SOPHOS

Cyber Insurance and Cyber Defenses 2024: Lessons from IT and Cybersecurity Leaders

Real-world insights into cyber insurance adoption, claim payouts, and the interplay between cyber defenses and insurance coverage.

A Sophos Whitepaper. June 2024

Introduction

Cyber risk is inevitable. No business with internet-connected devices can eliminate cyber risk entirely; rather it's a question of how to manage it. Two of the primary approaches to cyber risk management are treatment by deploying cyber controls and changing user behaviors, and transfer through cyber insurance. Treatment and transfer are complementary elements of a balanced cyber risk management program, and each organization needs to identify where their equilibrium lies.

Cyber risk treatment and transfer are also interconnected, with security controls and behaviors having a direct impact on an organization's ability to transfer risk through insurance. Strong, effective cyber controls reduce cyber risk, making it easier to access lower priced coverage. Conversely, organizations with weak risk treatment often struggle to get the policy they need at a price they can afford.

With cyber risk now a board-level consideration for many organizations, this report shines light on cyber insurance adoption in mid-sized organizations, including the factors driving the purchase. It provides new insights into the interplay between defenses and insurance, illustrating the impact of investment in defense improvements on insurability. It also explores payout on claims, including the primary reasons for claims being denied.

Based on an independent survey of 5,000 leaders

The report is based on the findings of an independent, vendor-agnostic survey commissioned by Sophos of 5,000 IT/cybersecurity leaders across 14 countries in the Americas, EMEA, and Asia Pacific. All respondents represent organizations with between 100 and 5,000 employees. The survey was conducted by research specialist Vanson Bourne between January and February 2024, and participants were asked to respond based on their experiences over the previous year.

Executive summary

In the face of inevitable cyberattacks, adopting a holistic approach to cyber risk management that takes advantage of the interplay between cyber defenses and cyber insurance will enable organizations to lower their overall total cost of ownership (TCO) of cyber risk management while reducing their likelihood of experiencing a major incident.

As the survey findings illustrate, cyber insurance acts as both a carrot and a stick for security investments. By setting minimum security control requirements to attain coverage – the "stick" - the insurance industry is effectively forcing many organizations to elevate their cyber defenses. A common example is multi-factor authentication (MFA), which is often a prerequisite for policy purchase.

In parallel, by recognizing and rewarding strong defenses through lower premiums, higher policy limits and improved terms, cyber insurers are incentivizing risk reduction through superior protection. An example of this "carrot" is the improved access to coverage and lower policy costs that many insurance providers offer to organizations using a managed detection and response (MDR) service.

The research also reveals that investing in cyber defenses to optimize your insurance position is a double win: organizations report both easier and cheaper access to coverage as well as wider benefits such as improved protection, fewer alerts, and freeing up IT time. This finding further emphasizes the importance of considering cyber risk investments holistically, rather than as individual components.

One area of concern highlighted by the survey is the potential for policy purchases to be misaligned to business needs. Cyber insurance is an investment, and organizations should be sure that their policy provides the coverage they need in the event of a major incident. All stakeholders, including the IT/cybersecurity teams that will be at the frontline if an incident occurs, should be involved in the insurance policy decisions to ensure that any investment meets the organization's needs.

Cyber insurance adoption 2024

The survey confirms that adoption of cyber insurance is widespread within organizations with 100-5,000 employees, with 90% of organizations having some form of cyber coverage. 50% have a standalone policy while 40% have cyber as part of a wider business insurance policy, such as a general liability policy.

Organizational revenue has little impact on propensity to have cyber coverage:

- 92% of those with less than $50M annual revenue have coverage (n=664)
- 93% of those with $1B+ annual revenue have coverage (n=1,907)

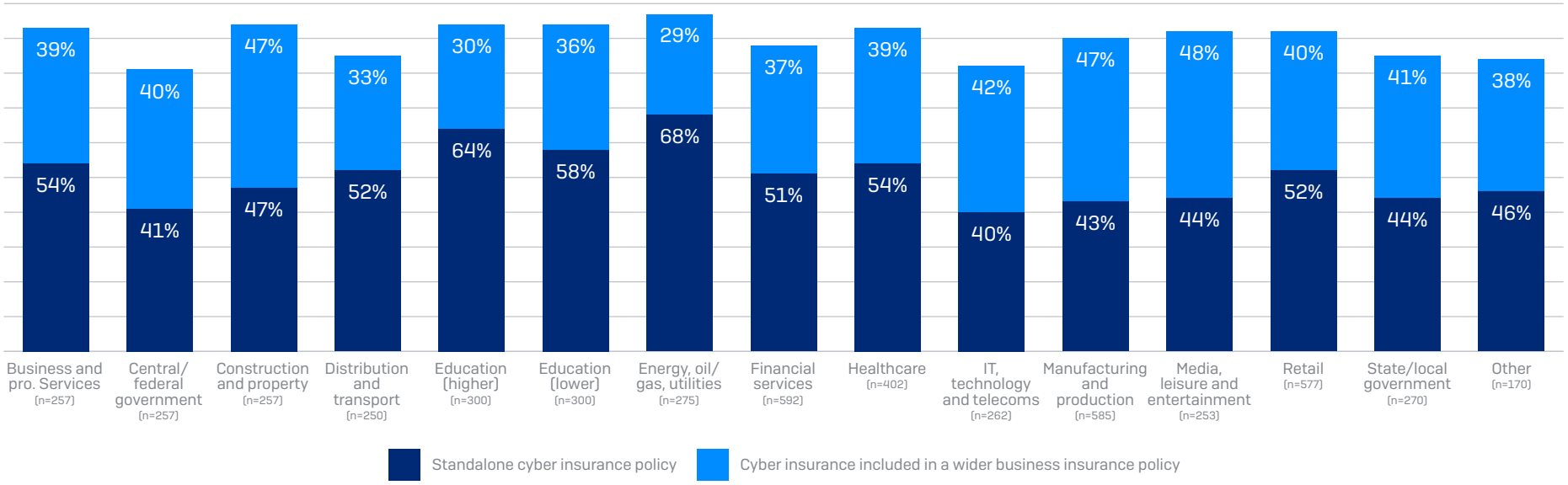
Similarly, when we look at the data based on the number of employees, there are just five percentage points difference between the highest adoption rate (93%, 100-250 employees) and the lowest (88%, 1,001-3,000 employees).

