SOPHOS
Cybersecurity delivered.

Cyber Insurance 2022: Reality from the InfoSec Frontline

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

A Sophos Whitepaper. May 2022

Introduction

Sophos' annual study of the real-world experience of IT professionals at the frontline has revealed how their experience of obtaining cyber insurance coverage has changed over the last year. It also shows the impact cyber insurance has had on their cyber defenses.

With ransomware a major driver of both cyber insurance purchase and claims, the study also shines light onto how often cyber insurance policies pay out in the event of an attack and the types of costs that are addressed, including how often insurers pay the ransom.

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 and a wide range of industries.

To ensure realistic representation of life at the frontline, respondents were from Europe, the Americas, Asia-Pacific and Central Asia, the Middle East, and Africa, and from a broad spread of organization sizes:

- 25% from organizations with 100-500 employees
- 25% from organizations with 501-1,000 employees
- 31% from organizations with 1,001-3,000 employees
- 19% from organizations with 3,001-5,000 employees

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

For comparative purposes, our 2021 study surveyed 5,400 respondents across 30 countries and our 2020 study surveyed 5,000 respondents across 26 countries.

5,600
respondents

31
countries

100-5,000
employee organizations

Jan/Feb 2022
research conducted

Cyber insurance adoption

Overall, 92% of all respondents said that their organization currently has some level of cyber insurance coverage in place. 83% of respondents have cyber insurance that covers ransomware, although 41% of them (34% of all respondents) say there are exceptions and exclusions in their ransomware coverage.

Cyber insurance adoption has increased over the last two years: in our 2020 survey (which reflected organizations' experiences in 2019) 84% of the 5,000 respondents said their organization had cyber insurance and only 64% had cyber insurance that covered ransomware[1].

On a per-country basis, European countries top the cyber insurance coverage chart this time round with respondents in the Czech Republic (99%), Sweden and Belgium (both 98%) most likely to report that their organization has coverage. Hungary reported the lowest level of cyber insurance coverage (82%) while Israel has the lowest rate of coverage against ransomware (66%).

At a sector level, the energy, oil/gas and utilities sector has both the joint highest level of cyber insurance coverage (96%), together with retail, and the highest level of coverage against ransomware (89%). This is unsurprising given that this sector is a major target for attacks (for example, the Colonial Pipeline ransomware incident of 2021), and also has high levels of legacy infrastructure that is often hard to keep up to date, increasing exposure to attack.

At the other end of the scale, manufacturing and production has both the lowest level of cyber insurance coverage (86%) and the lowest level of coverage against ransomware (75%).

This high overall rate of cyber insurance coverage is understandable given the growing cyber threat challenge facing IT teams: over the last year 57% of respondents experienced an increase in the volume of cyberattacks on their organization, 59% saw the complexity of attacks increase, and 53% said the impact of attacks had increased.

Ransomware is the number one driver of cyber insurance claims[2] and over the last year there was a 78% increase in the percentage of organizations that experienced an attack: up from 37% in 2020 to 66% in 2021. As adversaries have become more capable at executing attacks at scale it follows that demand for cyber insurance has also increased.

△ Cyber Insurance Coverage △

84%
2019

92%
2021

△ Cyber Insurance Coverage Against Ransomware △

64%
2019

83%
2021

[1] Note: The 2022 survey included an additional answer option to identify those with exceptions/exclusions in their ransomware coverage

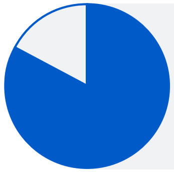
[2] Source: NetDiligence Cyber Claims Study 2021 Report

Ransomware experience drives ransomware cyber insurance coverage

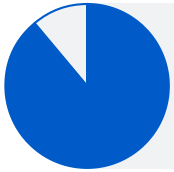
Organizations hit by ransomware in the last year are much more likely to have cyber insurance that covers them against ransomware than those that avoided falling victim to an attack. Among those that were hit, 89% have cyber insurance that covers ransomware compared with 70% of those not hit.

The cause-and-effect is not clear here. It may be that direct experience of a ransomware incident has driven many organizations to take out insurance to help mitigate the impact of future attacks. Alternatively, adversaries may target their attacks on organizations that they know have insurance coverage to increase their chances of a ransom pay out. Another option is that some organizations took out coverage to balance known weaknesses in their defenses. The reality is likely a combination of all three.

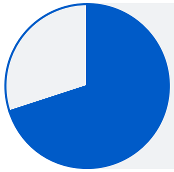
It's worth noting that a prior claim can make securing new or renewed coverage more difficult without a significant investment in a changed approach to cybersecurity as insurers look to reduce the risk of a major payout.



83%
of all respondents have cyber insurance against ransomware



89%
hit by ransomware have cyber insurance against ransomware



70%
not hit by ransomware have cyber insurance against ransomware

Rising ransoms

As previously noted, many organizations have exceptions or exclusions to their ransomware coverage. For example, should an organization choose not to include having the provider pay the ransom component of a ransomware attack, that will often bring down the overall price of coverage. When evaluating what to include in a policy, it's helpful to understand the reality of ransom payments today.

965 respondents whose organization paid the ransom shared the exact amount, revealing that average ransom payments have increased considerably over the last year. However, there is considerable variation in ransom payment by country and/or sector.

Overall, 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.

Globally, 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 sector 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 – note: this is a low base number)

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)

Major changes to organizations' experience of getting cyber insurance over the last 12 months

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

Collectively, these findings illustrate the profound impact the recent hardening of the cyber insurance market has had on organizations looking to secure coverage. What's more, in light of the rising cyber threats and ransom payments revealed by the study, we anticipate the challenges will continue throughout 2022.

Fewer insurers are writing policies

40% of respondents said there are fewer companies now offering cyber insurance. This reduction in supply is in response to the heavy losses many providers have experienced in recent years. Illustrating this point, in November 2021 it was reported that Lloyds of London, which underwrites around one-fifth of the global cyber insurance market, had discouraged its members from taking on cyber business in 2022 due to mounting losses[3].

