SOPHOS
Cybersecurity evolved.

Sophos Guide to Cyber Insurance

How cybersecurity can help reduce premiums and lower risk

The cyber insurance market is changing fast, and conditions are getting tougher as the market hardens for the first time in its 15-plus year history. While most organizations already have some cyber insurance coverage, many are finding the bar for renewal is getting higher as capacity shrinks – and premiums are going up.

Good cybersecurity can help with cyber insurance in multiple ways: from facilitating access to a policy approved through underwriting to lowering premiums and reducing the likelihood of making a claim. This guide provides an overview into the state of the cyber insurance market and explains the different ways that cybersecurity can positively impact your insurance. It also details the Sophos technologies and services that can help you reduce your premiums and lower your risk.

A Sophos Whitepaper. September 2021

The basics

Why have cyber insurance

Cyber insurance, also commonly known as cyber risk insurance and cyber liability insurance, protects you from the impact of cybercrime (though not from the crime itself). Broadly speaking, there are three main benefits to having cyber insurance:

1. **Financial**. The insurance covers costs in the event of a cyber incident
2. **Operational**. The insurance team provides immediate access to experts in the event of an incident, including IT forensics specialists, privacy lawyers, and PR pros
3. **Peace of mind**. Having cyber insurance gives confidence to your customers, partners, suppliers, and employees that you are prepared and covered should a cyber incident strike

While cyber insurance claims can be triggered by a wide range of incidents, the most frequent cause of claims according to NetDiligence's Cyber Claims Study 2020 are four common threats: ransomware, social engineering, hackers, and business email compromise (BEC)*.

What cyber insurance covers

Cyber insurance covers the costs incurred as a result of a cyberattack. While individual policies vary, they typically cover:

- Forensic analysis to identify the attack source
- Ransom demands and specialists to handle ransom negotiations
- Costs to regain access or restore your data from backups or other sources
- Legal costs
- Public relations services
- Notification of clients and/or regulatory bodies
- Credit monitoring services for affected individuals

When sourcing policies and comparing costs, it's worth noting that the costs of business interruption, such as loss of income or additional costs of work due to the cyberattack, are included in some policies, but not others.

In the event of a cyber incident, the insurance provider will step in and provide experts to help deal with the situation. For a ransomware attack, they will typically:

- Appoint a consultant to advise on the handling and negotiation of the ransom demand
- Identify the lowest cost way to restore the data (ransom payment, backups etc.)
- Bring in the necessary experts to deal with the issue

First-party vs. third-party coverage

Many policies include both first- and third-party coverage. **First-party coverage** is direct costs associated with the response to the attack, for example legal fees, forensic fees, customer notification fees, PR fees, and so on. **Third-party coverage** is primarily costs associated with lawsuits.

Within a policy, there may be specific sub-limits for first-party coverage, and even for specific items of first-party coverage. For example, first-party coverage may be limited to $500,000, which includes a limit of $50,000 for PR costs.

* Source: NetDiligence Cyber Claims Study 2020. Data for organizations with less than US$2 billion annual revenue