Adoption rates by industry

Energy, oil/gas, and utilities is the sector with the highest rate of insurance adoption (97%) and also the highest use of standalone cyber insurance policies (68%) to transfer risk. This likely reflects the high level of regulation in the sector and high potential liability. It is also likely a result of the industry's widespread use of legacy technology and infrastructure controls, which make it harder to secure devices, limit lateral movement, and prevent attacks from spreading.

Central/federal government reports the lowest adoption rate together with *IT, technology, and telecoms* (both 81%). However, with more than four in five organizations in all sectors having coverage, it's clear that cyber insurance is very much the norm.

Cyber insurance adoption by industry

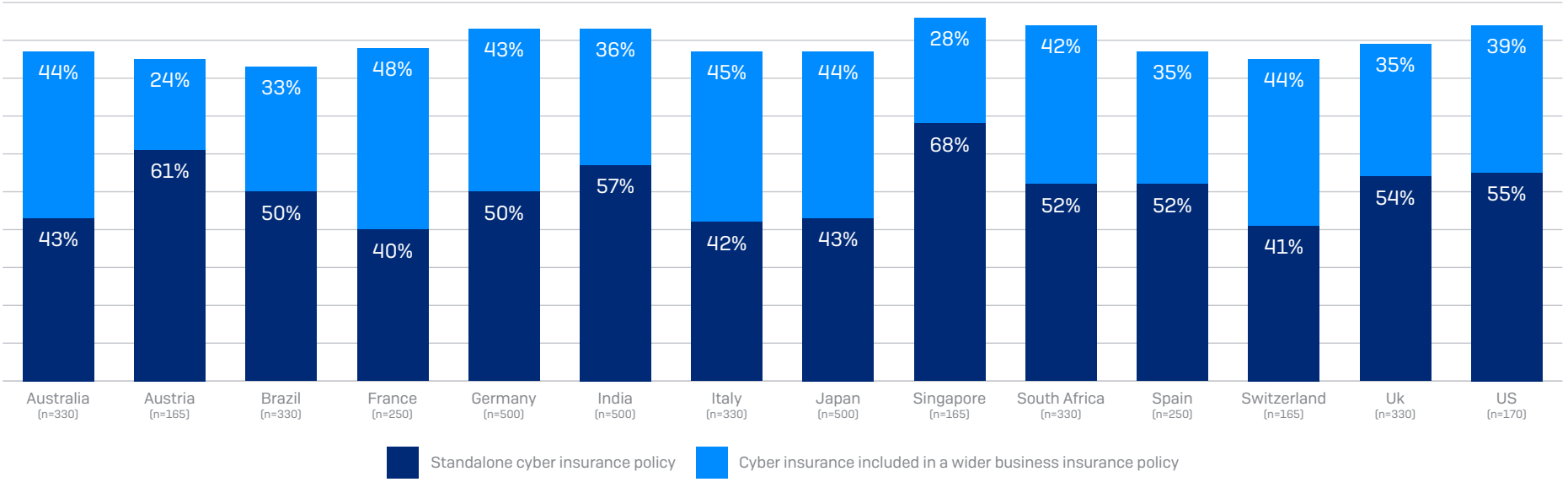


Does your organization have cyber insurance? Yes, we have a standalone cyber insurance policy; Yes, we have cyber insurance as part of a wider business insurance policy (e.g. a general liability policy). Base numbers in chart.

Adoption rates by country

Cyber insurance is widely used to transfer cyber risk in all countries surveyed. Respondents in Singapore reported the highest adoption rate (96%), and those in Brazil the lowest (83%). Singapore also has the highest percentage of organizations with standalone cyber policies (68%), while France has the greatest coverage through business policies that include cyber (48%).

Cyber insurance adoption by country



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.

Factors driving cyber insurance adoption

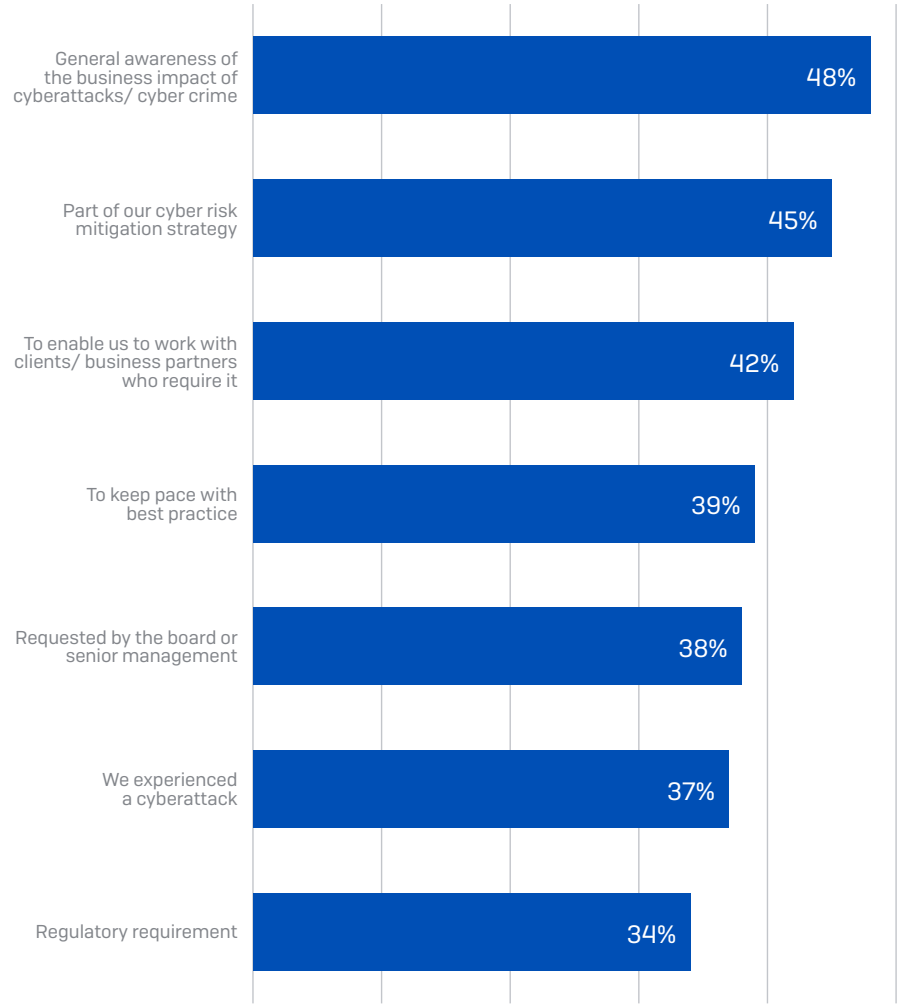
While multiple factors motivate organizations to adopt cyber insurance, *general awareness of the business impact of cyberattacks/cyber crime* is the most common reason behind the purchase, cited by 48% of respondents. Approaching half (45%) of respondents said that cyber insurance is *part of their cyber risk mitigation strategy*.