This reduction in cyber insurance provision was particularly severe in Sweden, Nigeria, Chile, the Czech Republic, Australia and the Philippines where more than half of the respondents indicated the number of providers had dropped. At the other end of the scale, reports of reduced availability were lowest in Brazil (24%), Mexico (29%) and France (29%), however, this still represent a notable drop of insurance outlets on the prior 12 months.

Higher cyber controls are needed to qualify for coverage

With reduced supply, cyber insurance has become a sellers' market, with providers in a much stronger position to stipulate policy conditions and pre-requisites for coverage. Consequently, over half of the respondents (54%) said the level of cybersecurity needed to qualify for coverage has increased over the last year.

Organizations applying for new and renewal policies in 2022 are often faced with a new normal: If you want to qualify for cyber insurance, you will need stronger cyber defenses. Common cyber controls required/desired to secure coverage, according to leading brokers Marsh McLennan Agency and Hub, include multi-factor authentication (MFA), endpoint detection and response (EDR), email security, web controls and more.

Coverage is more expensive...

Another consequence of both the reduced market capacity and heavy insurer losses has been an increase in the cost of cyber insurance. One third of respondents said that the price of coverage had gone up over the last year. However, given that the major cyber insurance price rises began in the second and third quarters of 2021[4], it's likely that many of the respondents hadn't experienced the impact of this change at the time of the research. Organizations looking to take out a policy in 2022 should adjust their budgets accordingly.

... and more difficult to secure

Not only is coverage more expensive, it is also often harder to secure. Almost half of the respondents (47%) reported that policies are now more complex. Possible examples include an increase in sub-limits, i.e., maximum payouts for different types of costs, or more detailed and/or extensive exclusions.

In addition, over one third (37%) report that it now takes longer to secure the policy. This is likely due to a combination of the more stringent cyber controls that are in place and the reduced supply.

Organizations looking to secure a policy this year would do well to act early: by doing so you give your organization the best chance of getting coverage while there is still available capacity and also having the time needed to negotiate your policy fully.

[3] *https://www.reuters.com/markets/europe/insurers-run-ransomware-cover-losses-mount-2021-11-19/*

[4] *James Tuplin, Marc Schein, Optimizing your Cyber Insurance Position*

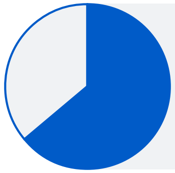
Cyber insurance is driving improvements to cyber defenses

As the cyber insurance market hardens and it becomes more challenging to secure coverage, almost all organizations (97%) with cyber insurance have made changes to their cyber defenses to improve their insurance position.

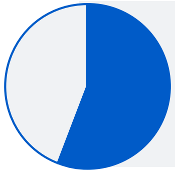
- 64% have implemented new technologies/services
- 56% have increased staff training/education activities
- 52% have changed processes/behaviors

Interestingly, there was very little variance in responses between those that had experienced an increase in the volume/complexity/impact of cyberattacks over the last year and those that hadn't. This suggests that these changes are being driven solely by the demands of the cyber insurance providers and not in response to direct experience of attacks.

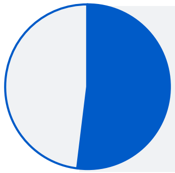
There was also little change in experience by geography, sector or organization size, indicating that the impact of cyber insurance is universal.



64%
have implemented new technologies/services



56%
have increased staff training/education activities



52%
have changed processes/behaviors

Insurance payouts

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 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. Higher education (universities, colleges and equivalent institutions) reported the highest level of cleanup cost coverage (87%)

Conversely, there was a drop in ransom payout rates by insurers with 40% reporting that the insurer footed the ransom bill, 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%), local/state 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 that reported being able to recover fastest from an incident, emphasizing the importance of disaster recovery planning and preparation.

In all cases, 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 or enabled the attack.

98%
pay-out rate on ransomware claims

△ Clean-up Cost Payout △

67% 2019	**77%** 2021

▽ Ransom Payout ▽

44% 2019	**40%** 2021

Conclusion

Observers of the cyber insurance market likely will agree that the changes over the past 12 months have been astonishing. While most organizations have some form of cyber insurance, the vast majority of survey respondents have experienced a change in their experience of securing coverage over the last year, including higher premiums and more stringent cyber controls.

