How To Qualify for Cyber Insurance As Claims Skyrocket

More risk means tighter qualifications and higher premiums when it comes to insurance — cyber insurance is no different. The past few years have seen enormous increases in cybercrime and, not surprisingly, skyrocketing claims.

"Policyholders can expect 20% to 50% rate increases for cyber coverage throughout 2021 as trends that began last year continue at an accelerated pace," states a report from Aon, a global insurer. Other research concurs.

Plus, many companies may be surprised to learn their insurer is no longer including cyber coverage in their general business insurance policies. They need to apply and qualify for it separately.

How might this affect your ability to get or afford cyber insurance? And is there anything you can do about it?

Of companies that paid the ransom, only 8% got all of their data back and 29% got half or less of their data back.

Stats driving cyber insurance changes

The pandemic has pushed cybercrime into overdrive, with remote working and digitally transforming without proper risk management being the prime drivers:

- Ransomware attack rates are the highest ever and ransom demands are increasing — Garmin recently paid a $10 million ransom. Sophos found the average cost for recovering from a ransomware attack has more than doubled since last year, averaging $1.85 million in 2021 (so far). Datto found the cost of downtime almost doubled as well, and downtime can cost nearly 50x the ransom demanded.
- Sophos also reported that of companies that paid the ransom, only 8% got all of their data back and 29% got half or less of their data back.
- In 2020, it took an average of 280 days to identify a breach and the average total cost of a data breach was $3.86 million, according to a Ponemon Institute and IBM report. The average savings of containing a breach in under 200 days was $1M.
- Businesses are now spending 21% of their IT budget on cybersecurity — up 63% from 2019, according to Hiscox, a global business insurance provider.
- Cybersecurity Ventures, a leading cybersecurity researcher, estimates cybercrime losses in 2021 will total $6 trillion globally and will continue to grow by 15% per year, reaching $10.5 trillion per year by 2025.

What's more, cybercriminals are getting bolder and adding new tactics.

For example, ransomware attackers are using "name and shame" to coerce companies to pay up even if they can restore from backups to avoid having their sensitive data published online. The FBI issued a warning in March 2021 about malicious actors who are now using deep-fake video and audio scams, and, as the SolarWinds attack proved, nation-states have moved beyond targeting critical infrastructure to focusing 90% of their effort outside the sector, according to Microsoft's Digital Defense Report.

All of these trends are alarming for business leaders. They create both increased risk and an increased need for cyber insurance.

But companies like yours aren't the only ones facing higher risks.

Insurance companies face higher risks, too

You might think that insurance companies see the growing demand for their cyber products as a windfall. They can charge more while growing the line of business.

However, cybersecurity insurance is unlike other insurance in that it's relatively new and not yet well-established or widely adopted by C-suites. Plus, it's unpredictable. This means insurance providers might not have enough money from cybersecurity policyholders to cover just a few major simultaneous incidents. Even with reinsurance, providers' risk is increasing substantially, according to Harvard Business Review.

Companies in industries that face especially high cyber-crime risk — and, therefore, higher insurance risk — include municipalities, healthcare, financial services, higher education, and technology, among others, according to Gallagher research.

The greater risk means that insurance providers offering cyber insurance have to be pickier about who they insure, charge higher premiums to cover the risk, and, potentially, revise what they cover.

Some providers, for example, now only cover ransom paid to ransomware attackers under a separate policy or rider — ransomware attackers know they are more likely to get paid by companies that have cyber insurance, putting ransoms in a different risk category. Other providers are offering lower limits.

The greater risk means that insurance providers offering cyber insurance have to be pickier about who they insure.

How insurance companies are beefing up their approval processes

To determine a company's risk profile, providers look at the company's loss experience, industry, location, individual account specifics, and the security questionnaire. The questionnaire can be complex – asking about the security framework you follow, what you use for intrusion detection and security monitoring, how you manage backups and back-up encryption, how you protect company data on mobile devices, and other details. Your IT department or managed IT provider can answer accurately.

Now insurance companies are going deeper.

To validate the self-reporting, some insurers are conducting penetration tests on your company to see if their experts can get into your system. If they can, the provider may either turn you down, allow you to remediate the problems, or be satisfied if you can provide proof that you're moving toward a more mature cybersecurity posture. The proof might include providing your IT security roadmap, signed proposals for professional services engagements, or a recent risk assessment report.

Some insurers are conducting penetration tests on your company to see if their experts can get into your system.

What you can do to get a good cyber policy and premium

Everything that improves your qualifications for cyber insurance revolves around assuming more responsibility for protecting your IT environment.

The actions range from performing basic IT hygiene and using multi-factor authentication (MFA) — often a policy prerequisite — to upgrading your security policies and procedures to practicing your incident response and disaster recovery plans.

At a minimum, protect and defend your environment:

- Apply the most recent patches and updates to all of your systems as soon as they are available (applications and appliances in addition to Windows)
- Implement Multi Factor Authentication (MFA)
- Replace or retire hardware and software that have reached end of life
- Use data encryption
- Use concise access controls and permissions
- Identify your most critical business information and store it on ransomware-resistant backups
- Train and test your employees
- Use a modern Unified Threat Management (UTM) system for all business users and data

To further reduce your risk, contain and monitor your environment:

- Perform network segmentation and enforce firewall policy-based boundaries within your environment
- Implement the latest security controls for your network, cloud platforms, and endpoints
- Monitor for stolen or compromised credentials
- Proactively look for software and system vulnerabilities
- Require your third-party vendors to meet the same security standards you meet
- Update and practice your Incident Response Plan (IRP)
- Update and practice your Disaster Recovery Plan (DRP)

Finally, consider hiring an external security firm to try to penetrate your network before insurance company experts try.

Other ways to cover potential losses

If you can't find a cyber insurance policy that covers the IT areas you can't currently control and also fits your budget, you have a few options. Consider getting a smaller policy, self-insuring (setting aside money to cover potential incidents), or looking at captive insurance, which is becoming part of a group that creates its own licensed insurance agency with member premiums covering incidents incurred by the group.

Some insurers offer tangible incentives to companies that assume more of their own risk.

The bottom line is clear. The more cyber risk your company can manage through proactive security programs and options that cover at least some of your potential financial loss, the more attractive you are as a cyber insurance client.