In third position is *to enable us to work with clients/business partners* who require it (42%). Cyber insurance is increasingly a condition of doing business as organizations look to mitigate the risk of supply chain attacks by ensuring their commercial partners have insurance coverage. We will explore this at an industry level on the next page.

Board or senior management request is a contributing factor to more than a third (38%) of purchases, illustrating the business-critical impact of the effects of a cyber incident. While *regulatory requirement* is the least common purchase driver overall (34%), there is considerable variation by sector, reflecting their different compliance needs.

- Highest
  - 48% of respondents in IT, technology and telecoms
  - 40% of respondents in energy oil/gas and utilities
- Lowest
  - 25% of respondents in local government
  - 26% of respondents in construction and property

Factors driving cyber insurance purchases



What main factor(s) drove the decision for your organization to purchase cyber insurance? n=4,498 organizations with cyber insurance.

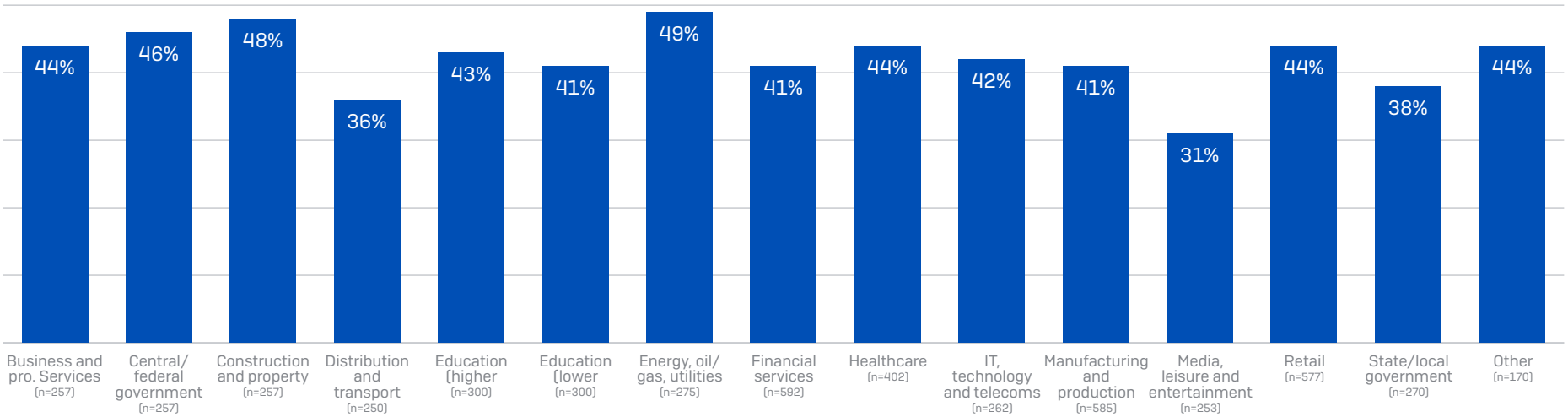
Insurance as a condition of business

Across all sectors, the *need to enable us to work with clients/business partners who require it* contributed to 42% of insurance purchases. When we dive deeper, we see that there is considerable variation by industry.

Energy, oil/gas and utilities has the highest proportion of respondents that cited business requirement as a purchase driver (49%), closely followed by *construction and property* (48%). It is likely that the high impact of attacks on the energy/utilities sector together with their legacy technology challenges is driving a high need for risk mitigation through insurance in their clients and business partners.

Conversely, *media, leisure and entertainment* is the sector least likely to be motivated by this purchase driver (31%), followed by distribution and transport (36%). This result in the logistics sector is surprising given that, if a distribution provider is paralyzed by an attack, the ramifications for the customers whose goods cannot be delivered is very high.

Insurance as a condition of business by industry



What main factor(s) drove the decision for your organization to purchase cyber insurance? To enable us to work with clients/ business partners who require it. n=4,498 organizations with cyber insurance.

Policy coverage

Respondents were asked what their policy would cover in the event of a cyber incident, revealing widespread uncertainty as to what assistance they would receive if they made a claim.

Illustrating this point, 40% of respondents whose organization has a cyber insurance policy *think* it covers ransom payments, but are not certain, and 41% *think but are not sure* that their policy covers income loss.

These findings are cause for concern on several fronts:

1. **Organizations risk not getting the coverage they need.** It is essential that all parties within the business are clear on what they require in their policy and these needs inform the insurance purchase.
2. **Organizations risk not getting the support they expect in the event of a claim.** Dealing with a major cyber incident is a stressful and pressured time for all involved. To discover in the heat of an attack that expected support is not included in the insurance policy adds further complexity, delay, and cost to remediation.

The lack of visibility into policy coverage likely results, at least in part, from a disconnect between those purchasing the policy (typically finance and/or compliance teams) and those on the frontline should a major incident occur (typically IT and cybersecurity functions). Organizations should be sure to involve all stakeholders in the purchase decision, and to ensure that all parties are aware of what the policy does and does not cover. This will enable teams to put in place alternative options to address any gaps.