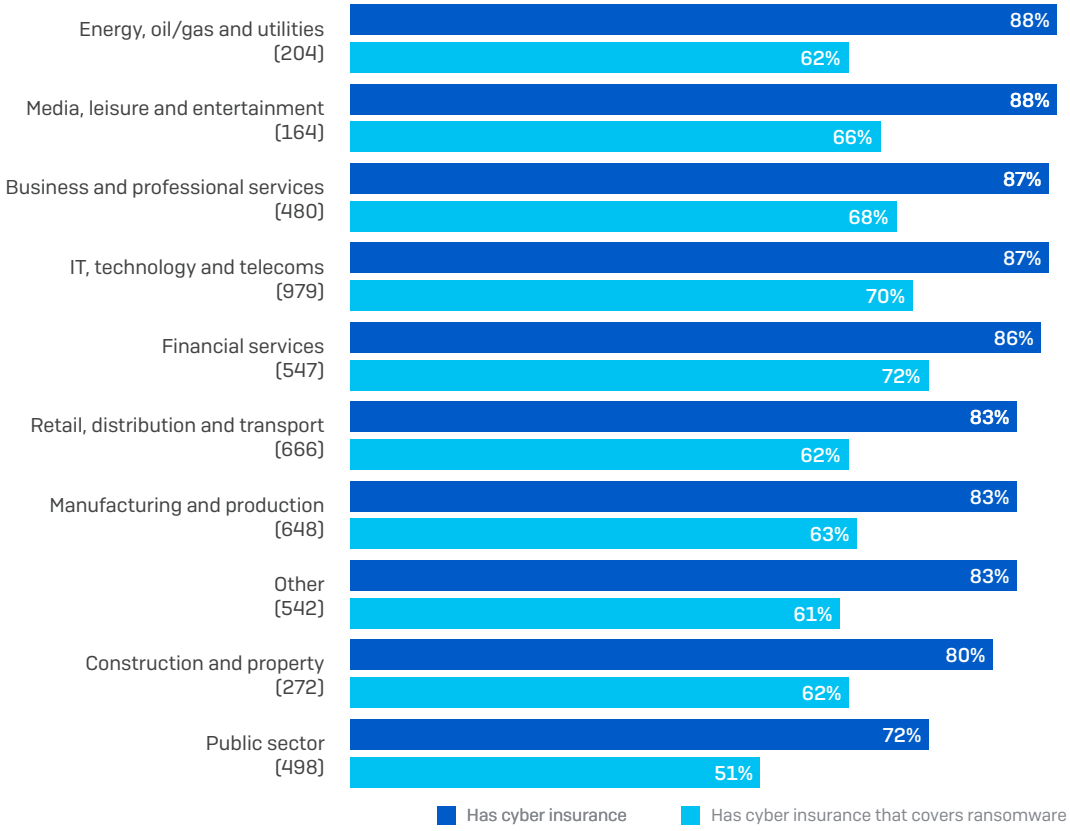
The realities of cyber insurance

The prevalence of cyber insurance

84% of organizations have some form of cyber insurance according to an independent survey of 5,000 IT decision-makers in mid-sized organizations commissioned by Sophos*. Cyber insurance is commonplace across all industries, however the utilities sector, including energy and oil/gas, is most likely to have cyber insurance (88%), alongside media, leisure, and entertainment. This is understandable, given the high impact of a cyberattack on the utilities sector and its extensive use of legacy infrastructure that is often a target for attacks.

Only 64% of organizations surveyed, however, had cyber insurance that covers ransomware, leaving one in five (20%) exposed to the full cost of a ransomware incident despite investing in cyber insurance*. The takeaway here is to make sure that you're fully aware of the details of your policy and what it covers.

Cyber insurance coverage by sector



The public sector is least likely to have both cyber insurance (72%) and insurance against ransomware (52%). This is concerning, as public entities are a frequent target for cyber criminals as well as amongst the least able to defend against a ransomware attack with the Sophos State of Ransomware 2021 report revealing that:

- Education was the sector most likely to have been hit by a ransomware attack in the last year
- Local government was the sector least able to stop attackers encrypting data

