SOPHOS

The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption

Findings from a research study into the relationship between cybersecurity, cyber insurance, and ransomware

A Sophos Whitepaper. May 2023

Key Findings

Cybersecurity, cyber insurance, and ransomware are closely connected, with both security and insurance providers focused on reducing the business impact of ransomware, one of the biggest threats facing organizations today.

To understand the reality of this three-way relationship in 2023, Sophos has conducted new research into cyber insurance adoption, the role of cyber defenses in securing a policy, and how insurance coverage impacts response to ransomware incidents.

Our survey of 3,000 cybersecurity/IT professionals conducted in January and February 2023 across 14 countries reveals that:

- 91% of organizations have some form of cyber insurance coverage, with standalone policies slightly more popular than including cyber in a broader business policy
- Cyber insurance adoption increases with revenue, with the highest revenue organizations reporting the highest propensity to have cyber coverage
- 95% of organizations with cyber coverage say that the quality of their cyber defenses directly impacted their insurance position, including their ability to get a policy, the cost of their coverage, and the terms of their policy
- Organizations with cyber insurance are better able to recover data after a ransomware incident, with almost all ransomware victims that have insurance getting their data back
- Organizations with standalone cyber insurance policies and that had data encrypted in a ransomware attack are almost four times more likely to pay the ransom to recover their data than those without cyber coverage

91%
have some form of cyber insurance

95%
report that the quality of the cyber defenses directly impacted their insurance purchase

Organizations with cyber insurance are more likely to recover data encrypted by ransomware

Cyber Insurance Adoption 2023

The research has revealed that cyber insurance is now the norm. Independent of geography, industry or revenue, the vast majority of organizations have some form of cyber coverage:

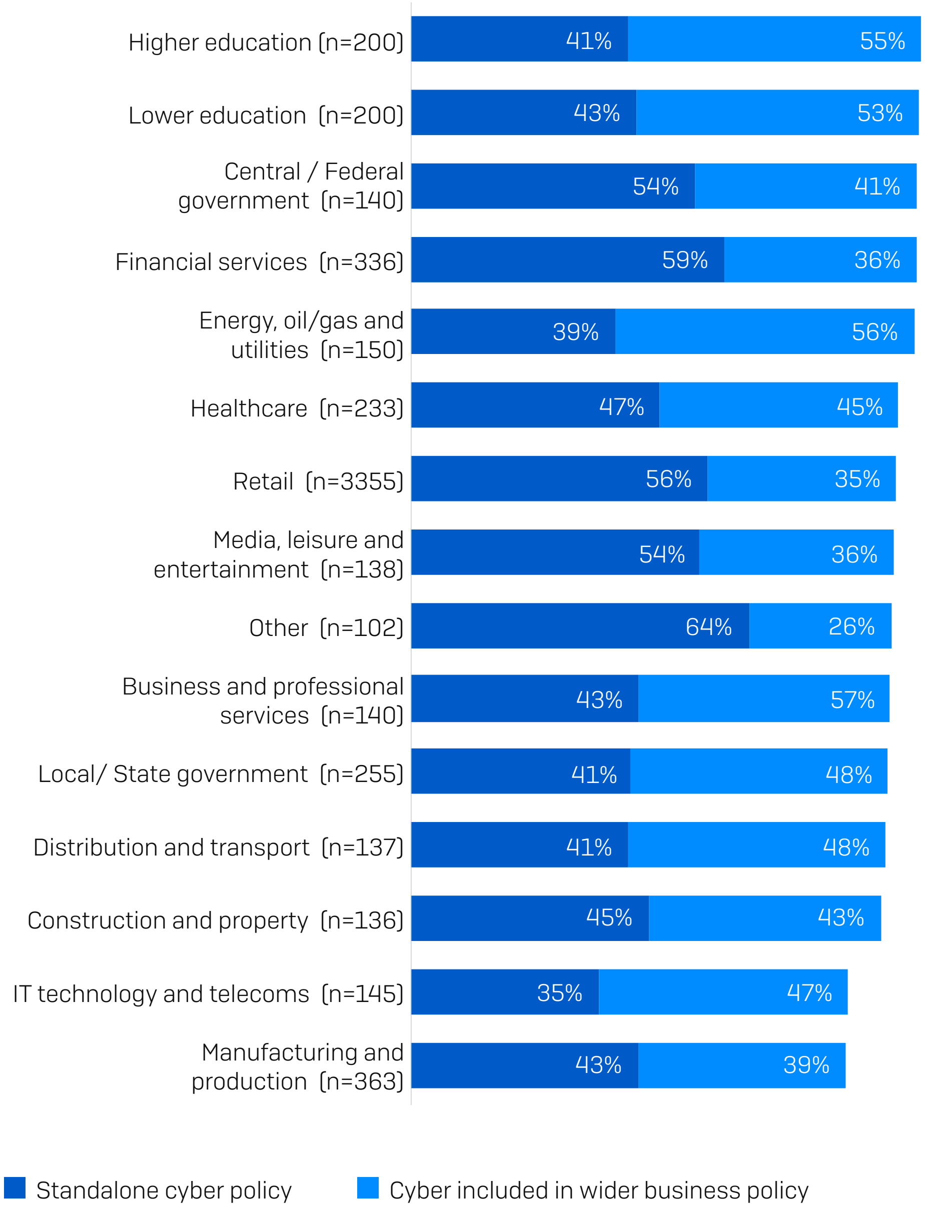
- 47% have a cyber standalone policy
- 43% have cyber insurance as part of a wider business policy
- 8% don't currently have cyber insurance but plan to get coverage in the next year