Ransomware is one of the biggest cyberthreats facing businesses today and the financial impact on victims can be severe. The average (median) ransom payment is now $2M, and the overall recovery cost excluding any ransom payment comes in at $2.73M (source: The State of Ransomware 2024, Sophos). It is therefore surprising to see that one in ten organizations has invested in insurance that does not cover many of the costs incurred with a ransomware attack, including ransom payments, breach notification, breach negotiations and income loss.

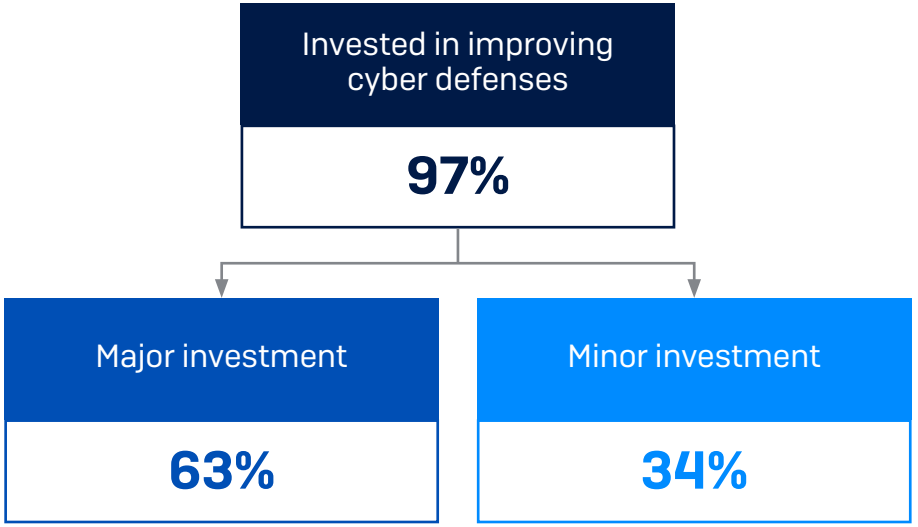
Policy coverages

	RANSOM PAYMENTS	DATA RECOVERY SERVICES	BREACH NOTIFICATIONS	PR SUPPORT/ REPUTATION MANAGEMENT	INCIDENT RESPONSE SUPPORT	BREACH NEGOTIATIONS	INCOME LOSS	COMPUTER SYSTEM RESTORATION
I know it covers this	50%	58%	47%	47%	54%	48%	49%	55%
I think it covers this, but it might not	40%	35%	43%	42%	38%	42%	41%	38%
I know it doesn't cover this	10%	7%	9%	11%	8%	10%	10%	7%
Don't know	0%	0%	0%	1%	0%	1%	0%	0%

What does your organization's cyber insurance policy cover in the event of a cyber incident? n=4,498 organizations with cyber insurance.

Cyber insurance and cyber defense investments

97% of organizations that purchased a cyber insurance policy last year said that they invested in improving their defenses to optimize their insurance position. Almost two thirds (63%) said they made major investments in their cyber defenses while 34% made minor investments.



If your organization has purchased a cyber insurance policy in the last year, did you invest in improving your cyber defenses to optimize your cyber insurance position? n=4,498.

Cyber insurance and cyber defense investments by industry

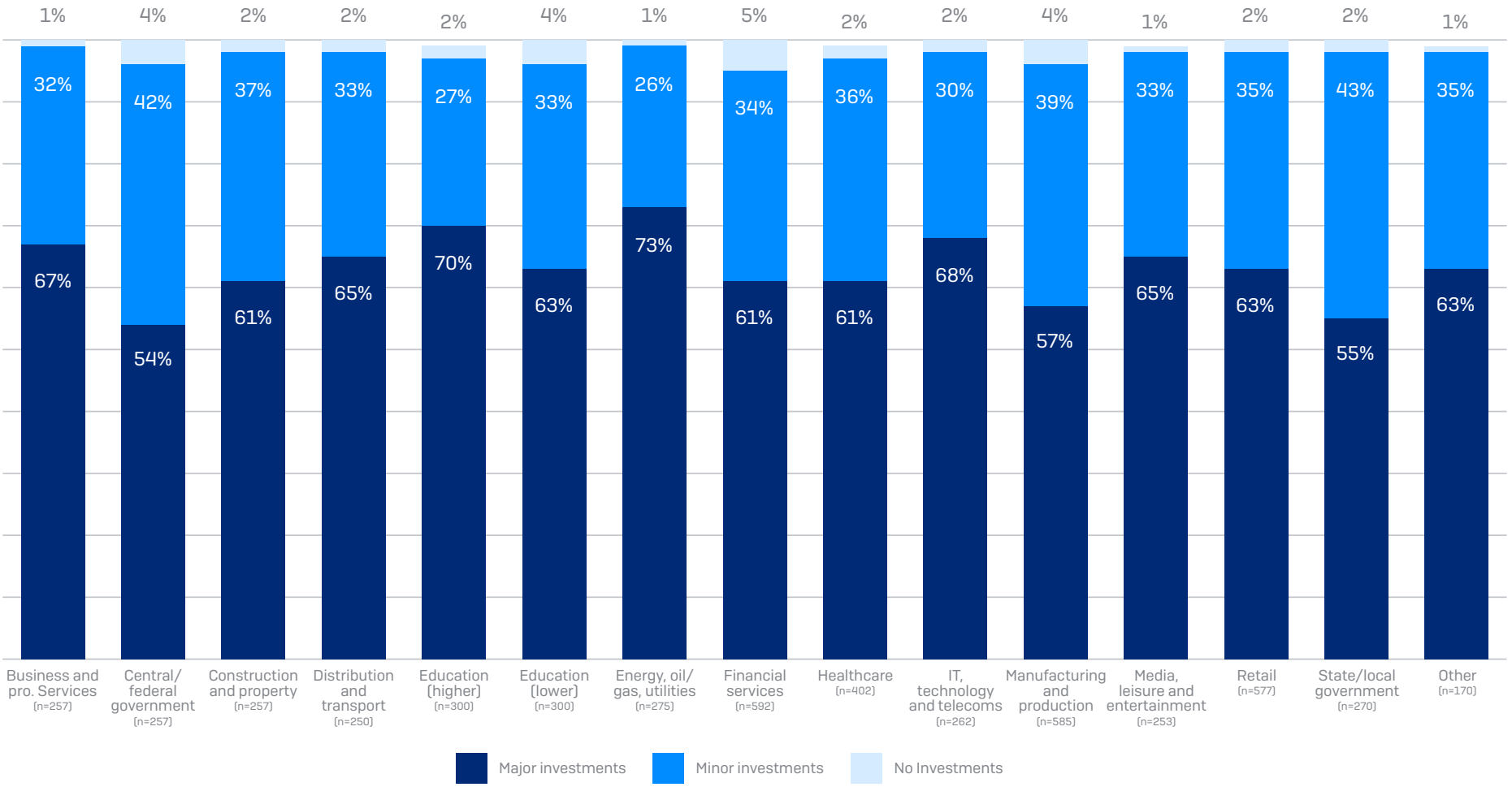
While almost all organizations across all sectors that purchased a policy invested in improving their defenses to improve their insurance position, some sectors report higher levels of major investment than others.

