CISO ToGo
Technology Risk Consulting

Cyber Insurance Considerations

What is cyber insurance?

Cyber insurance is a type of liability coverage that can help cover the data recovery costs businesses face when dealing with ransomware or similar attacks. Cyber liability insurance also covers court and attorney fees, settlements, and compliance fines should a data breach happen and affect a third party. For software vendors and managed services providers (MSPs), an errors and omissions (E&O) policy covers bugs in an application you provided or mistakes you make in configuring your client's network.

Businesses purchase cyber insurance to offset the costs they face in the aftermath of a cyberattack by moving some of the costs to the insurer in exchange for a recurring fee, typically monthly or quarterly. There are usually several different policy options to choose from, along with add-ons for extra coverage.

The Pros and Cons of Cyber Insurance

As the world continues to become increasingly digitized, businesses can expect to come under continued threat from cyber-attacks. For many firms, cyber insurance can provide a much-needed shield against this danger.

Cyber-attacks are the new normal, so many CEOs are looking for ways to protect their businesses from emerging risks. From large corporations to small businesses, everyone is a potential target for hackers. As a result of the risks to revenue and business, cyber insurance has become a necessity, and should be considered another "cost of doing business". The prospect of getting money back after an attack becomes increasingly appealing.

New World Realities

A Sophos survey found that 84% of its 5,000 respondents have a cyber insurance policy. This service is sometimes also called cyber-liability insurance. Additionally, a report by cyber insurance provider Zurich North America and Advisen Ltd. found that the specific risks managers want to insure against include:

- Bricking (when a cyberattack renders a device unusable) – 72%
- Contingent business interruption – 72%
- System failure – 70%
- Funds transfer fraud – 66%
- Social engineering – 66%
- Internet media liability – 63%
- Reputational harm – 60%

What Does Cyber Insurance Typically Cover?

In no particular order of importance, cyber insurance covers the following:

1. **Media Liability**

   Advertising your services can result in intellectual property infringement. Cyber insurance covers its consequences (patent infringement not included). Do note that it covers both online and offline forms of advertising.

2. **Network Security**

   With information and privacy risks abound, you need to keep your bases covered against network security failure. It includes malware infection, business email compromise, cyber extortion demand, and ransomware. Cyber insurance covers against malware infection, business email compromise, cyber extortion demand, and ransomware. If you have cyber insurance, you can recover first-party costs related to:

   - IT forensics
   - data restoration
   - legal expenses
   - notifying your customers of the breach
   - public relations
   - identity restoration

3. **Errors and Omissions**

   If a cyber-attack impacts your organization, you could find yourself no longer able to fulfill your contractual obligations, leaving your customers hanging. Once there is a cyber incident, all your time and energy go toward addressing its repercussions and minimizing the damage ... therefore, you won't likely have the resources to focus on consulting, upkeep, and other services. Since your customers may not be as understanding as you'd like them to be, it makes sense to protect yourself by investing in cyber insurance.

4. **Network Business Interruption**

   Modern businesses tend to rely on advanced technology to remain operational. In the event of an incident, some form of interruption is imminent. For instance, if your provider's network goes down, you can't recover expenses sustained as a result and lose profits as well. Think of system failures, unstable system patches, security failures, human error, and more.

5. **Privacy Liability**

   When a breach happens, it can expose the sensitive data of your customers that lies on your servers. As a result, your business could be held liable – and a class-action lawsuit will certainly result in legal fees to cover. Regulatory fines resulting from the likes of GDPR (and a growing list of others) are another threat. It could bring your company to its knees. Without insurance, you could find yourself closing down the doors for good.

What is Left Out?

As comprehensive as it may be, do bear in mind that cyber insurance does not cover everything. For instance, losing value due to theft is not part of it. Nor does it cover the loss of potential profits in the future. It also doesn't allow you to improve your existing internal technology systems or amass the funds to make security upgrades.

The Advantages of Cyber Insurance *(summary)*

- **Improved standard of security ... t**he work done by insurance companies could improve and redefine security standards.
- **Financial incentives to improve IT security ...** better insurance coverage at lower rates could become a possibility.
- **Greater executive awareness ...** recognizing the scope of cyber risks and the severity of their consequences could pave the way for much-needed security initiatives.

The Disadvantages of Cyber Insurance *(summary)*

- **Smaller companies could stay behind ...** if a business operates with a more modest budget, they may not have the funds necessary for insurance; therefore, compared to large corporations, they will have a disadvantage as a result.
- **Increased burden of legislation ...** lawmakers are not IT or cybersecurity experts; therefore, their moves may not be accurate in addressing the risks involved.
- **A false sense of security ...** after insuring themselves, businesses must ensure that they continue to put in enough effort into developing appropriate policies and procedure, and to continue their investment in maturing their security program.

Why Cyber Insurance Is "Worth It"

As cyber-attacks grow in frequency and complexity, many businesses are asking, "*Is Cyber Insurance worth it?*" The short answer is a resounding "yes"! Consider this: Ransomware-related data breaches doubled in both 2020 and 2021, yielding a record number of data compromises.