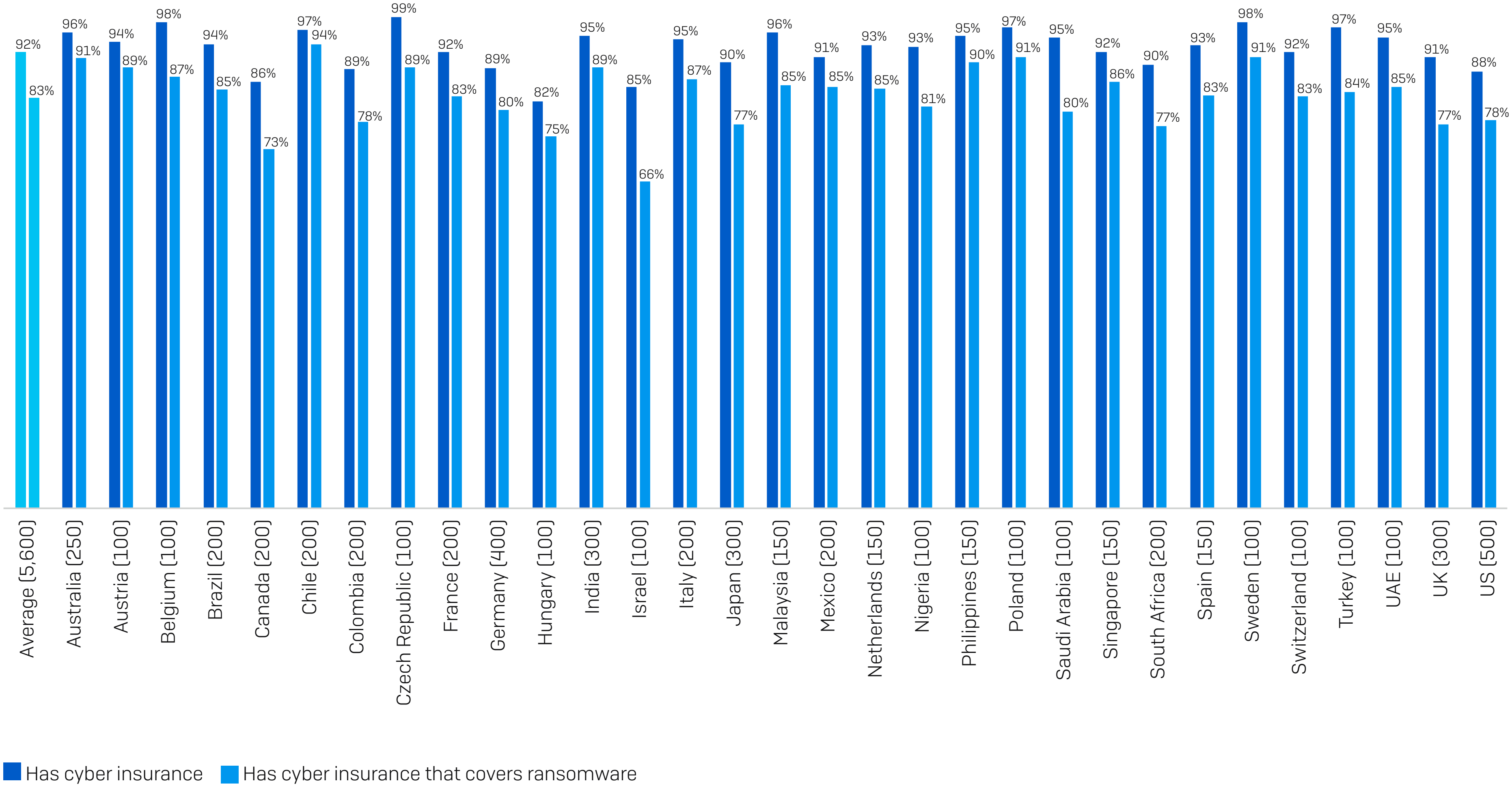
Qualifying for cyber insurance today requires a concerted effort to do all you can to reduce your risk profile. Those who get the best terms, rates and limits will be those who pose the least risk to the underwriters. If you want to obtain cyber insurance in 2022 you should have in place strong technological defenses combined with educated and trained users, plus up-to-date procedures.

With some providers leaving the market, getting your organization's cybersecurity defenses in place and submitting your application early could help you obtain a policy before the supply runs out. If you have questions about what your insurance provider requires, bringing them into the conversation sooner rather than later could help you direct your cybersecurity investments to meet the criteria they are setting to qualify for coverage.

The good news is that cyber insurance firms have diligently been holding to their side of the agreement, with a 98% payout rate on cyber insurance claims reported by survey respondents.

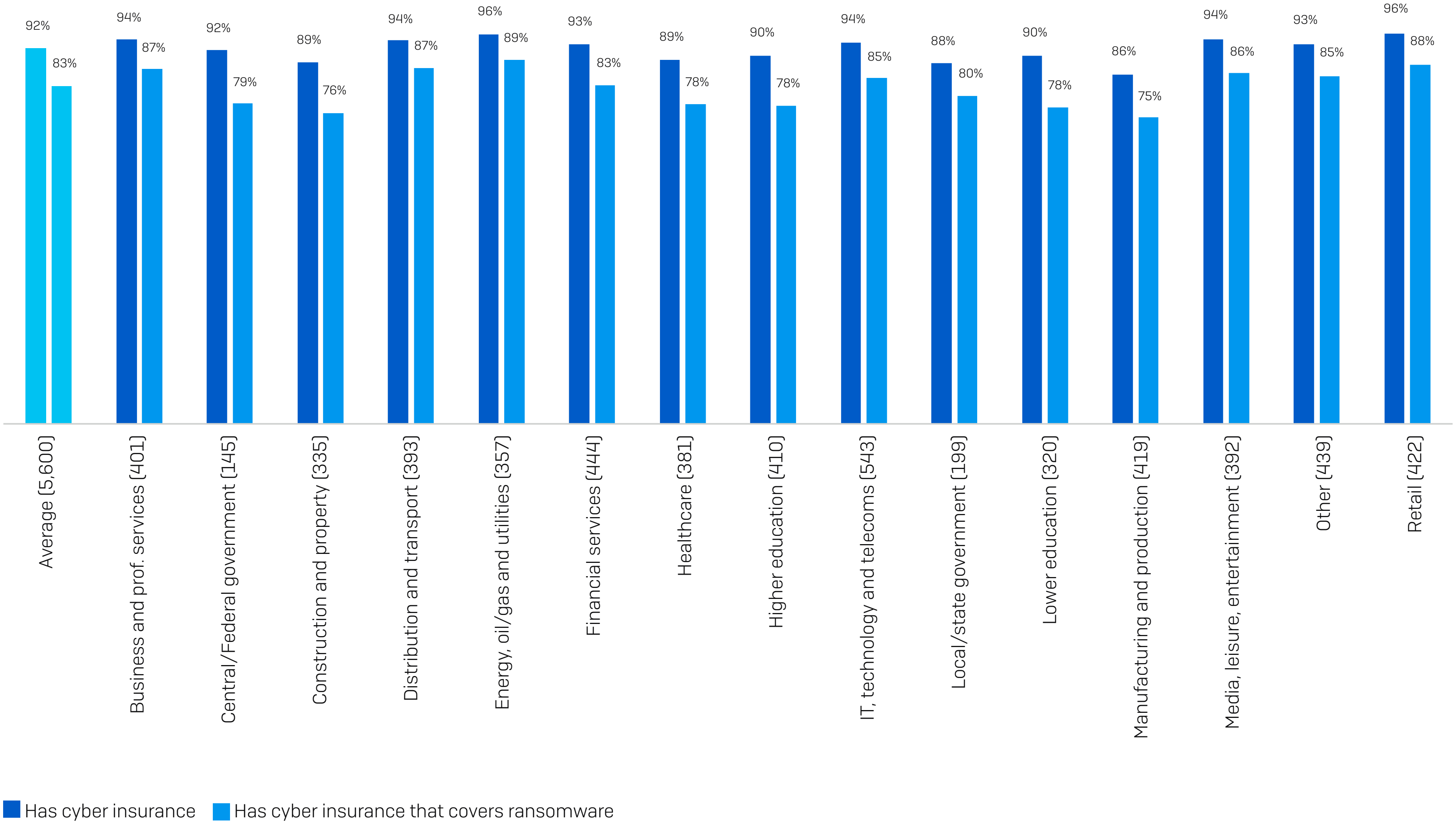
Sophos can help you meet many of the cyber control requirements that are required by insurers as conditions of coverage. To discuss your cyber risk profile and how you can position yourself to better qualify for cyber insurance, speak with your Sophos representative.