Energy, oil/gas and utilities had the highest percentage of respondents that said they had made major investments in their cyber defenses in order to optimize their insurance position (73%). This likely reflects the cybersecurity struggles the industry has faced due to high levels of legacy technology as well as the high impact of critical infrastructure outages.

Higher education reported the second highest level of major investment (70%). This sector has also been challenged by previous under-investment in cyber defenses, increasing exposure to attack.

The two government sectors are least likely to have made major investments in their defenses (54% in *central/federal government*, 55% in *state/local government*). It may be that strained government budgets have reduced available funding for these industries.

Cyber insurance and cyber defense investments by industry



If your organization has purchased a cyber insurance policy in the last year, did you invest in improving your cyber defenses to optimize your cyber insurance position? Base numbers in chart.

Impact of cyber defense investments on cyber insurance position

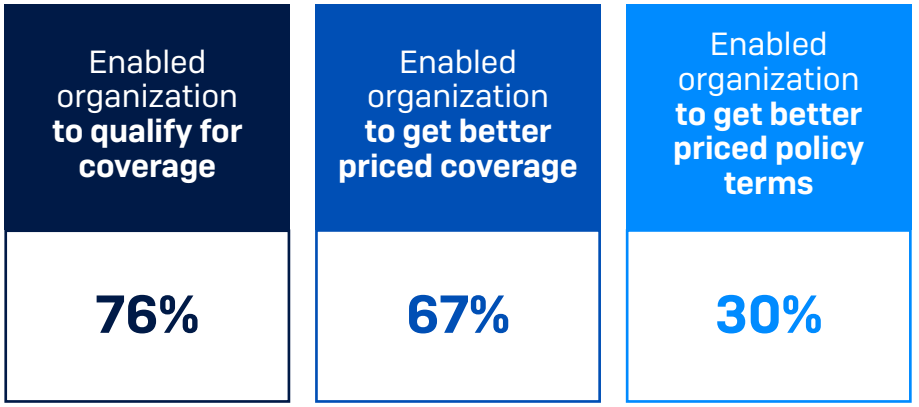
The good news for any organization considering spending in this area is that almost every company that invested in improving their cyber defenses said it had a positive impact on their cyber insurance position (99.6%, 4,351 of 4,370 respondents).

Substantiating the role of cyber insurance as a "stick" to drive better defenses, over three-quarters (76%) of respondents said that their investment enabled them to get insurance coverage that they would not have been able to secure otherwise.

The "carrot" is that two thirds of organizations were able to access better priced coverage (e.g., cheaper premiums or lower deductible/excess) as a result of their investments in their cyber defenses, while 30% said their improved protection enabled them to get better terms (e.g., higher coverage limits).

These figures make clear the importance of considering the overall total cost of ownership (TCO) of cyber risk reduction. **Investments in elevated defenses unlock cyber insurance savings** while also reducing the likelihood of experiencing a major cyber incident.

Impact of cyber defense investments

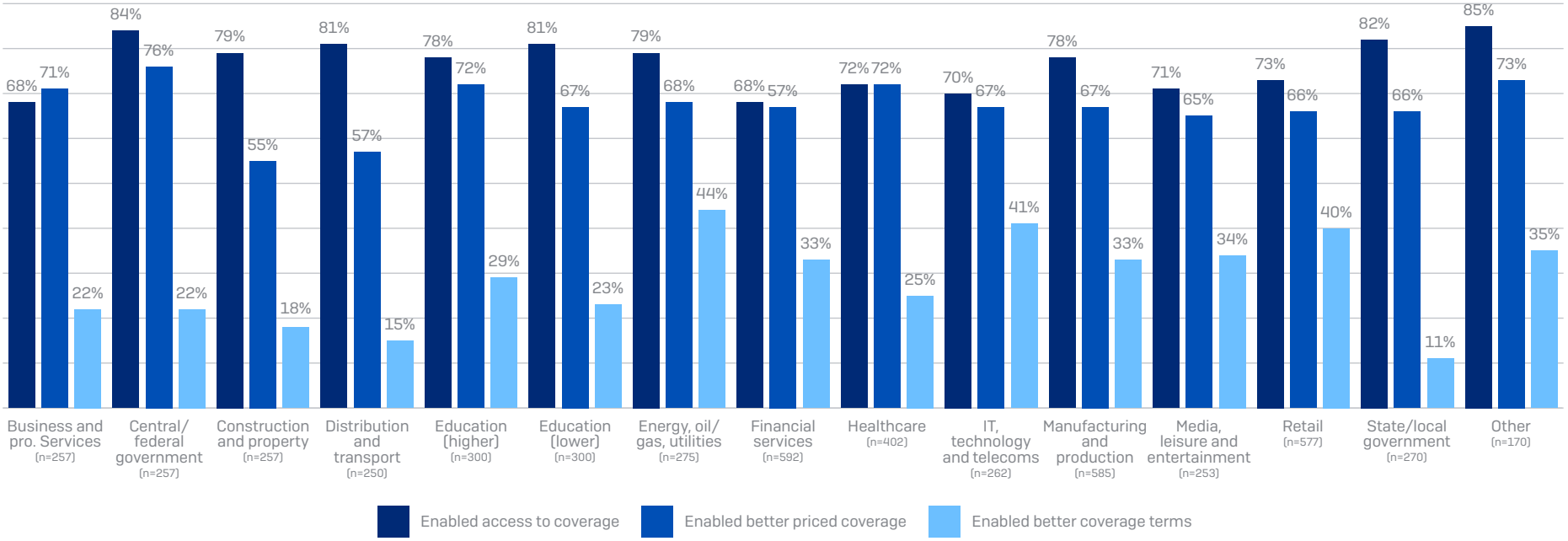


How did investing in improving your cyber defenses positively impact your insurance position? n=4,370 organizations that invested in improving their cyber defenses to optimize their cyber insurance position

