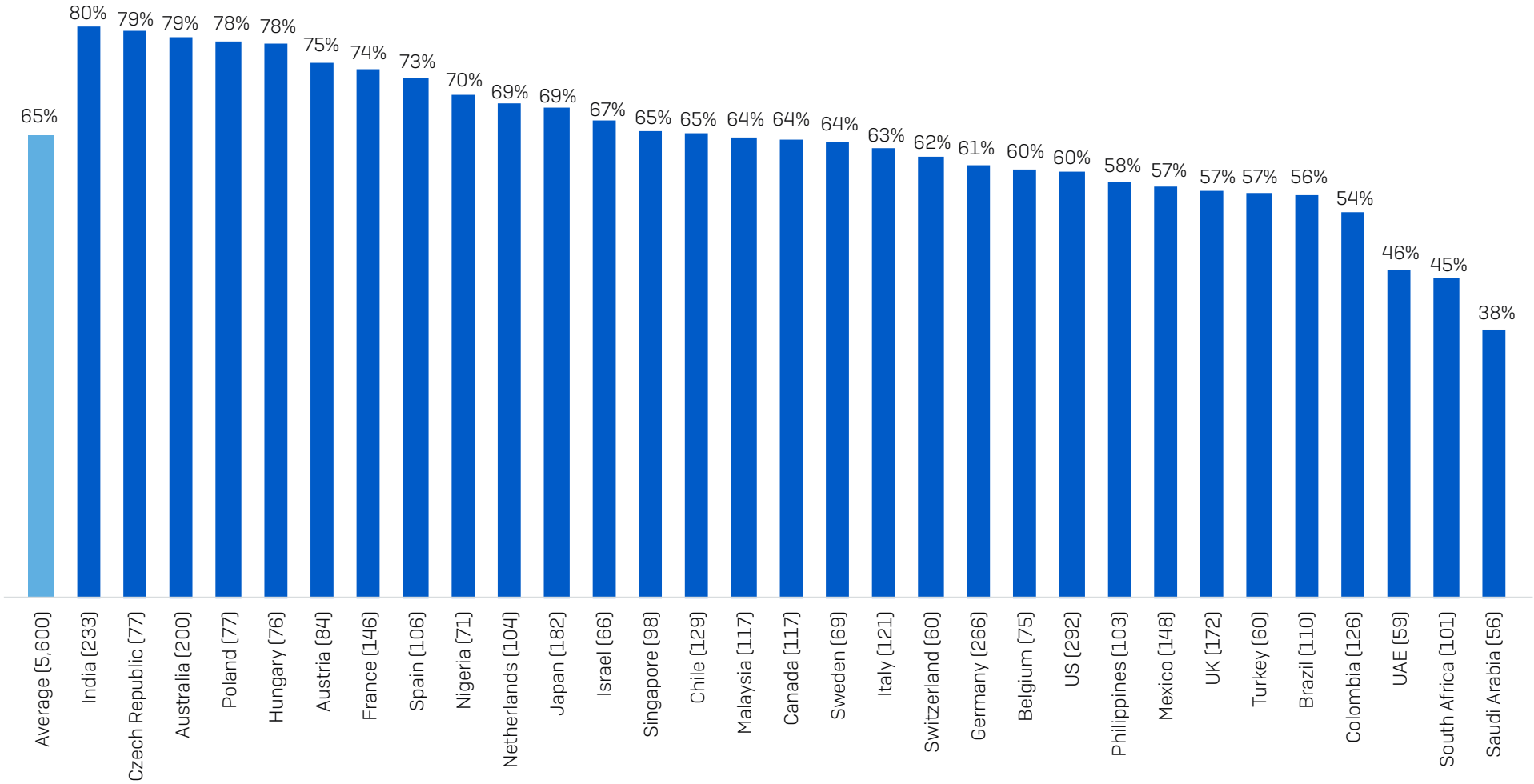
In the last year, has your organization been hit by ransomware? (n=5,600): Yes