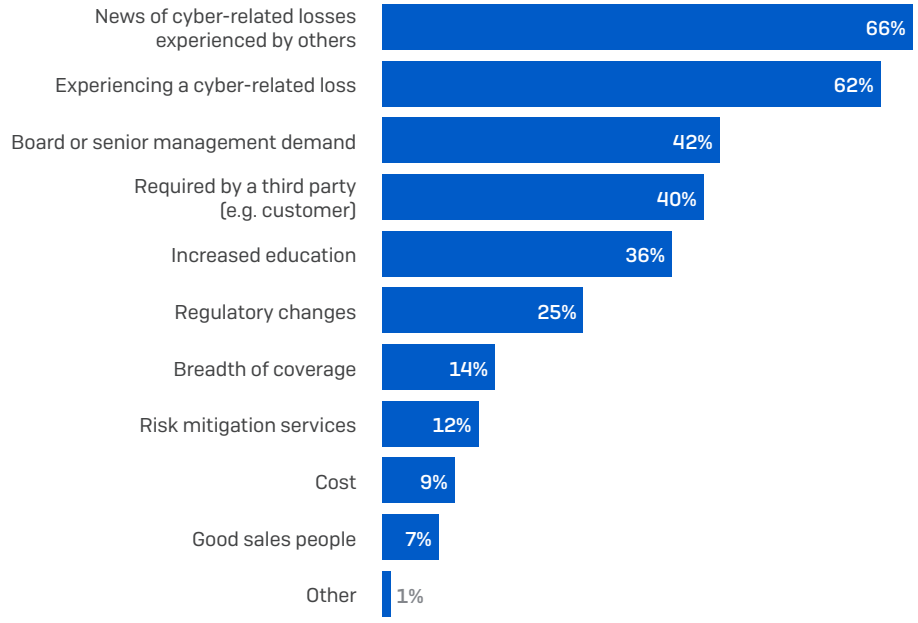
Conversely, financial services is the sector with the highest level of insurance coverage for ransomware (72%) as well as one of the highest overall levels of cyber insurance. This sector, which can be perceived to be a lucrative target for cybercriminals, is leading the way in insurance readiness.

* Source: The State of Ransomware, 2020, Sophos

Cyberattacks are fuelling cyber insurance

A recent survey of cyber insurance brokers and cyber underwriters from around the world by Advisen and Partner Re provides insight into the top drivers of new or increased cyber insurance sales*. It is perhaps unsurprising that the top two factors behind the take up of cyber insurance are *news of cyber-related losses experience by others* and *experiencing a cyber-realated loss*. However, in third place is *board or senior management demand*. This high level of demand from leadership teams reflects the cross-organization devastation that a major cyber incident can cause. Defending against the implications of a cyberattack is now a mainstream business issue, not just an IT challenge.

What do you see as the top driver(s) of new/increased cyber insurance sales? Please select top three:



Source: Cyber Insurance – The Market's View, Advisen – Partner Re, September 2020.

The cost of cyber insurance

As with all other forms of insurance, the cost depends on multiple factors, including:

- **Demographics:** Size, industry, sector, location, revenue etc.
- **Potential exposure**: Type and volume of sensitive data stored/collected/processed
- **Level of cybersecurity**: The security defenses an organization uses
- **History**: Previous claims invariably result in higher premiums
- **Policy terms**: Coverage/liability limit etc.

It is important to be aware of the distinction between deductible and retention policies. With a deductible policy, the deductible (known as 'excess' in some countries) is included in the overall policy limit. Conversely, with a retention policy, the retention amount is in addition to the policy limit.

* Source: Cyber Insurance – The Market's View, Advisen – Partner Re, September 2020. Survey of 260 cyber insurance brokers and 190 cyber underwriters from around the world

DEDUCTIBLE	***RETENTION***
$100K policy limit, $10K deductible (excess) You pay first $10K of claim, insurer pays $90K **Total coverage $100K**	$100K policy limit, $10K retention You pay first $10K of claim, insurer pays $100K **Total coverage $110K**

In the SMB market, it is not uncommon for there to be just a single carrier for cyber insurance. However, in the large enterprise market, cyber insurance towers are common, as one single insurer cannot provide all the necessary risk transfer. Insurance brokers build towers for individual customers, bringing together two, three, four, or more providers. The first provider covers cover the primary risk transfer, with the remainder covering the excess risk transfer.

Insurance panels

Cyber insurance carriers will often have pre-approved vendors/suppliers, called a 'panel', that they work with in the event of an incident. If the company experiencing the incident does not have any existing relationships with vendors/suppliers, the cyber insurance carrier will encourage or even require them to work with one of these 'on-panel' organizations.

That said, most carriers are also open to working with other reputable vendors/suppliers, especially if a pre-existing relationship and/or contractual terms exist. This is referred to as an 'off-panel' approval. Naturally, there are many financial and operational advantages to working with a supplier that already knows the organization experiencing the incident and is familiar with their IT and business set-up.