Impact of cyber defense investments by industry

Across all sectors, the insurance benefits of cyber defense investments are considerable. While there are no losers, *central/federal government* is the named sector with the highest percentage of respondents reporting that their improvements enabled them to qualify for coverage (84%) and is also the sector that most benefited from better priced coverage (76%). *Energy, oil/gas and utilities* has the highest percentage of respondents able to access better coverage terms as a result of their investments (44%).

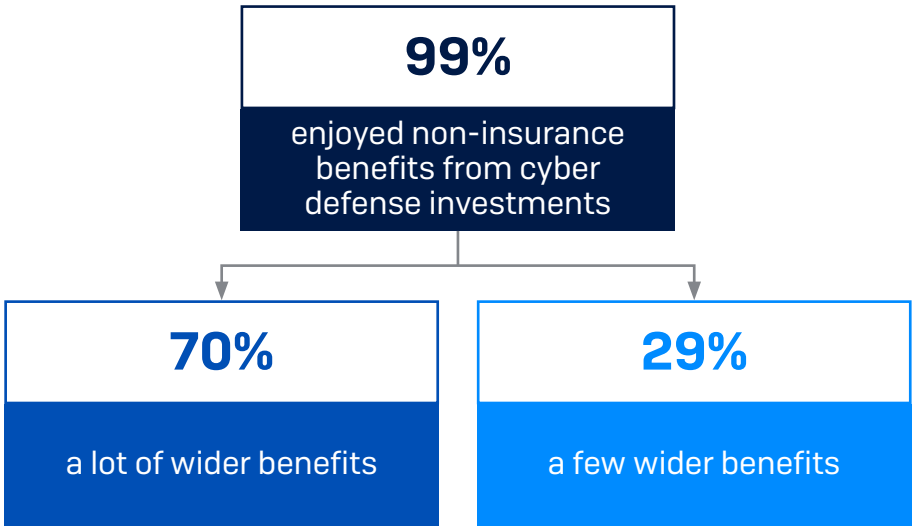
Impact of cyber defense investments by industry



How did investing in improving your cyber defenses positively impact your insurance position? Base numbers in chart

Broader impact on defense investments

Not only do organizations that invest in improving their cyber defenses see insurance benefits, 99% also report wider benefits to their organization, such as improved protection, fewer alerts, freeing up IT time, etc. Diving deeper, we see that 70% have seen a lot of wider benefits from their improved cyber defenses, while 29% have seen a few wider benefits.



Did investing in improved cyber defenses for cyber insurance purposes positively impact your organization in other ways? n=4,370 organizations that made investments in improving their defenses to optimize their cyber insurance position.

All industries reported high levels of wider benefits from their investments, however *energy, oil/gas and utilities* was most likely to report seeing a lot of wider benefits (82%). Conversely, *manufacturing and production* had the lowest percentage reporting wider benefits – although even here nearly two thirds (63%) saw a considerable positive impact.

These wider benefits are the icing on the cake for organizations that make cyber defense improvements: not only do they benefit from easier and cheaper access to coverage, they also enjoy reduced cybersecurity impact.

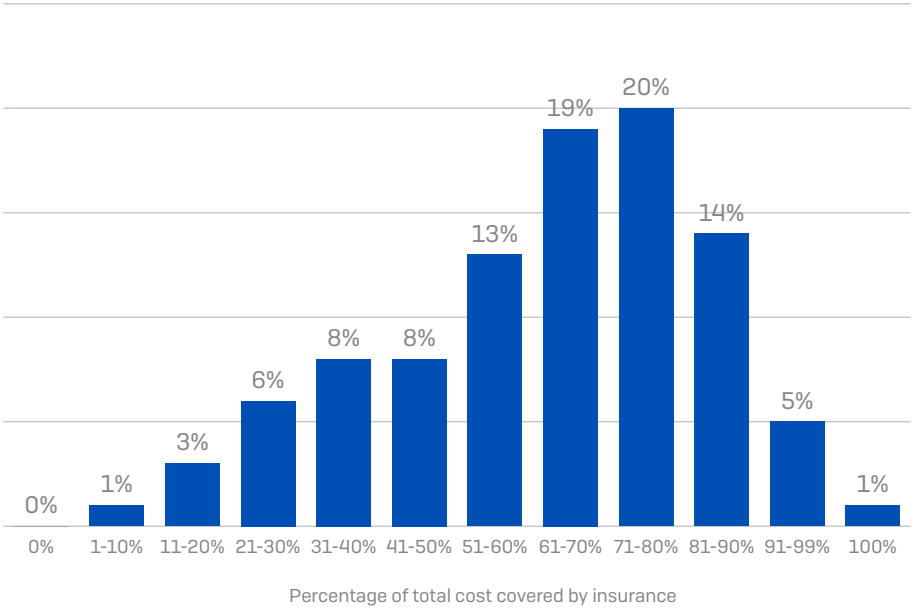
Percentage of costs covered by insurance

Cyber insurance enables organizations to transfer cyber risk, providing peace of mind that they will not be exposed to the full costs of the incident should the worst happen.

Organizations that have invested in a cyber policy will be encouraged to learn that insurers almost always pay out in some capacity on a claim. Overall, only one respondent said that their carrier did not pay out at all on their claim.