Percentage of Organizations Hit by Ransomware In the Last Year



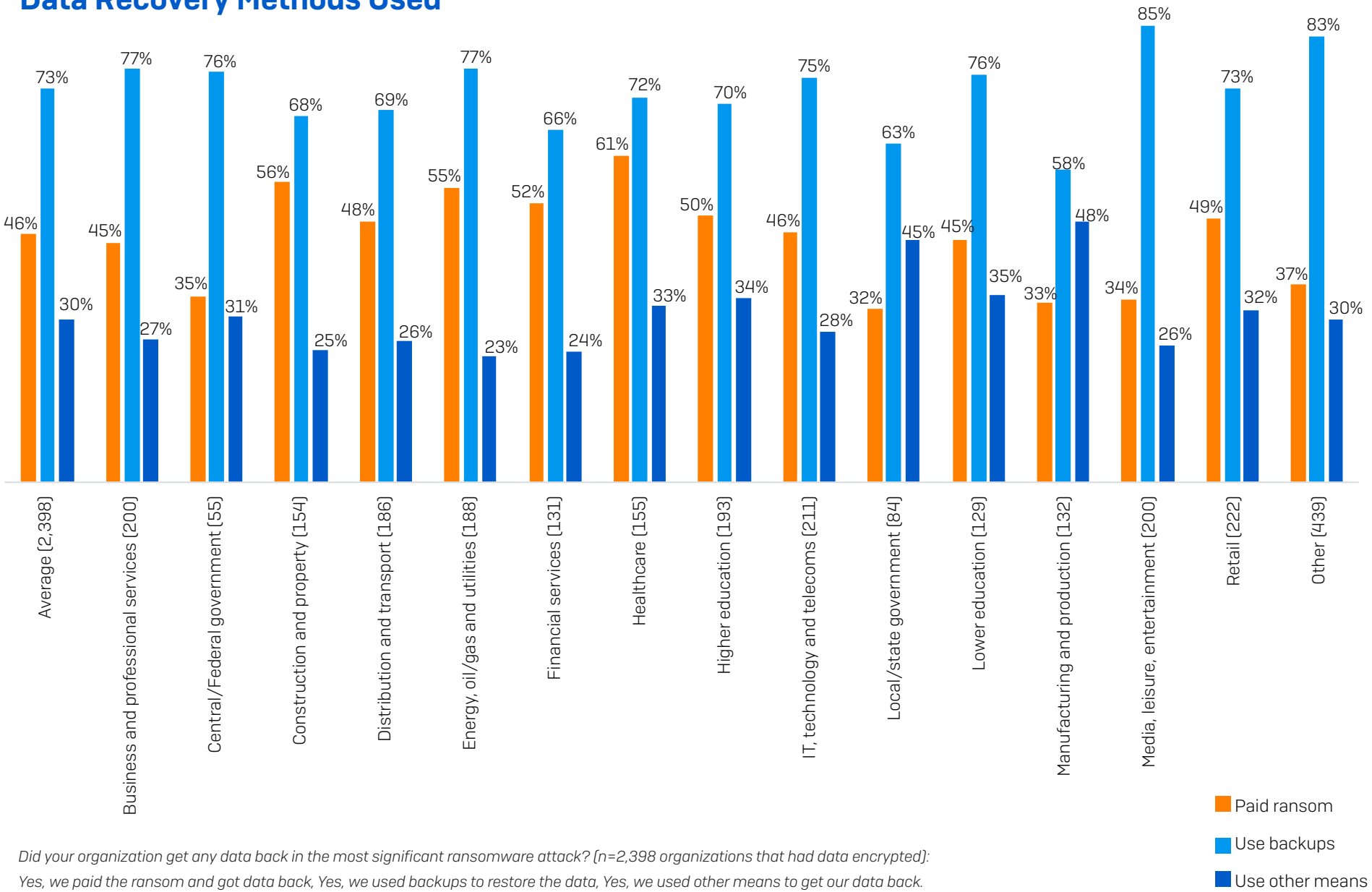
In the last year, has your organization been hit by ransomware? (n=5,600): Yes