Note: 91% have some form of coverage due to rounding.

Cyber Insurance Adoption by Industry

At an industry level, education (both higher and lower) reported the highest overall level of cyber insurance coverage (96%) although they are more likely to have cyber as part of a wider business insurance policy than to have a standalone policy.

Financial services is the sector most likely to have a standalone cyber policy (59%), closely followed by retail (56%). Conversely, IT, telecoms, technology is the least likely (35%) with energy, oil/gas, and utilities close behind on 39%.

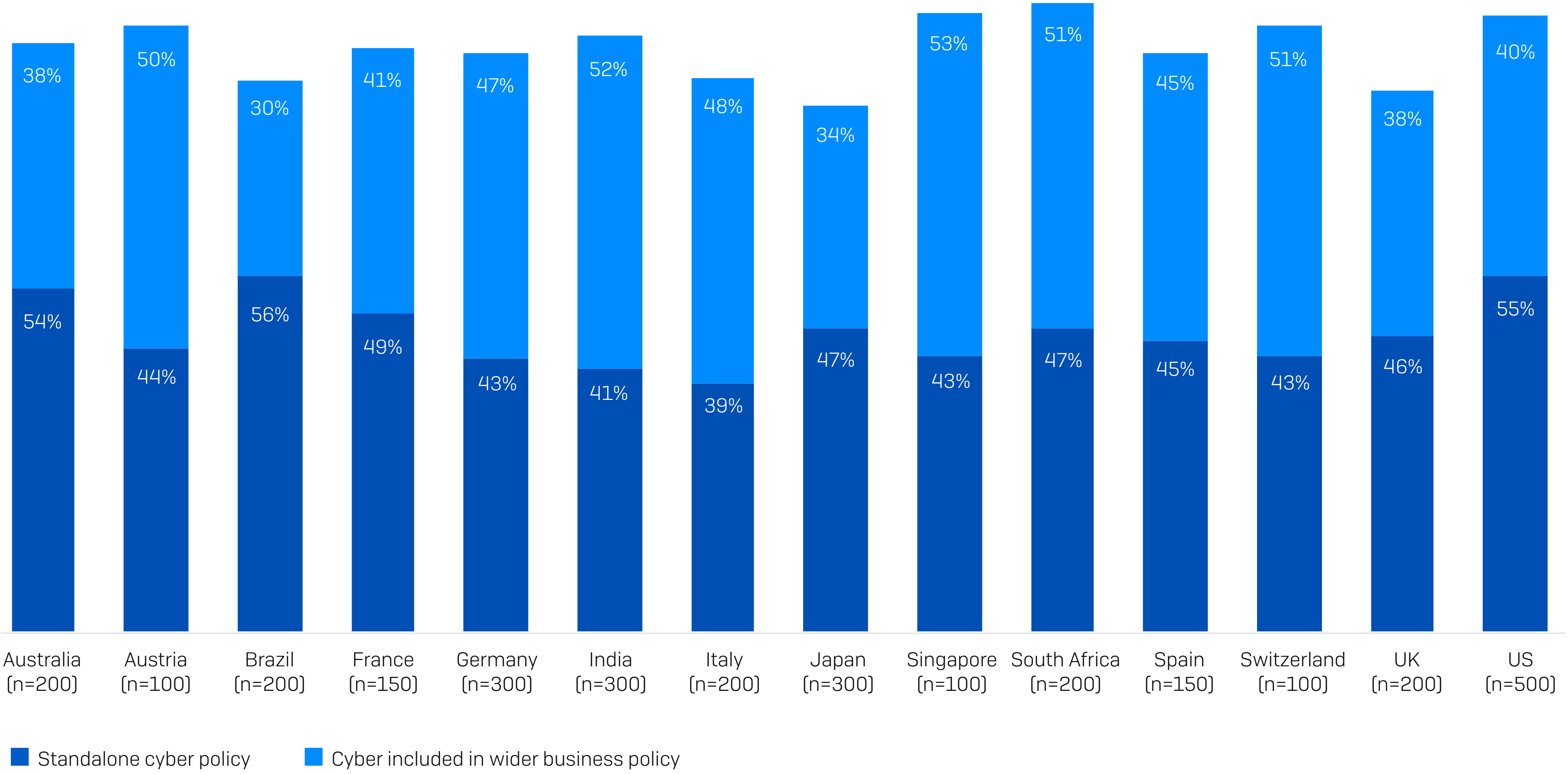


Does your organization have cyber insurance? Yes, we have a standalone cyber insurance policy, Yes, we have cyber insurance as part of a wider business insurance policy (e.g. a general liability policy). Base numbers in chart

Cyber Insurance Adoption by Country