Cyber Insurance Adoption by Country



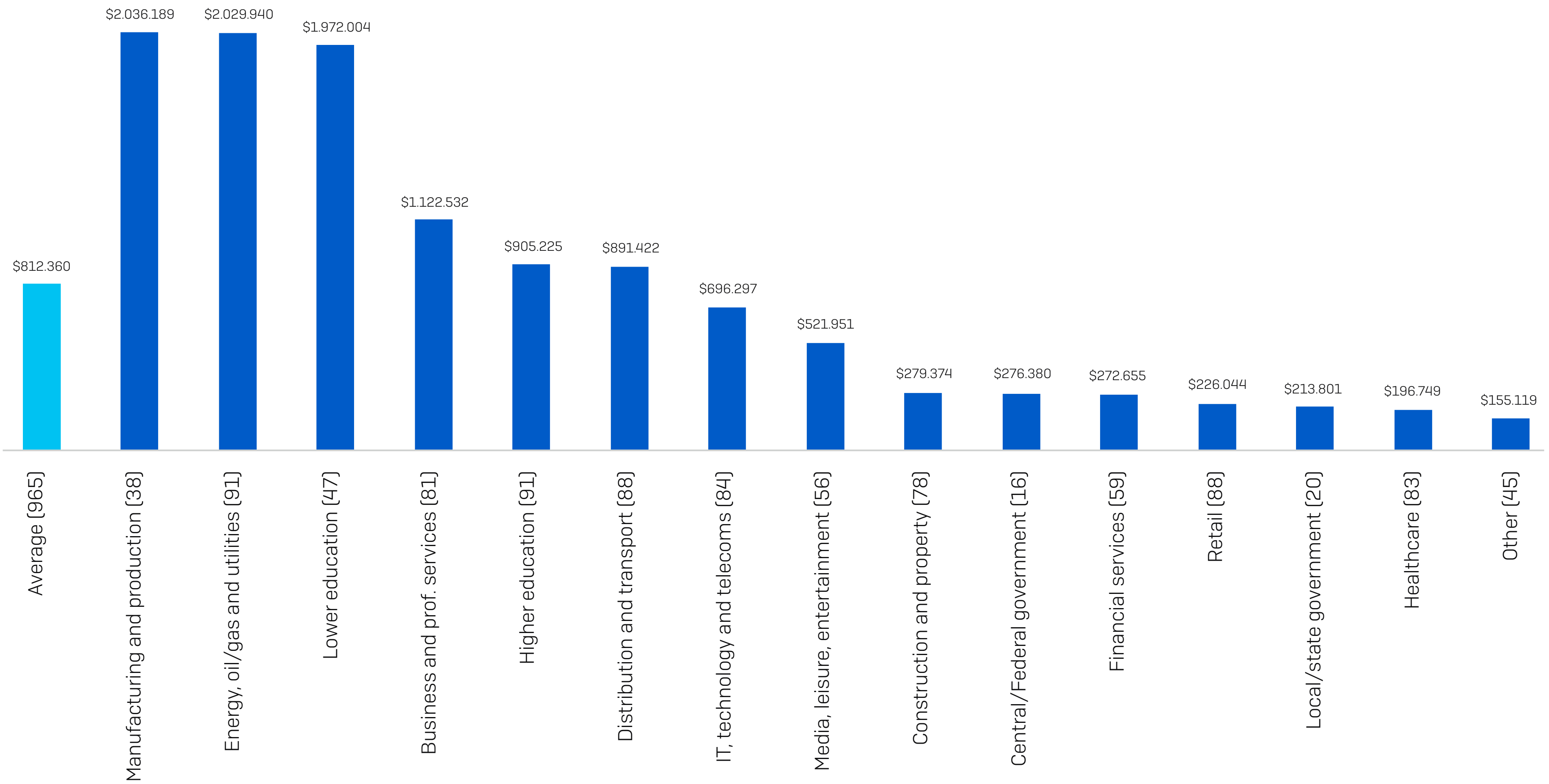
Does your organization have cyber insurance that covers it if it is hit by ransomware? (base numbers in chart). Yes; Yes, but there are exceptions/exclusions in our policy; No, our cyber insurance does not cover ransomware; I don't know if our cyber insurance covers ransomware.