Encryption Rate In Ransomware Attacks



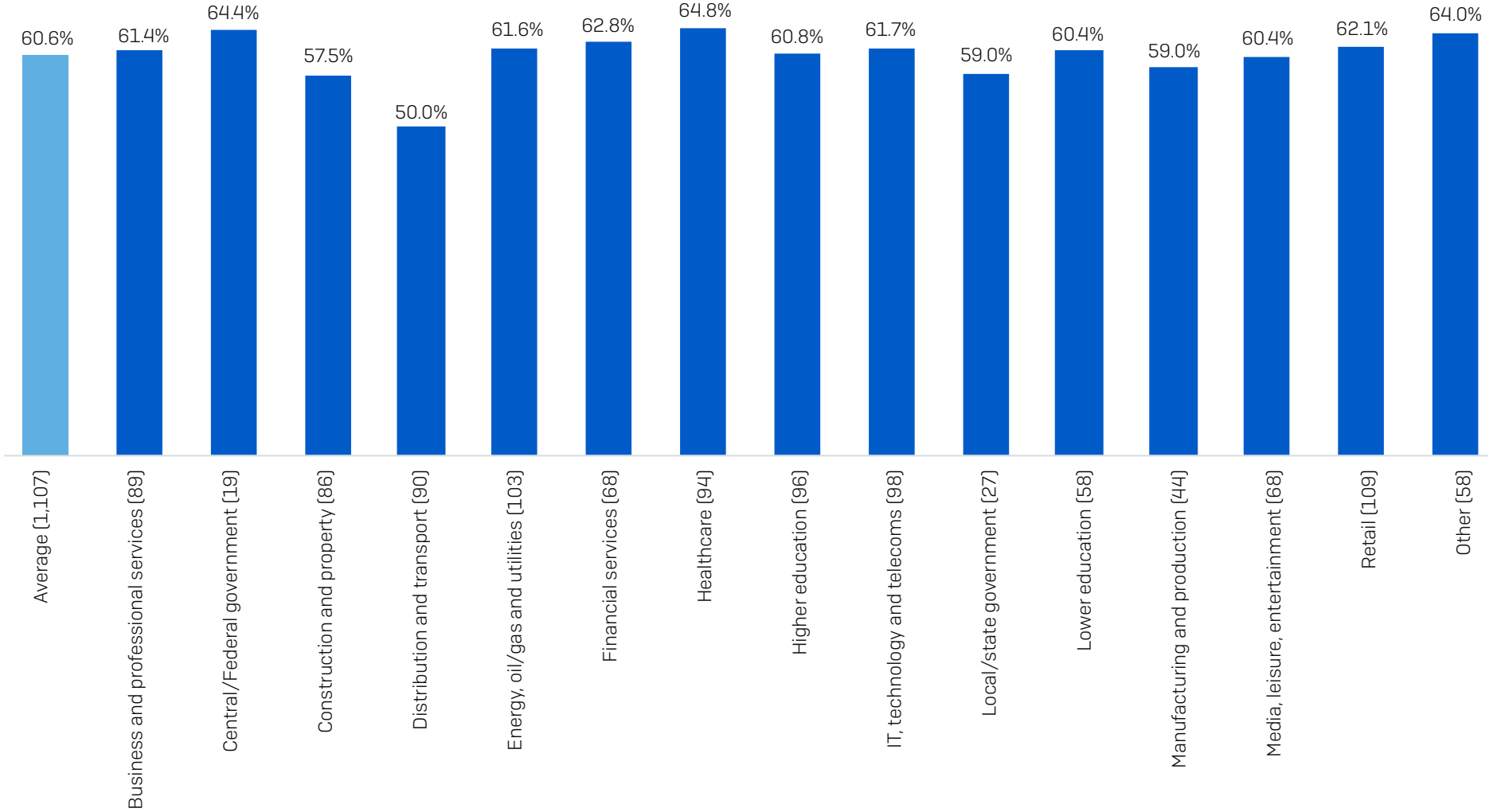
Did the cybercriminals succeed in encrypting your organization's data in the most significant ransomware attack? (n=3,702 organizations hit by ransomware in the last year): Yes