South Africa reports the highest overall rate of coverage of the 14 countries surveyed (98%), while Brazil (56%) and the United States (55%) have the highest levels of standalone policy adoption.

The lowest level of coverage was reported in Japan (82%) although still more than four in five organizations have some form of cyber insurance. Italy reported the lowest level of standalone policy take-up (39%).

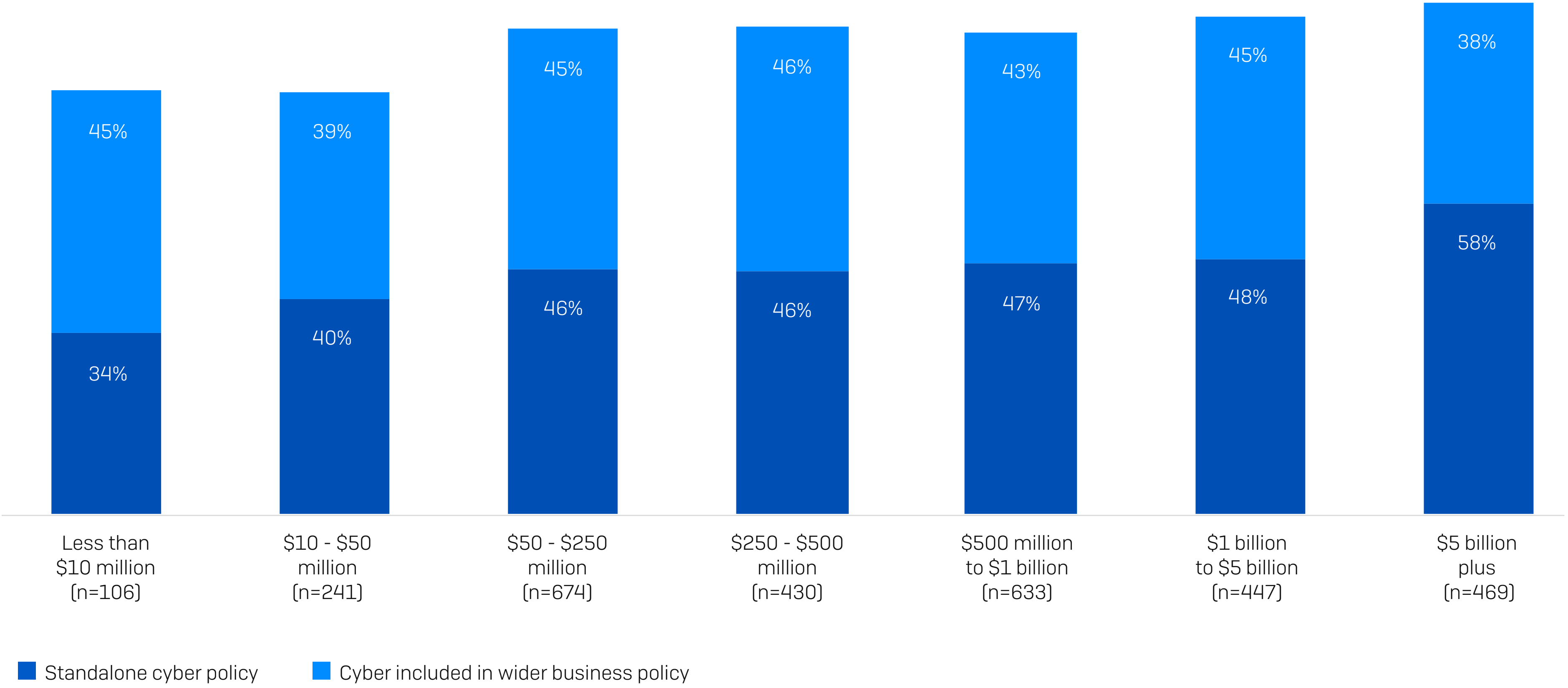


Does your organization have cyber insurance? Yes, we have a standalone cyber insurance policy, Yes, we have cyber insurance as part of a wider business insurance policy (e.g. a general liability policy). Base numbers in chart

Cyber Insurance Adoption by Revenue

Perhaps unsurprisingly, cyber insurance adoption increases with revenue. 96% of organizations with $5 billion + annual turnover have some form of cyber coverage compared with 79% of those reporting revenue of less than $50 million.