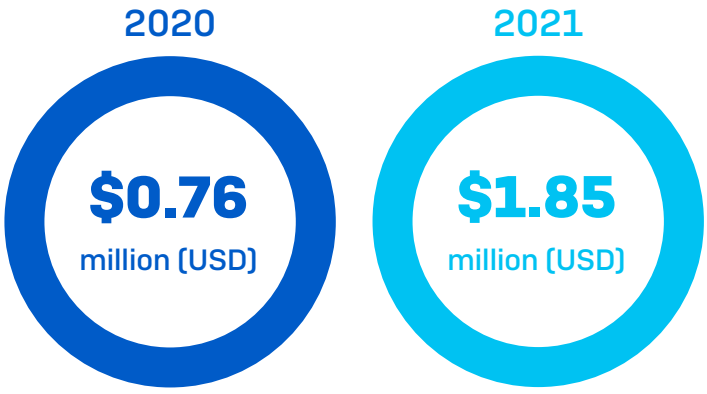
If your preferred supplier is not 'on-panel' with your insurance provider, you can request to use them. Early communication with your insurance provider is paramount so your preferred supplier's cyber insurance team can engage with the insurance provider for the appropriate approvals.

Coverage needs

When selecting a cyber insurance policy, it's important to choose the appropriate level of coverage for your organization. You need to be able to recover successfully and keep your business afloat if you experience a cyberattack – while at the same time keeping your premiums at an affordable level.

The costs to recover from a cyberattack are considerable, and rising. The average ransomware recovery cost for a mid-size organization hit $1.85 million last year, more than double the previous year's figure of $760,000*.

Ransomware recovery cost doubled in last year



This increase is driven in large part by the growing complexity of many cyberattacks. Adversaries are increasingly combining automation and tools with hands-on hacking, leading to far more destructive attacks that are harder to recover from. We should also remember that a large part of the recovery costs is restoring IT systems to the level they should have been before the attack with advanced protection on all devices, not just returning to status quo.

* Source: The State of Ransomware 2021, Sophos

The cyber insurance market

Cyber insurance conditions are getting harder

Cyber insurance has, until now, been a 'soft' market, characterized by high capacity and low premiums. However, for the first time in its 15-plus year history as a standalone policy, the market is starting to harden, as insurers see their payouts rising faster than the income from premiums: the industry's loss ratio has risen for the last three consecutive years, rising to 72.8% in 2020*. (Loss ratio is insurance costs divided by total earned premiums. For example, if a company pays $80 in claims for every $160 in collected premiums, the loss ratio would be 50%.)

A number of factors are driving this hardening of the market:

- Cyberattacks are constantly evolving, making it hard for insurers to assess the true risk of a client being attacked
- The costs to recover from a cyberattack are increasing
- The pandemic and growing use of the cloud have accelerated the interconnectedness of the business environment, increasing exposure

The result of this market hardening is higher premiums, with the cost of standalone policies in the US climbing 28.6% in 2020*. It's also getting harder for many organizations to get insurance in the first place as the underwriting process grows more and more rigorous and overall capacity drops.

"Our cyber insurance is up and we're having to jump through more hoops than we've ever had to before."

Corporate travel company

This hardening of the market creates a particular challenge for public entities, which are often considered to be easy targets for cybercriminals due to their weaker defenses. As a result, public organizations looking to obtain or renew coverage are facing fewer providers and tougher conditions, with prices sometimes doubled year over year.

"Where [insurers] used to offer $10 million in limit, it's now $5 million."

Jack Kudale, CEO, Cowbell Cyber Inc.

Insurance providers pay up

The good news is that cyber insurance invariably delivers if the worst happens and you fall victim to a cyberattack. In Sophos' State of Ransomware 2020 survey, 95% of respondents insured for and hit by ransomware said the insurance provider covered costs resulting from the attack. In over two thirds (69%) of incidents the insurance provider covered the cleanup costs to get the organization back up and running again. In 44% of incidents the insurance paid the ransom, and in 29% it paid other costs such as those incurred for downtime and lost opportunities.