Cyber Insurance Adoption by Sector



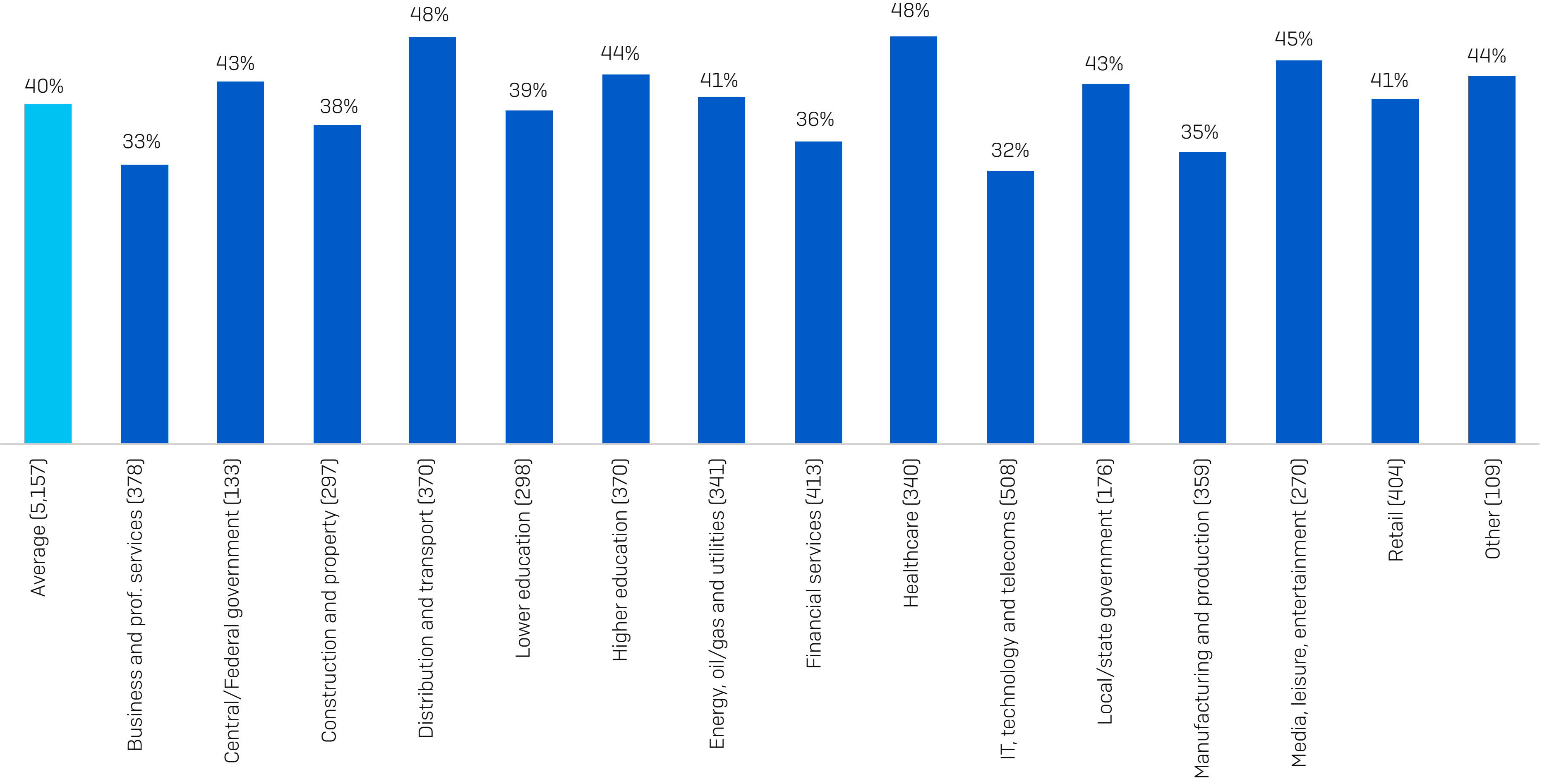
Does your organization have cyber insurance that covers it if it is hit by ransomware? (base numbers in chart). Yes; Yes, but there are exceptions/exclusions in our policy; No, our cyber insurance does not cover ransomware; I don't know if our cyber insurance covers ransomware.

Average Ransom Payments By Sector



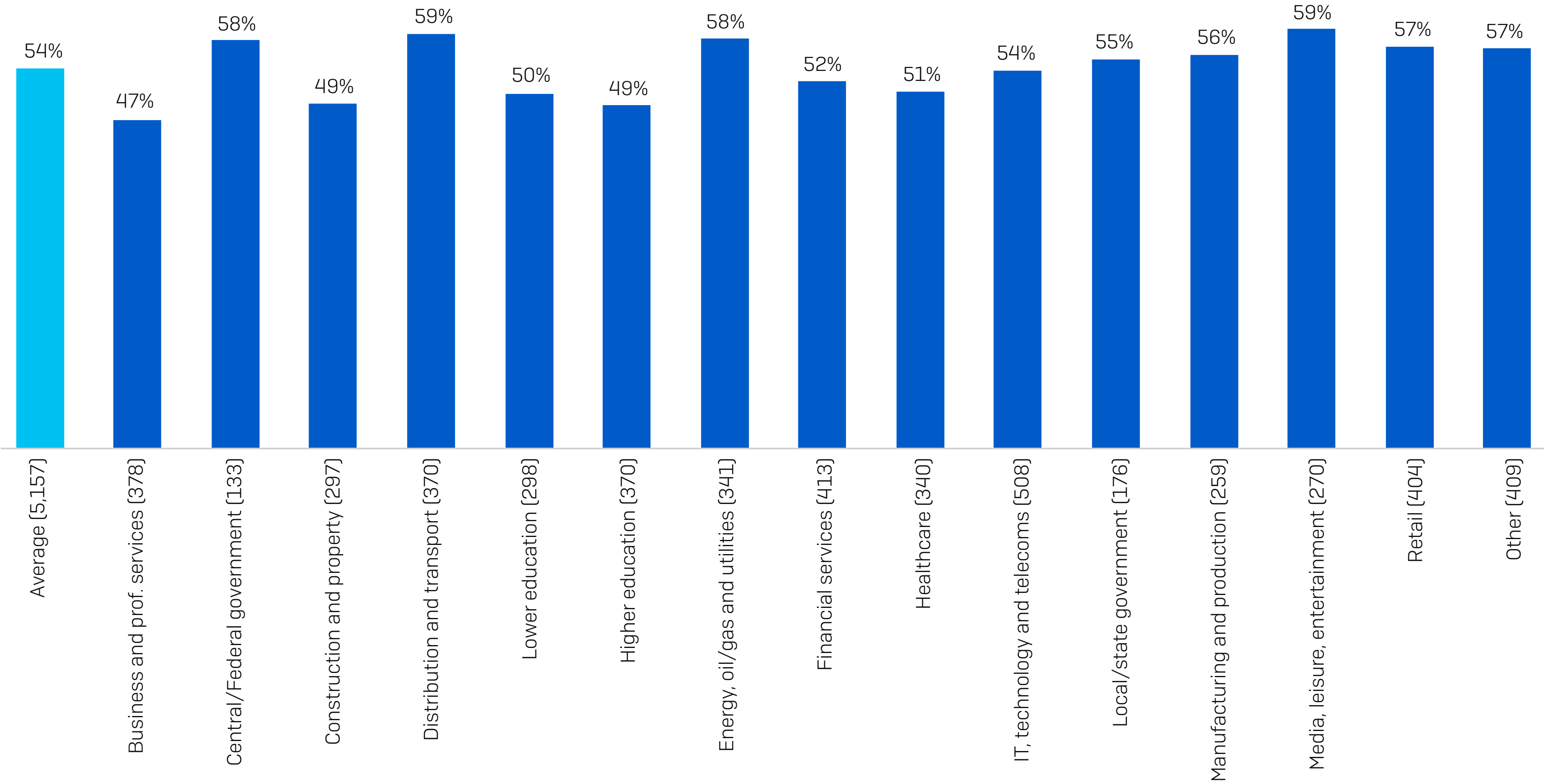
How much was the ransom payment your organization paid in the most significant ransomware attack? US$. Organizations that paid the ransom in the most significant ransomware attack. Base number in chart. Excluding "Don't know" responses. N.B. For sectors with low base numbers, findings should be considered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