Larger revenue organizations also have a greater propensity to have a standalone cyber policy than smaller revenue ones: 58% of organizations reporting an annual revenue of over $5 billion have a standalone policy compared with 34% of those reporting annual revenue of less than $10 million. Overall, the study reveals a steady increase in standalone policy adoption with revenue.



Does your organization have cyber insurance? Yes, we have a standalone cyber insurance policy, Yes, we have cyber insurance as part of a wider business insurance policy (e.g. a general liability policy). Base numbers in chart

Impact of Cyber Defenses on Cyber Insurance Purchase

Quality of cyber defenses is a major factor in the ability of organizations to secure cyber insurance coverage, with 95% of those that purchased a policy in the last year saying their defenses impacted their cyber insurance position.

60% said that the quality of their defenses impacted their ability to get coverage, while 62% said they impacted the cost of their policy. 28% reported that their defenses impacted the terms of their policy e.g., total amount of coverage, sub-limits etc.

Impact of Ransom Payment on the Role of Cyber Defenses in Securing Coverage

Paying the ransom has a considerable impact on the role of cyber defenses in securing a policy – but seemingly not on the cost of the policy. 81% of those that were hit by ransomware in the previous year and paid the ransom reported that the quality of their defenses impacted their ability to get coverage, a 35% increase over the average. However, 59% of those who paid the ransom reported that the quality of their defenses impacted the cost, in line with the global average of 62%. Overall, 99% of those that paid a ransom said their cyber defenses impacted their insurance position in some way.

Organizations with cyber insurance

60%	62%	28%
said that the quality of their defenses **impacted their ability to get coverage**	said that the quality of their defenses **impacted the cost of their coverage**	said that the quality of their defenses **impacted the terms of their policy**

If your organization has purchased a cyber insurance policy in the last year, did the quality of your cyber defenses have an impact on your cyber insurance position? n=2,715 organizations that have cyber insurance

Organizations with cyber insurance *and that made a ransom payment in the last year*

81%	59%	16%
said that the quality of their defenses **impacted their ability to get coverage**	said that the quality of their defenses **impacted the cost of their coverage**	said that the quality of their defenses **impacted the terms of their policy**

If your organization has purchased a cyber insurance policy in the last year, did the quality of your cyber defenses have an impact on your cyber insurance position? n=695 organizations that have cyber insurance and made a ransom payment

Standalone Policy vs. Wider Business Policy

The role of cyber defenses in securing coverage is much greater for standalone cyber policy purchases than when cyber is included in a wider insurance policy. 71% of those with a standalone policy said that the quality of their defenses impacted their ability to get coverage, compared with 49% of those with a more general policy.

Conversely, the quality of cyber defenses is more likely to impact the cost of the policy for those that include cyber in a wider business policy than for those with standalone coverage (67% vs. 58%).

QUALITY OF CYBER DEFENSES HAD AN IMPACT ON:	STANDALONE CYBER POLICY	CYBER INCLUDED IN WIDER INSURANCE POLICY
Ability to get coverage	71%	49%
Cost of coverage	58%	67%
Terms of policy	24%	32%

If your organization has purchased a cyber insurance policy in the last year, did the quality of your cyber defenses have an impact on your cyber insurance position? n=2,715 organizations that cyber insurance

Cyber Insurance and Ransomware

Encrypted Data Recovery

Organizations with cyber insurance are more likely to be able to recover data following a ransomware incident than those without coverage. The study revealed very little difference in data recovery between those with a standalone policy and those with a wider business policy, with almost everyone with some form of cyber coverage getting some data back. Conversely, only 84% of organizations without cyber coverage reported that they could recover data.