Insurers paid out in 95% of incidents

* Source: S&P Global, June 1, 2021

Good cybersecurity helps with cyber insurance

There is a direct relationship between cybersecurity and cyber insurance, and having strong cyber defenses in place can help in a number of ways:

1. Good cybersecurity makes it easier to get cyber insurance

In light of the challenges facing the cyber insurance market, providers are focusing increasingly on managing – and reducing – risk. Good cybersecurity can help you reduce your cyber risk which, in turn, makes you a more attractive prospect for cyber insurance coverage.

Advanced next-gen protection

Having robust security solutions in place and correctly deployed will reduce your cyber risk. In fact, next-gen protection is fast becoming a pre-requisite to secure cyber coverage, with managed detection and response (MDR) services, endpoint or extended detection and response (EDR/XDR) technologies and next-gen endpoint protection the most common requirements.

"Legal wants to get ransomware insurance and [MTR] is the step we need to get it done."

IT technology and solution provider, global reach

Multi-factor authentication

Multi-factor authentication is now often a requirement to secure coverage as insurers look to close a common security gap before they absorb risk.

"Our cyber insurance renewal is predicated on us enabling MFA for remote access."

IT support and services provider, USA

"I was told that if we don't get MFA within a year, our cyber insurance will be dropped."

Healthcare provider, USA

Incident response plan

A third area to consider is business continuity readiness i.e. how prepared are you for a major cyber incident. The best way to stop a cyberattack from turning into a full breach is to prepare in advance. Often, after an organization experiences a breach, they realize they could have avoided a lot of cost, pain, and disruption if they had had an incident response plan in place. Having a detailed plan that enables you to minimize the impact of an incident will reduce your cyber risk, making you a more attractive prospect to insurance providers.

2. Good cybersecurity helps reduce premiums

Just as an alarm and window locks reduce your home insurance premiums, so having advanced IT defenses helps reduce your cyber insurance costs. While the insurers' exact premium calculation algorithms are a closely-guarded secret, customers consistently say that the quality of their protection impacts their premiums.

"Because we didn't have EDR installed on 100% of our appliances, the insurance [costs] doubled."

Web hosting company, USA

3. Good cybersecurity reduces the likelihood of making a claim – and higher premiums in the future

As with other forms of insurance, if you make a claim, you can expect a significant increase in your premiums in subsequent years. By minimizing your risk of being impacted by a cyberattack you reduce the likelihood that you'll need to call on your policy – and help keep your premiums down.

4. Good cybersecurity reduces the risks of non-payment

Poor IT security hygiene can prevent you receiving financial support in the event of an incident. If the insurer believes that you 'left the door open' through weak practices, they may have grounds to not pay out.

"We do not pay for any claims, losses, breaches, privacy investigations or threats due to the use of outdated or unsupported software or systems."

Hiscox Cyberclear™ policy wording, UK, June 2021

By eliminating these gaps, you can help ensure that, should the worst happen, the insurance company will step in.

5. Good cybersecurity can minimize the impact and cost if an incident occurs

Responding quickly and appropriately to a cyberattack can significantly reduce the impact and cost of the incident. Having a malware incident response plan in place and being able to call on experienced incident responders will help you minimize the fall-out from the attack.

How Sophos can help

Qualify for insurance and keep premiums down

Advanced next-gen protection

Sophos provides the advanced threat protection that is increasingly required to qualify for insurance coverage and keep premiums down – all backed by the threat intelligence and cybersecurity expertise of SophosLabs, Sophos AI, and Sophos SecOps.

- **Sophos Managed Threat Response (MTR)** gives you the ultimate protection, with 24/7 threat hunting, detection, and response delivered by an expert team as a fully-managed service. They have identified and neutralized attacks for thousands of customers around the globe.
- **Sophos Extended Detection and Response (XDR)** enables you to hunt for threats across your environment and neutralize an attack before the damage is done.
- **Sophos Intercept X** gives your endpoints and servers the world's best protection against ransomware. Layered protection stops attackers at multiple points in the attack chain, including:
  - CryptoGuard stops and rolls back the unauthorized encryption of files by ransomware
  - Exploit prevention blocks the techniques adversaries use in their attacks
  - AI-powered deep learning identifies both known and never-before-seen threats

- **Sophos Firewall** secures your network against advanced attacks, keeping your data safe from malicious hackers and ransomware actors.