Frontline Experience: Fewer Companies Are Now Offering Cyber Insurance



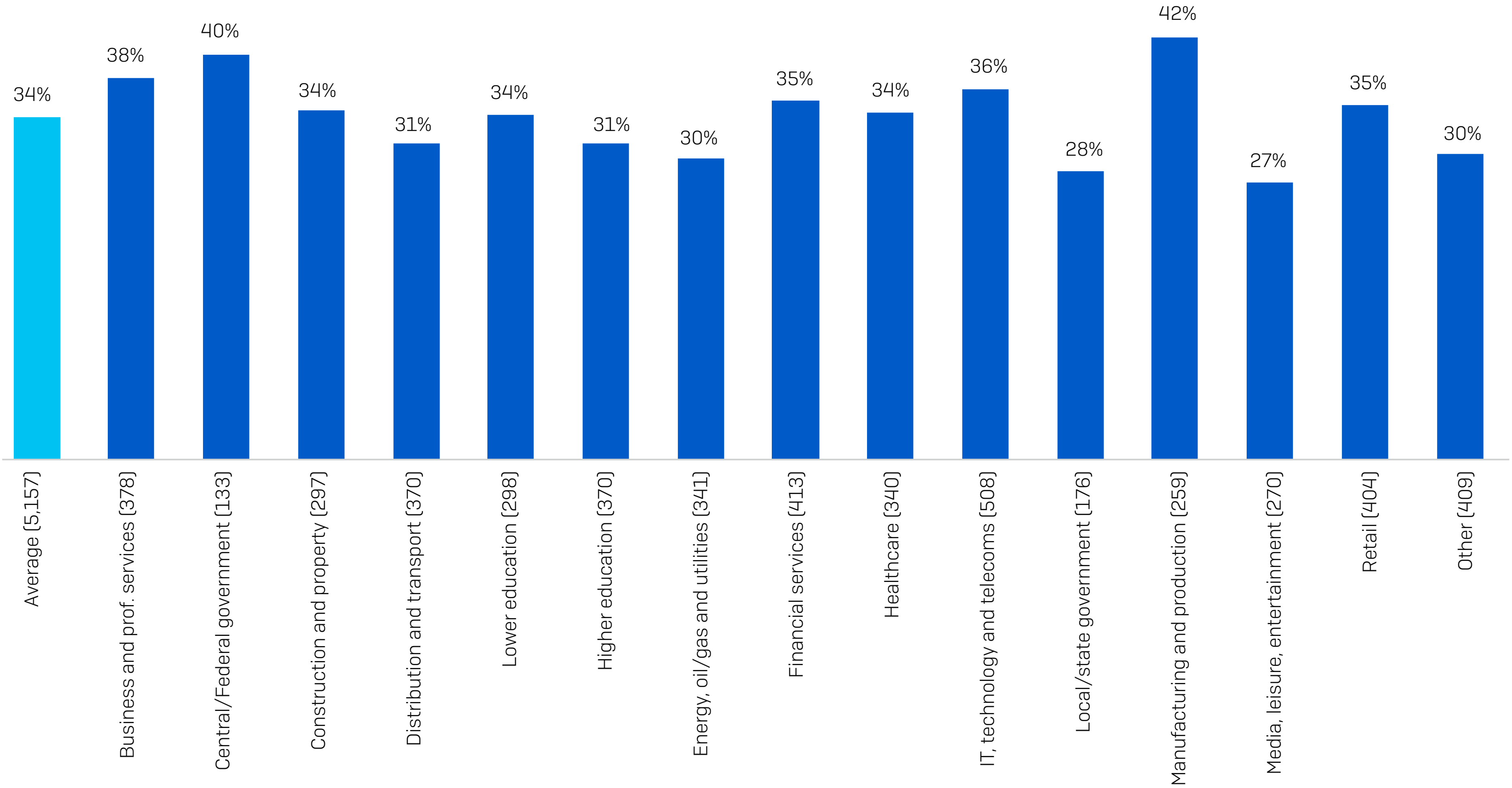
How has your organization's experience of getting cyber insurance changed over the last 12 months? Fewer companies are now offering cyber insurance (n=5,157 respondents whose organization has cyber insurance)

Frontline Experience: Higher Level of Cybersecurity Needed to Qualify for Insurance