For all three groups, backups were the most common method used to recover data, followed by paying the ransom. One fifth (21%) of organizations reported using multiple methods to recover their data. Factors that may drive the increased ability of organizations with cyber insurance to recover data include:

- Assistance from the insurer in the data recovery process
- The strong cyber controls required to secure a policy put organizations in a better position to recover data e.g., secure backups, incident response plan

Percentage of ransomware victims that recovered encrypted data

98%	97%	84%
With a standalone cyber policy	With a wider insurance policy that includes cyber	Without a cyber policy

Did your organization get any data back? n=1,497 organizations that were hit by ransomware in the last year and had data encrypted

Propensity to Pay the Ransom

The study also revealed that ransomware victims with standalone cyber insurance policies are almost four times more likely to pay the ransom to recover encrypted data than those without cyber coverage.

58% of organizations with a standalone cyber insurance policy and had data encrypted in a ransomware attack last year paid the ransom to get their data back. In comparison, 36% of those with cyber as part of a broader insurance policy paid the ransom and 15% of those without cyber insurance.

Standalone cyber policy	Wider insurance policy that includes cyber	No cyber policy
58% paid the ransom	**36%** paid the ransom	**15%** paid the ransom

Did your organization get any data back? Yes, we paid the ransom and got data back. n=1,497 organizations that were hit by ransomware in the last year and had data encrypted (771 standalone policy, 658 cyber as part of wider policy, 67 no cyber policy)

Optimize your Cyber Defenses with Sophos

The research has highlighted the importance of the quality of cyber defenses for the purchase of cyber insurance. Sophos' award-winning managed detection and response (MDR) and incident response services, and endpoint detection and response (EDR), extended detection and response (XDR), network, email, and cloud security technologies enable organizations to optimize their protection and their insurance position.

Sophos services and products to protect more than 500,000 organizations from active adversaries, ransomware, phishing, malware, and more, and Sophos is the world's most trusted MDR service, securing more than 15,000 customers with 24/7 human-led threat detection and response.

Testament to the quality of our defenses, Sophos has been named a Leader in the Gartner Magic Quadrant for Endpoint Protection Platforms for 13 consecutive reports and is AAA rated by SE Labs with a 100% protection score. Customers give Sophos top ratings on Gartner Peer Insights and G2 alike, and Sophos is also the only provider named a Leader for MDR, XDR, EDR, Endpoint Protection, and Network Firewalls in G2's Spring 2023 Reports.

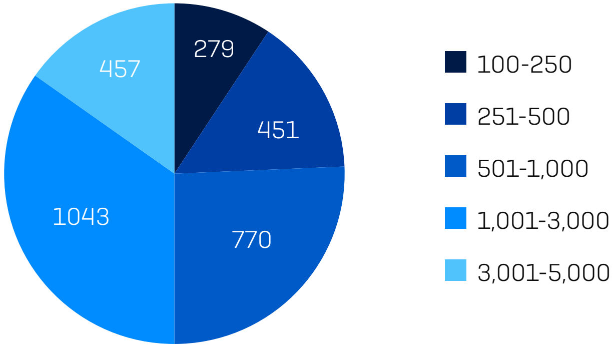
To discuss your cybersecurity requirements and how Sophos can help you elevate your defenses, visit www.sophos.com to speak to one of our security advisers today or start a no-obligation free trial.

About the Survey

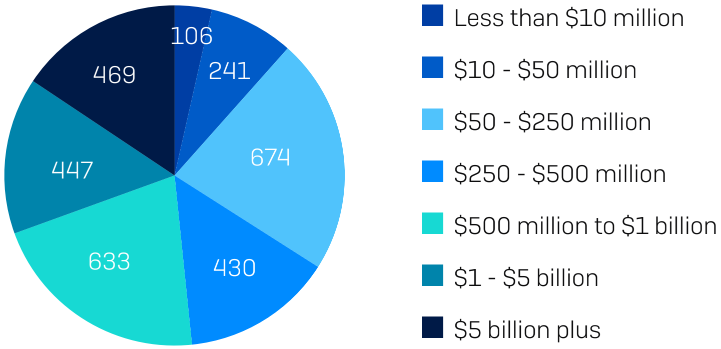
Sophos commissioned an independent survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries. All respondents were from organizations with between 100 and 5,000 employees (50% 100-1,000 employees, 50% 1,001-5,000 employees). The research was conducted in January and February 2023 and reflects organizations experiences of ransomware and cyber insurance in the previous 12 months.

COUNTRY	NUMBER OF RESPONDENTS	COUNTRY	NUMBER OF RESPONDENTS
United States	500	United Kingdom	200
Germany	300	South Africa	200
India	300	France	150
Japan	300	Spain	150
Australia	200	Austria	100
Brazil	200	Singapore	100
Italy	200	Switzerland	100

Respondents by Organization Size (number of employees)



Respondents by Organization Size (annual revenue)



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.

2023-04-28 (WP-NP)