Compromised data can cost companies dearly. The ransoms, lost business, system restorations, and third-party notification expenses (among other costs) associated with such incidents add up. Without data breach insurance, businesses often find themselves 'on the hook' for more than they can afford.

In 2021, the average total cost of a data breach rose to $4.24 million, up from $3.86 million in 2020. In response to these rising costs, a new industry has emerged: cyber insurance. While there are benefits to purchasing cyber insurance, the product is mostly new and untested, leaving many variables for the buyer. So, is cyber insurance worth it, and is it right for your business?

When considering whether you should purchase cyber insurance coverage, however, more than "the short answer" is required. An informed decision regarding purchasing and maintaining cyber insurance requires an understanding of how much a data breach really costs, who it's most likely to affect, and what help cyber insurance provides.

Who Needs Cyber Security Insurance in Today's Marketplace?

Any business using the internet or computers – big, small, or in-between – can benefit from cyber insurance. A business is vulnerable to cyberattacks whenever it:

- Accepts payments online.
- Accepts in-store credit card transactions.
- Communicates with customers online or via voice over internet protocol (VoIP).
- Stores personal information electronically.
- Transfers documents electronically.
- Would be harmed from ransomware and a business interruption event

While virtually all modern enterprises are at risk, understanding what data breaches can cost small and medium-sized businesses (SMBs) is particularly important. Cyber criminals often prefer to target SMBs. They think SMBs are less prepared and more vulnerable.

And they are usually correct! A majority of small business owners (56%) are "unconcerned" about cyberattacks, the CNBC | Momentive Q3 Small Business Survey found. A scant 28% have cyber incident response plans in place. Yet, per a 2020 report from automation company ConnectWise, 55% of SMBs have experienced a cyberattack.

Transnational cybersecurity corporation Kaspersky Lab breaks down the cost of cyber incidents to SMBs. Viruses and malware cost an average of $68,000. Targeted attacks cost $188,000. Some other cyber incidents and their latent cost to SMBs include:

- Loss of devices containing sensitive data – $83,000
- Misuse of IT resources by employees – $79,000
- Loss of business – $21,000
- Hiring of external cyber experts – $21,000

Third party exposure presents a particular problem for businesses. Transferring services to a third party doesn't transfer liability. Companies without cyber security insurance coverage often pay the price when one of their vendors is attacked.

Even businesses not handling sensitive information remain at risk. Cyber criminals often don't care what kind of information a company has, especially when they target SMBs. Motivated by financial gain, hackers can hold a network hostage or demand payment in exchange for restored access to vital company records, no matter the kind of data involved.

A ransom payment can be significant, but so are the lost revenue and other costs associated with a data breach. The costs of dealing with a cyber-attack can keep mounting long after the incident occurs. And companies without data breach insurance must pay all these expenses out of pocket.

Finally, organizations that are interested in being seen as "attractive" candidates for acquisition, should expect that common due diligence by a prospective interested party will most certainly include an evaluation of cyber security maturity ... a component of which considers whether cyber insurance is in place.

How Cyber Insurance Coverage Can Help

What cyber liability insurance costs is a small price to pay for coverage that comes with experts ready to help the moment a data breach or other cyber-attack happens.

Cyber Insurance goes a long way toward ensuring a business can survive the financial costs of a data breach. Competitive policies include preventative measures to protect businesses from a breach, and incident response measures in the event a breach occurs.

Data breach insurance often saves businesses more than they expect. Several factors identified in an IBM-sponsored study from the Ponemon Institute can reduce the average cost to business per stolen record (which is identified as $148.00):

- Incident response team – $14.00 reduction
- Employee training – $9.30 reduction
- Security analytics – $6.90 reduction

A comprehensive cyber insurance policy includes all these elements. According to the study mentioned above, simply having cyber insurance in itself reduces the cost per record by nearly $2.00!

Cyber Insurance Is Not The Same As Security

Apart from cases where cyber insurance is obligatory, is it worth investing in on its own merits? There is a place for good cyber insurance in the mix of insurance cover a business may require. Like all insurance, though, there is good and bad.

Ultimate responsibility for data breaches rests with the board and the CEO, however ... and insurers know this. The insurer's position will be that it is a significant business risk not to have cover if a breach happens.

While this is true, but the danger is, some companies could think a cyber risk policy by itself is enough. However, this approach treats security as a tick-the-box exercise. Insurance cover should never be a substitute for making an investment in the appropriate security controls for your business, based around technology, people and processes.

What to do before choosing an insurer

Before deciding which insurance provider to work with, a useful first step is to carry out an internal risk assessment. Depending on the level of security and risk management expertise in the business, this exercise might involve an external provider to carry out the assessment.

At the end of this process, the business will have playbooks outlining how different types of security incidents could affect its operations. Depending on the severity, a serious breach could lead to a few weeks' downtime. In that case, then a cyber insurance policy might help to cover the loss of revenue as well as the cost to put the business continuity plan into action such as spinning up new servers to replace the ones affected by the breach.