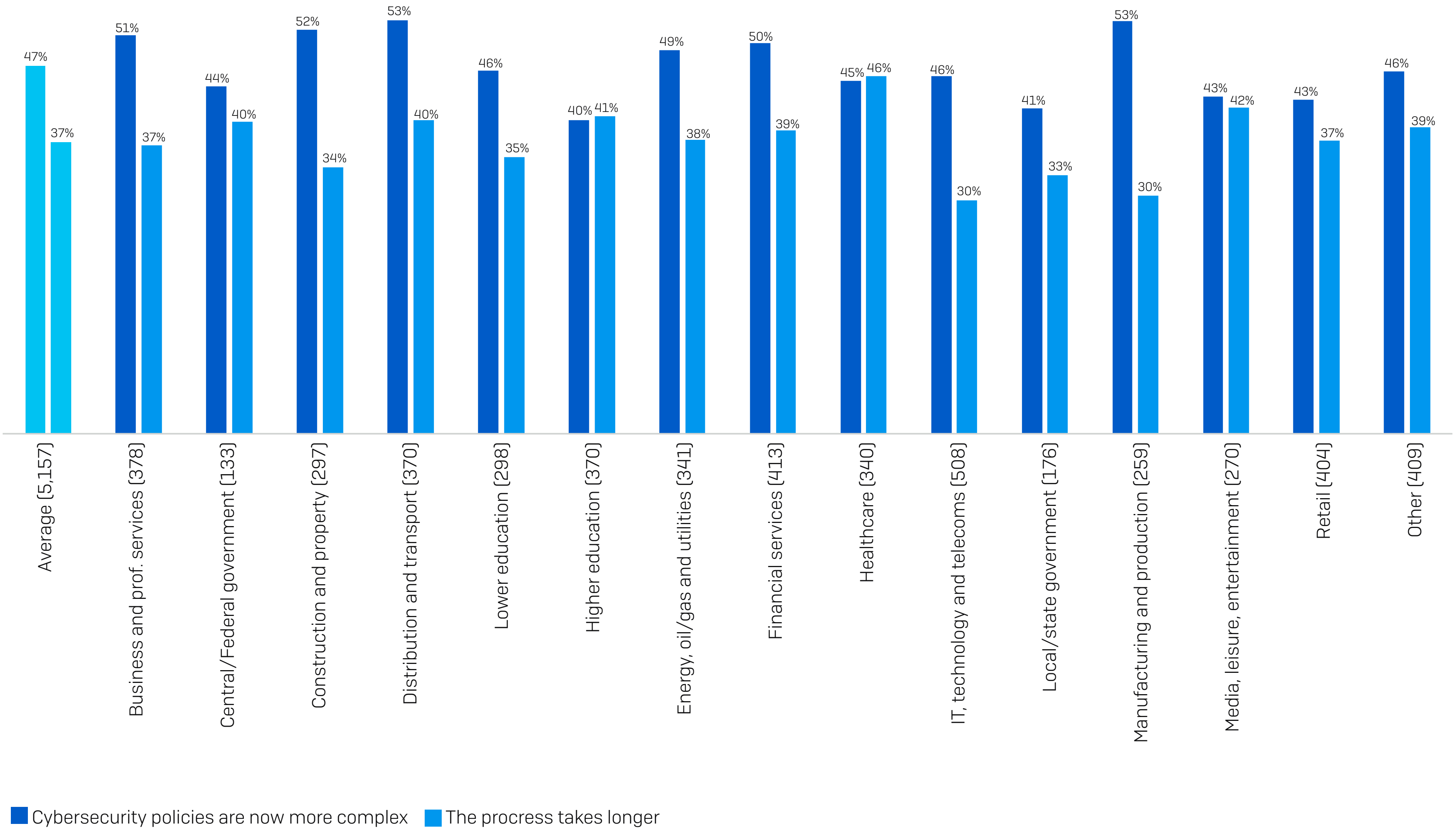
How has your organization's experience of getting cyber insurance changed over the last 12 months? The level of cybersecurity we need to qualify for insurance is higher (n=5,157 respondents whose organization has cyber insurance)

Frontline Experience: Cyber Insurance Is More Expensive



How has your organization's experience of getting cyber insurance changed over the last 12 months? It is more expensive (n=5,157 respondents whose organization has cyber insurance)

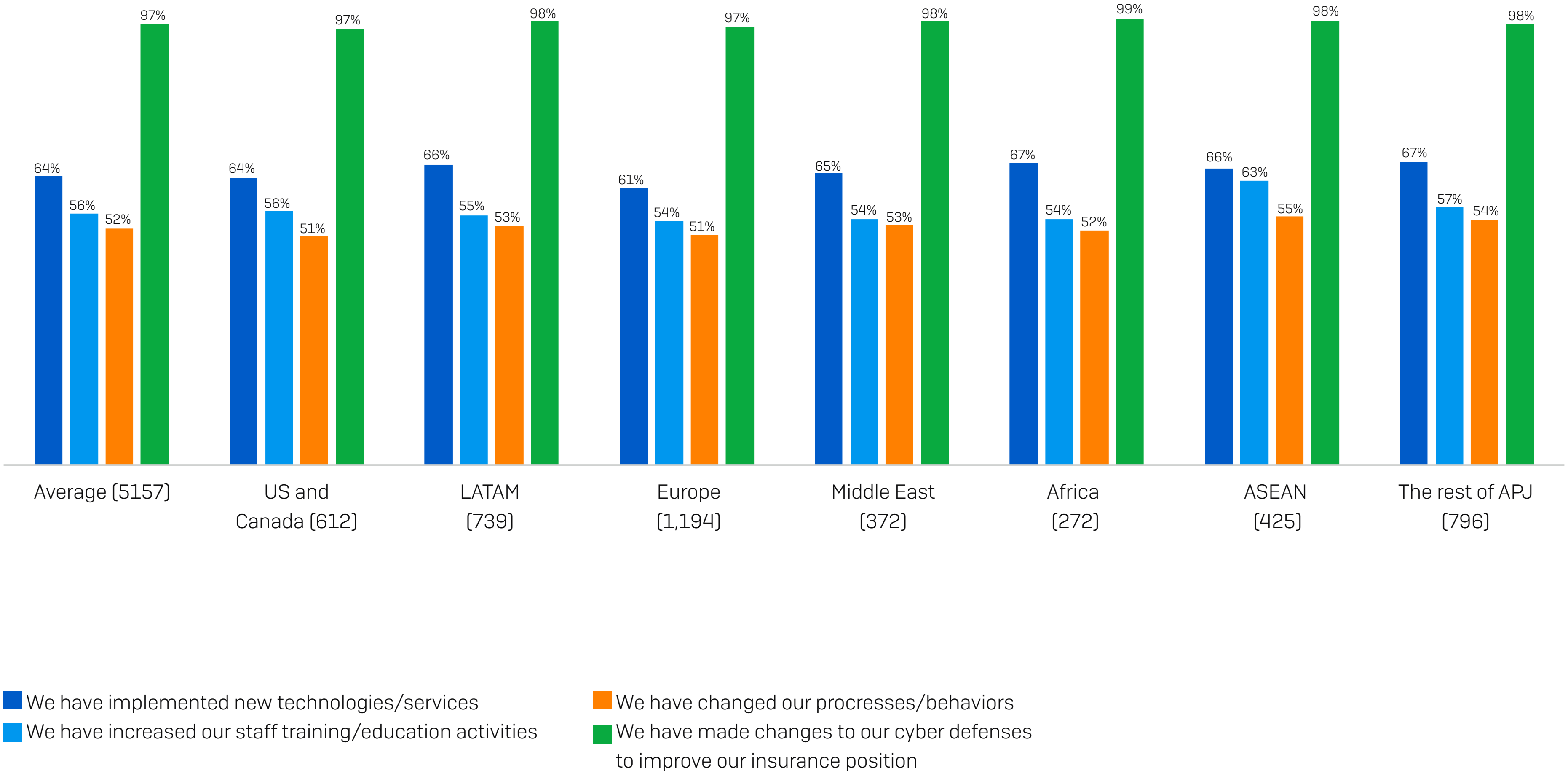
Frontline Experience: Cyber Insurance Is More Difficult to Secure