Multi-factor authentication

Sophos enables you to meet MFA requirements, while also elevating your security.

- **Sophos Central**, the cloud-based management platform for all Sophos next-gen products, enforces MFA, securing access to all your protection solutions.
- **Sophos ZTNA** enables MFA to access your applications from any location**.
- **Sophos Firewall** supports MFA for admin, user portal, and remote access VPN. Sophos Firewall users can also access the firewall management interface via Sophos Central for elevated security.
- **Sophos Cloud Optix** monitors AWS/Azure/GCP accounts for Root user and IAM user access with MFA disabled so you can address and ensure compliance.

Incident response plan

When assessing risk, insurance providers are increasingly asking organizations about their disaster recovery readiness as good preparation can reduce the cost, pain, and disruption of a cyber incident.

The free Sophos Incident Response Guide is based on the real-world experiences of the Sophos Managed Threat Response and Sophos Rapid Response teams, who have tens of thousands of hours of experience when it comes to dealing with cyber attacks. It will help you to:

- **Define the framework for your cybersecurity incident response plan**
- **Learn the 10 main steps your plan should include**
- **Understand the role managed detection and response (MDR) services play in supporting your plan.**

Reduce likelihood of making a claim

Sophos gives you world-leading protection against ransomware, malicious hacking, and other advanced threats. Our solutions help you minimize the risk of experiencing a major cyber incident, reducing the likelihood of needing to make a claim and helping keep premiums down in the future.

Sophos Intercept X Advanced with XDR is the #1 rated endpoint protection:

- Leader in Gartner Magic Quadrant for Endpoint Protection Platforms for 12 consecutive reports
- Best Product Small Business Endpoint – SE Labs
- #1 Malware protection rate – AV comparatives
- #1 Exploit Protection – MRG Effitas

** Currently in EAP. General availability targeted for October 2021

Reduce the risk of non-payment

Sophos XDR makes it easy to identify IT hygiene issues and security gaps that could prevent an insurer paying out, such as the use of outdated software. Armed with this information, you can address issues and help ensure that, should an attack happen, the insurance company will step in.

SOPHOS XDR QUERY TO CHECK WHETHER SOFTWARE IS UP-TO-DATE OR OUTDATED

```
-- VARIABLE $$Version$$   String

--VARIABLE  $$Name$$    String

SELECT name, version, publisher,

CASE

  WHEN version = '$$Version$$' THEN 'Software is up-to-date'

  WHEN version != '$$Version$$' THEN 'Software is outdated'

  ELSE 'Application Not Installed'

END AS Status FROM programs WHERE name = '$$Name$$';
```

Minimize the impact if an incident does occur

If the worst happens and you get hit by a cyberattack, the incident response experts in the **Sophos Rapid Response** service can help you get out of the danger zone fast and minimize the impact and cost of the incident.

Available to Sophos customers and non-customers alike, the Rapid Response Team has helped hundreds of organizations deal with a cyberattack. They also work closely with insurance providers, furnishing carriers with any forensic insights they may need. Where Sophos solutions are already deployed, the speed, efficiency and impact of Rapid Response are elevated even further.

Conclusion

The cyber insurance market is getting tougher as premiums and the bar to get coverage go up. Having good cybersecurity in place will help you reduce the cost of your cyber insurance and minimize the risk of making a claim. It also helps ensure that, should the worst happen, the insurance provider will pay out.

Sophos can help you get the cyber defenses you need to optimize your cyber insurance coverage. To discuss your requirements and how Sophos can help, please reach out to your Sophos representatives or contact cyberinsurance@sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

21-09-22 EN (PS)

SOPHOS