Of course, there's always small print

Some policies, for instance, exclude claims for extortion and fraud, which rules out payouts for ransomware attacks and invoice re-direct scams – yet these are two of the most common forms of security breach.

In a specific example, Merck & Co. (the multinational pharmaceutical company) sued its cyber insurer providers (Allianz and Zurich Insurance Group) who had denied coverage for the impact of the 2017 NotPetya malware attack on Merck's computer systems ($1.4B in losses), citing a policy exclusion for acts of war, as the malware attack was attributed to Russia's military intelligence agency, deployed as part of a conflict with Ukraine. The New Jersey Superior Court, however, has ruled that the insurers can't claim the war exclusion because its language is meant to apply to armed conflict. The ruling noted that insurers didn't change the war language to put companies like Merck "on notice" that cyberattacks wouldn't be covered, despite a trend of attacks by countries like Russia hitting private sector companies.

So ... be sure to read the small print!

Questions to ask your insurer

If you do decide to take out a cyber risk policy, do some due diligence of potential insurers first. Use the following questions as a guide:

- Will the insurance company expect you to pay a ransom if you suffer a ransomware attack?
- If so, would this be acceptable to your board of directors?
    - For obvious reasons, law enforcement bodies oppose the paying ransoms for decrypting data and systems, because it funds criminality.
- How does the insurance company assess a claim, using what metrics?
- How many claims has it rejected and why?
- What types of breaches does it not cover?
- What security measures will the insurance company ask you to have?

The first point hints at the tense relationship between cyber insurance and ransomware. The insurance provider Hiscox found that just over 58 per cent of its customers pay. A separate study for Marsh McLennan, a cyber insurance broker, arrived at a similar figure of 60 per cent for its clients in North America. But even where victims pay, there's no guarantee they will get all their data back. In a global survey by Sophos, those that paid only recovered 65 per cent of their data. In 29 per cent of cases, half the data remained inaccessible even after handing over money.

The final point is an important one. Just like having a "kill switch" and alarm on your car can reduce your automobile insurance premium, your cyber insurance provider may well ask you what extra security checks you have implemented. Your organization may be deemed to be at risk from phishing attacks (for instance), so the insurance company may require that you carry out annual awareness training and simulated phishing exercises. Coverage tends to be the strongest when there is due diligence on both sides.

Conclusion

The business value of good cybersecurity practices is high and growing, even more so in finance, health care and other fields where the risks and costs of attacks are high. It's also true that the shift toward working from home in 2020 and now 2021 has changed the landscape in ways nobody predicted.

Cyber insurance remains an important consideration for every executive. While it's important to balance cost and need against benefits, the more an organization depends on technology, the greater the role and consideration of cyber insurance.

Small businesses and startups may not be able to justify the expense of cyber insurance, especially if they don't yet have a large portfolio or many digital assets. However, mid-sized and large enterprises that carry a lot of PII or financial information for their customers should invest in cyber insurance to protect themselves against legal and recovery expenses in the case of a breach. Because of the high costs associated with cyberattacks, a single breach could cause some businesses to go bankrupt unless they have cyber liability coverage.

Assessing business risks lies on the shoulders of senior executives. But the verdict is pretty clear ... **good cyber insurance is the best policy!**

Questions?

Reach out today, to discuss exactly how we can help:

www.CISO-ToGo.com

Providing services and support throughout the United States

Email: WRichmond@CISO-ToGo.com

Phone: **401-264-0880**

CISO ToGo
Technology Risk Consulting

because security is everyone's concern ... but it's OUR business!

ADDENDUM

A Few Cyber insurance Providers To Consider

The following cyber insurance providers offer flexible options for coverage and include add-ons that increase protection:

AIG

AIG offers standalone cybersecurity policies as well as the option to add cyber insurance to an existing commercial property insurance policy, which is great for businesses that already use AIG. The claims hotline is available 24/7 and provides access to a variety of relevant vendors including forensic investigators and recovery experts. AIG also provides preventative services, including phishing training and simulation, infrastructure vulnerability scans, and risk consulting options.

AXA XL

AXA XL accounts for about 10% of the current cyber insurance market. It offers a full suite of first- and third-party coverage, from cyber security breach expenses and privacy regulatory coverage to cyber extortion & ransomware coverage and business interruption coverages. Coverage is tailored for businesses across various industries and technology companies, available on a primary and excess basis. Its claims team are all attorneys with years of cyber incident response experience. They sit right alongside underwriters so they have a good understanding of clients and coverage before any incident occurs.

Chubb

Chubb offers standalone cyber insurance and an enterprise risk management solution that includes a cyber insurance policy, so you can get the coverage that meets the requirements of your industry or product. The policies are flexible, and you can choose which coverage to add to keep your business safe while staying within your budget. Chubb also offers other business insurance policies, allowing businesses to keep all of their policies under the same umbrella. The insurance also includes risk consulting to help you identify vulnerabilities and protect your business.