Data Recovery Methods Used



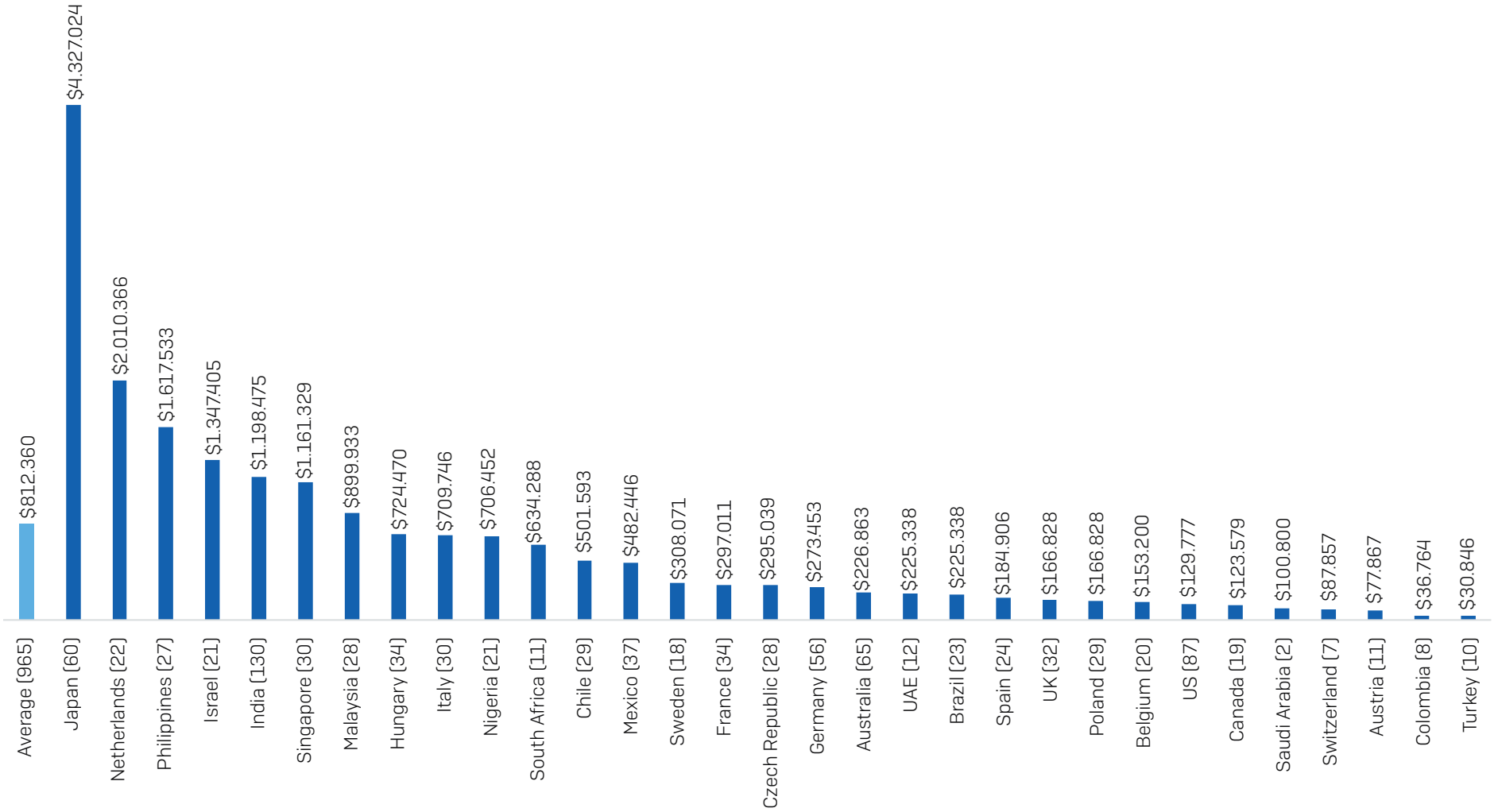
Did your organization get any data back in the most significant ransomware attack? (n=2,398 organizations that had data encrypted): Yes, we paid the ransom and got data back, Yes, we used backups to restore the data, Yes, we used other means to get our data back.

Percentage of Data Restored After Paying Ransom



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

Average Ransom Payments By Country



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 and outliers.
N.B. For countries with low base numbers, findings should be considered indicative.

Average Cost to Organization to Rectify the Attack (Millions of US$)