How has your organization's experience of getting cyber insurance changed over the last 12 months?

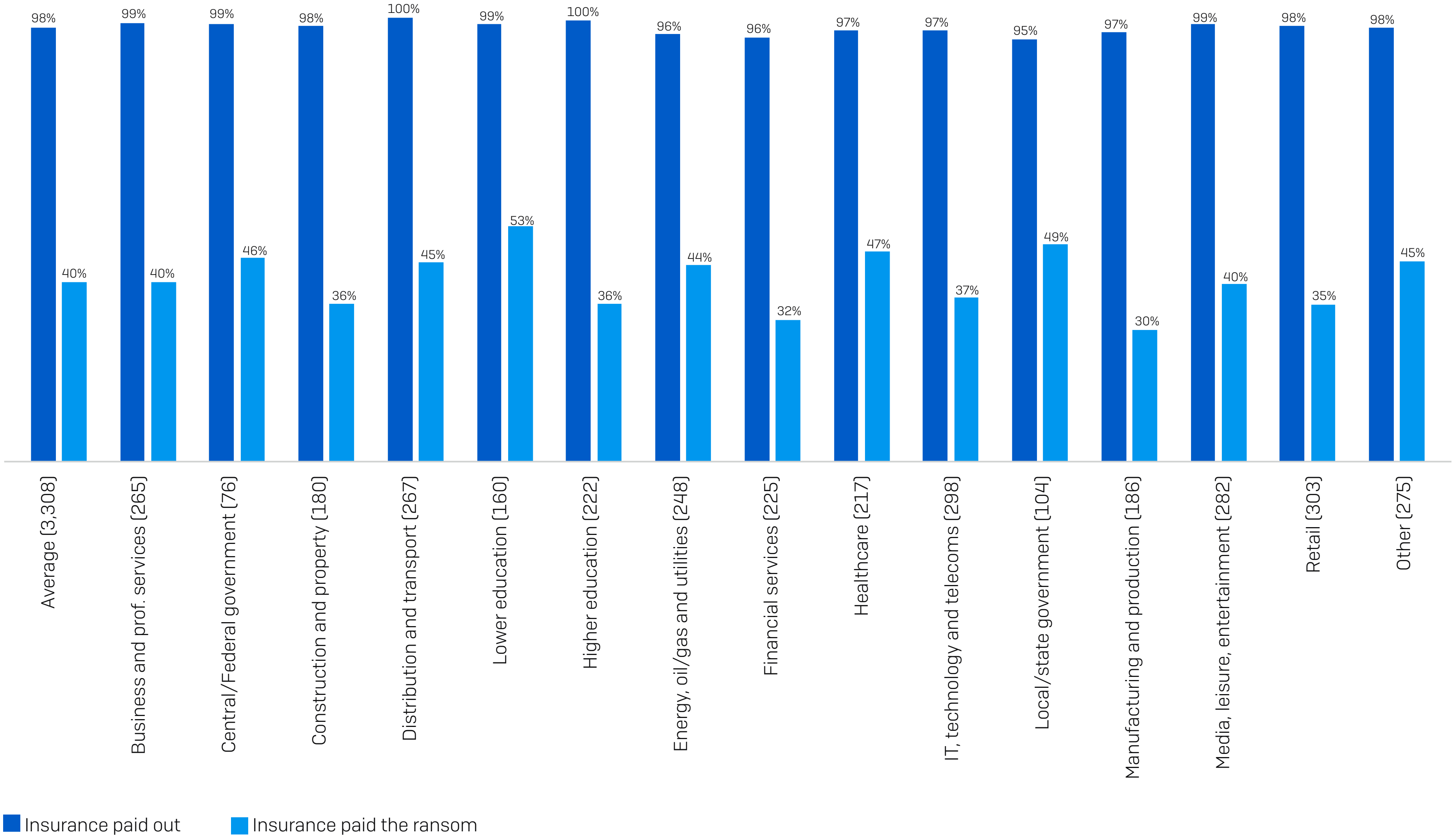
Cybersecurity policies are now more complex/The process takes longer [n=5,157 respondents whose organization has cyber insurance]

Changes to Cyber Defenses to Improve Insurance Position



Over the last year has your organization made any changes to its cyber defenses to improve its insurance position? Organizations that have cyber insurance. Base number in chart. Not showing some answer options

Insurance Pay-out on Ransomware Claims 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.

2022-05-04 (WP-NP)

SOPHOS