At the same time, insurers rarely cover the full incident cost, with 1% saying the carrier funded 100% of their costs incurred. Overall, insurers typically paid 63% of the total incident cost, with the modal payout rate coming in at 71-80%.

Percentage of total incident costs covered



If you made a claim on your organization's cyber insurance policy in the last year, what percentage of the total incident cost did the insurance cover? n=3,945

Reasons for costs not being fully covered

The reasons why the total incident cost was not covered by the insurance provider shine important light that can help inform future policy purchases.

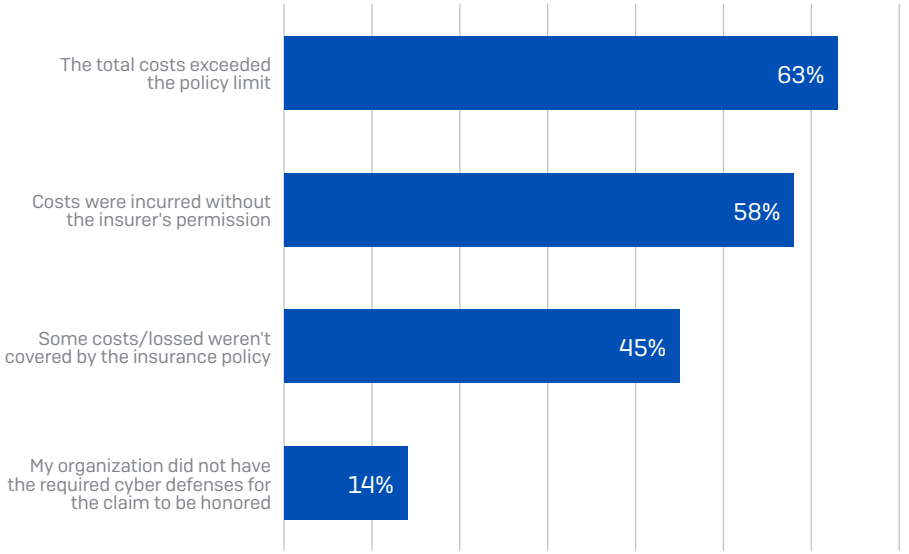
The most common reason for the recovery bill to not be paid in full is that the *total costs exceeded the policy limit* (63%). With the average cost to remediate a ransomware attack now $2.73M, organizations should ensure that their policy provides sufficient coverage should they experience a major incident.

In second position is *costs were incurred without the insurer's permission*, cited in 58% of cases. Organizations are advised to be aware of the requirements of their policies and the processes they need to follow in order for claims to be allowed.

45% of respondents said that they had *costs/losses that weren't covered by the insurance policy*. With nearly one in two cyber-attack victims reporting it, this suggests that mis-alignment of policy and needs is widespread.

14% of denied claims (one in seven) were due to the organization *not having the required cyber defenses for the claim to be honored*. Insurance providers stipulate required security controls as a condition of coverage, for example, regularly patching vulnerabilities, not running end-of-life software, or deploying an endpoint detection and response (EDR) solution. Not adhering to these requirements exposes organizations to the risk that they will not see full return on their insurance purchase.

Reasons why cyber insurance did not cover the full incident cost



Why didn't your organization's cyber insurance cover the total incident cost? n=3,886 organizations that did not have their full claim covered by the insurance provider

Impact of cyber insurance coverage on ransomware outcomes

The goal of insurance is to reduce the impact of perils on an organization. With this in mind, we analyzed the findings from the Sophos State of Ransomware 2024 study to identify whether there is any correlation between insurance position and outcomes, focusing on five core milestones of the victim journey:

- Propensity to be hit by ransomware
- Propensity to have data encrypted
- Ransom payment amount
- Propensity to pay the ransom to recover encrypted data
- Overall recovery costs (excluding the ransom payment)

One important caveat to preface this analysis is that ***we do not know whether the victim's current insurance policy was purchased before or after their ransomware attack***, i.e. if the purchase decision was influenced by their prior ransomware experience or whether it was already in place. However, with cyber insurance adoption by State of Ransomware participants remaining stable over the last two years (90% in the 2024 study, 91% in the 2023 study) the analysis provides a reasonable indicative starting point to facilitate further research in this area.

Propensity to be hit by ransomware

The data shows very little difference in the ransomware attack rate based on cyber insurance adoption, with all three groups reporting very similar propensity to have been hit in the last year:

- 62% with a standalone policy were hit by ransomware in the last year (n=2,523)
- 57% with cyber as part of a wider policy were hit by ransomware in the last year (n=1,975)
- 58% without a cyber policy were hit by ransomware in the last year (n=489)

Propensity to have data encrypted

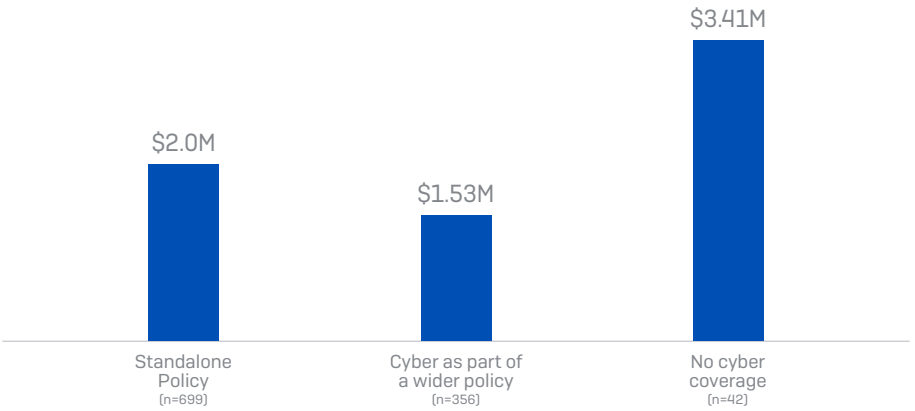
Organizations with coverage are more likely to have data encrypted than those without a policy, however they are less likely to also have data exfiltrated as part of the attack:

- 74% with a standalone policy had data encrypted, with data exfiltrated in 23% of cases (n=1,560)
- 68% with cyber as part of a wider policy had data encrypted, with data exfiltrated in 41% of cases (n=1,127)
- 52% without a cyber policy had data encrypted, with data exfiltrated in 61% of cases (n=284)

Ransom payment amount

Organizations with cyber policies report lower average ransom payment amounts than those without coverage. The median payment by those without cyber coverage came in at $3.41 million, considerably above the $2 million for those with a standalone policy and $1.53 million for those with cyber as part of a wider business policy.