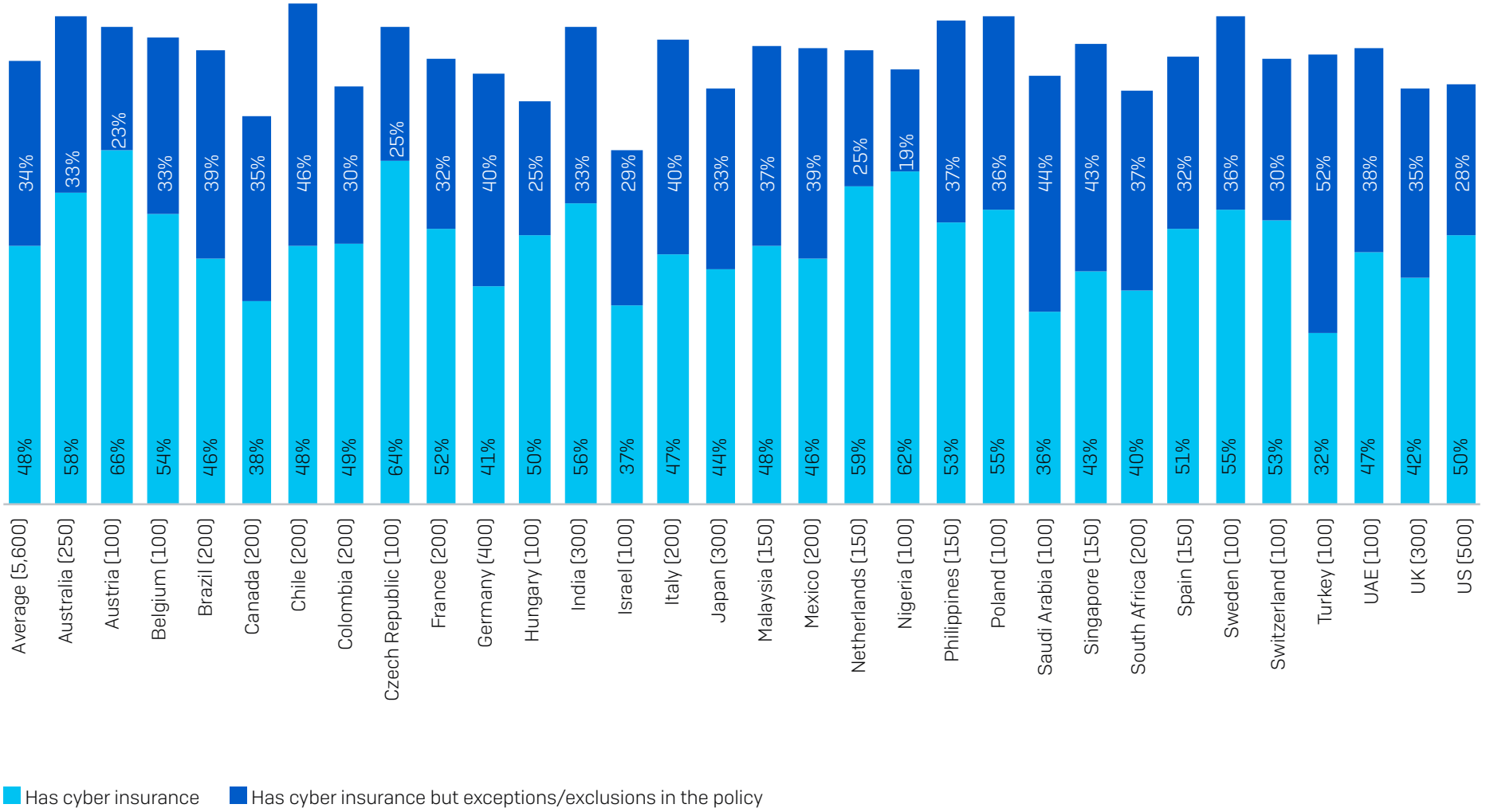
Country	2021	2020	YoY Change
Average (3,702)	$1.40	$1.85	-24%
Australia (200)	$1.01	$1.84	-45%
Austria (84)	$0.81	$7.75	-90%
Belgium (75)	$3.71	$4.75	-22%
Brazil (110)	$0.69	$0.82	-16%
Canada (117)	$0.65	$1.92	-66%
Chile (129)	$1.58	$0.73	116%
Colombia (126)	$0.50	$1.26	-60%
Czech Republic (77)	$2.58	$0.37	589%
France (146)	$2.03	$1.11	83%
Germany (266)	$1.73	$1.17	48%
Hungary (76)	$1.51	n/a	n/a
India (233)	$2.81	$3.38	-17%
Israel (66)	$1.41	$0.57	148%
Italy (121)	$1.65	$0.68	141%
Japan (182)	$0.96	$1.61	-40%
Malaysia (118)	$1.22	$0.77	58%

Country	2021	2020	YoY Change
Mexico (148)	$0.88	$2.03	-57%
Netherlands (104)	$0.98	$2.71	-64%
Nigeria (71)	$3.43	$0.46	644%
Philippines (103)	$1.34	$0.82	63%
Poland (77)	$1.78	n/a	n/a
Saudi Arabia (56)	$0.65	$0.21	212%
Singapore (98)	$1.91	$3.46	-45%
South Africa (101)	$0.71	n/a	n/a
Spain (106)	$0.75	$0.60	25%
Sweden (69)	$0.75	$1.40	-46%
Switzerland (60)	$1.64	$1.43	15%
Turkey (60)	$0.37	$0.58	-36%
UAE (59)	$1.26	$0.52	144%
UK (172)	$1.08	$1.96	-45%
US (292)	$1.08	$2.09	-49%

N.B. Base numbers are for 2021 data only. *N.B. Values are in Millions of US$*

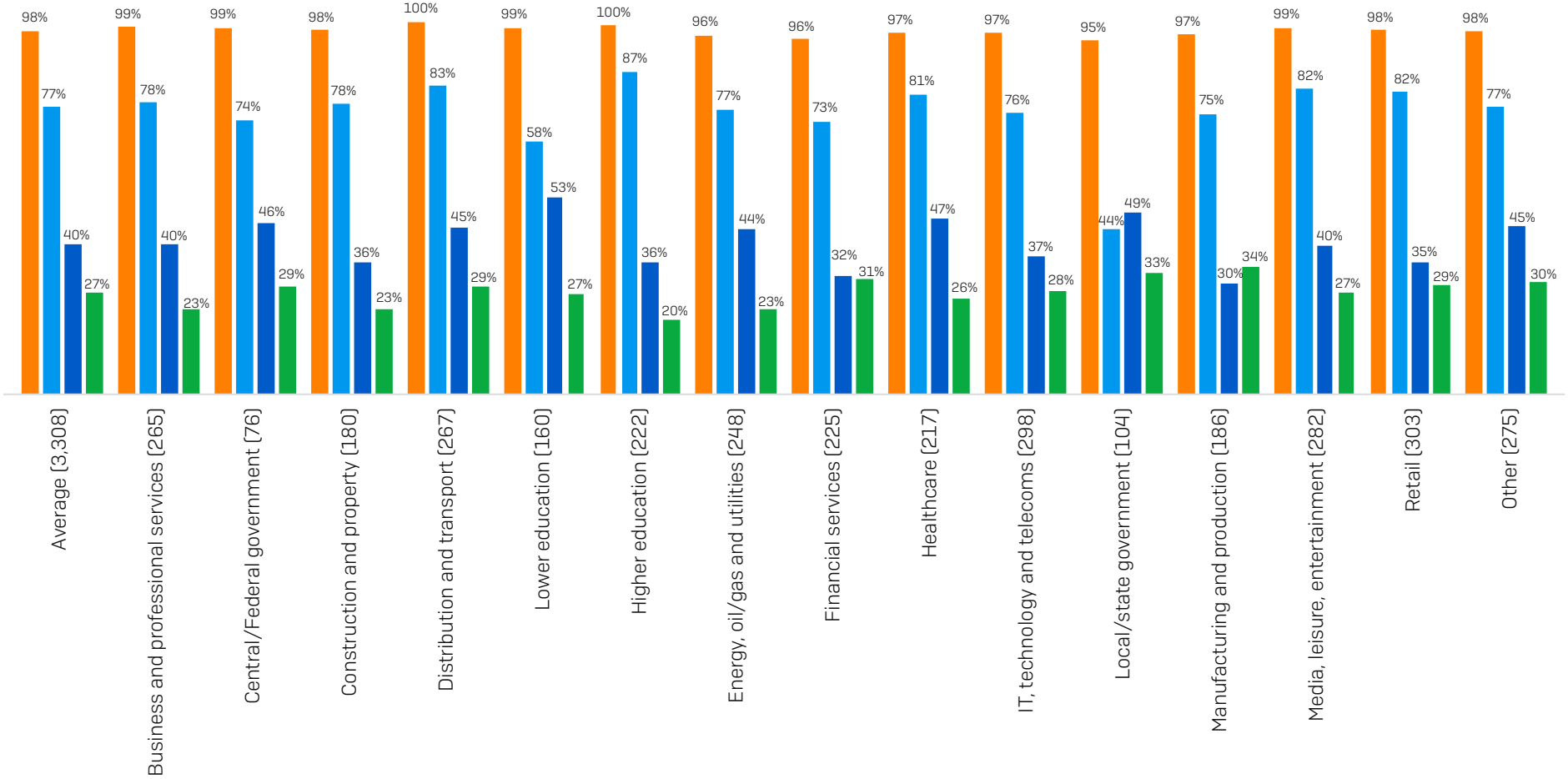
What was the approximate cost to your organization to rectify the impacts of the most recent ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc.)? (n=3,702 organizations that were hit by ransomware in the previous year)

Percentage of Organizations With Cyber Insurance Cover



Does your organization have cyber insurance that covers it if it is hit by ransomware? (n=5,600). Yes; Yes, but there are exceptions/exclusions in our policy

Cyber Insurance Payout Rate



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 costs
- 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.

2022-04-20 (WP-PS)

SOPHOS