Average ransom payment



How much was the ransom payment that was paid to the attackers? n=1,097 Base numbers in chart

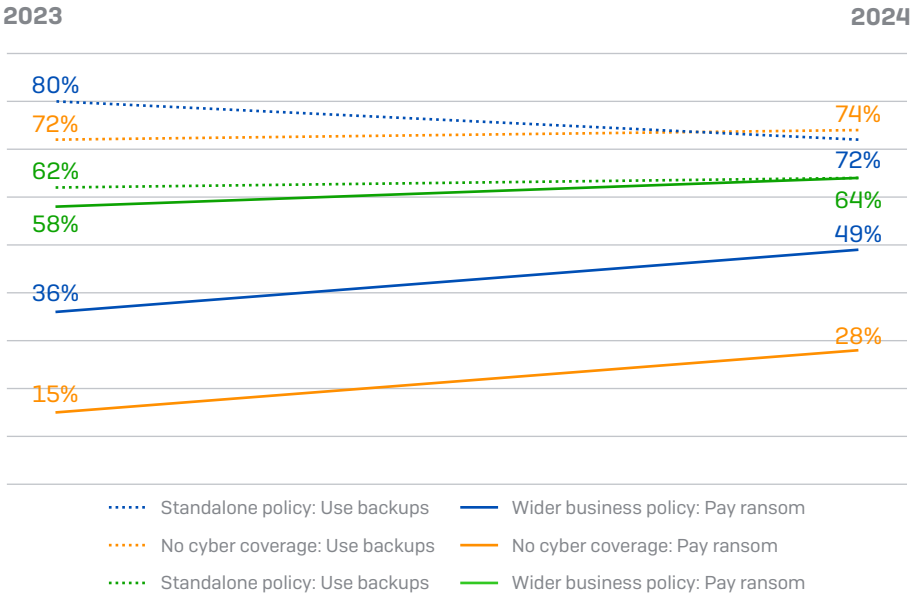
Propensity to pay the ransom to recover encrypted data

The data indicates that having insurance coverage correlates with higher propensity to pay the ransom to get data back. Standalone policy holders report the highest rate of ransom payment, and were more than twice as likely to pay the ransom than those without cyber coverage (64% vs. 28%). They are also the only group that is just as likely to pay the ransom than use backups to recover encrypted data.

Paid the ransom and got data back

64%	49%	28%
with a **standalone policy** (n=744)	with **cyber as part of a wider policy** (n=375)	**without a cyber policy** (n=42)

All three groups reported a greater likelihood of paying the ransom in our 2024 survey vs. 2023, and those with a standalone policy or no cyber coverage also reported increased use of backups to recover encrypted data over the last year.



Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. n=2,072 (2024), 1,497 (2023). Note: respondents could select both options if they deployed multiple methods to recover their data.

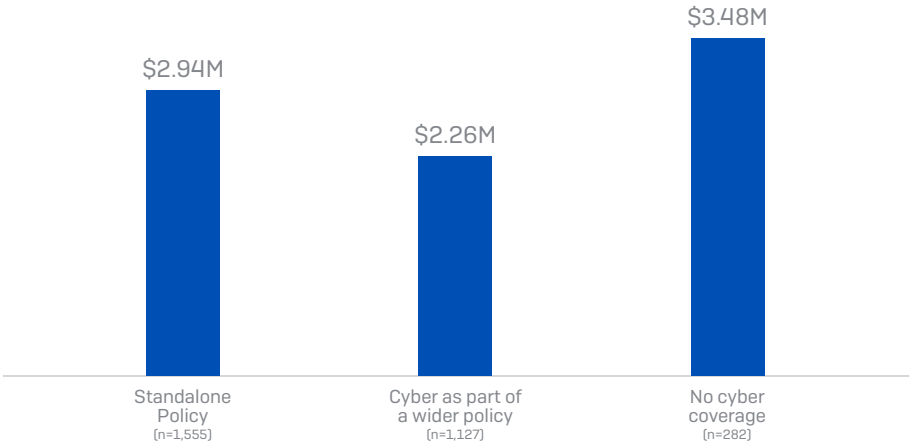
While the data may appear to suggest that cyber insurance — and in particular standalone policies — is driving the payment of ransom, it's important to remember that we do not know whether the insurance policy purchase was before or after the ransom was paid. It may be that the organization chose to purchase a standalone policy after experiencing the financial pain of a ransom payment. Alternatively, insurance policies may be making it more viable for organizations to pay by contributing to the funding.

Overall recovery costs

The ransom payment is just one element of the recovery cost. Independent of whether a ransom was paid, multiple factors contribute to the overall financial impact, including data notification costs, the opportunity cost from being unable to transact, people time, and more.

Across all respondents, the mean estimated cost to recover from the ransomware attack was $2.73M. The data shows that, while all organizations experience a considerable financial hit from the attack, those without insurance coverage incur the biggest bill.

Overall ransomware recovery costs (excluding ransom payment)



What was the approximate cost to your organization to rectify the impacts of the most signiificant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.)? n=2,964 Base numbers in chart

As stated, this analysis should be considered a starting point for further exploration of this area of research. With ransomware experience and cyber insurance coverage common to many organizations, it would be helpful to dive deeper into how having insurance impacts ransomware experiences.

Conclusion

Cyber insurance is now an established pillar in most cyber risk mitigation strategies. It's time to move from siloed solutions to a holistic approach to cyber risk management that takes advantage of the interplay between cyber defenses and cyber insurance. By making smart investments in elevated cyber defenses, businesses can unlock considerable cyber insurance savings while also enjoying wider operational benefits and reduced likelihood of experiencing an attack.

To discuss your cyber defense requirement, speak with a Sophos adviser today or visit www.sophos.com

2024-06-27 (WP-DD)

SOPHOS