Business Owners, Do You Know What Cyber Insurance Covers (and Why You Need It)?

Reasons to hack your business can range from proving it's possible to acquiring a ransom. The dark web is rife with sensitive data for sale, including Social Insurance numbers and company trade secrets. It's also a place to score malware starter kits or ways to exploit vulnerable code. While many known hacks are reported, it's difficult to quantify how many go unnoticed.

Smaller businesses often believe they fly safely under the radar when it comes to data protection and risk management. But the statistics show that small and midsize businesses are the most vulnerable to cyberattacks *because* they're smaller and easier targets. Other businesses assume their data isn't attractive to hackers since they don't track Social Insurance numbers or store credit card data. This is also an

incorrect assumption. In the cyber underworld, any data is valuable, and it's often used to design more intelligent (and profitable) social engineering scams.

One thing's for sure: Cyber liability insurance is a necessary part of risk management and shouldn't be viewed as merely an option.

What does cyber liability insurance cover?

Some insurance companies distinguish between cyber liability and data breach insurance. Usually, the difference has to do with the size of the business, if there's any difference at all. "Cyber liability" is generally a term used for larger companies, and "data breach" is often used for small and midsize companies. Cyber liability and data breach insurance aren't standardized the way property and auto policies are. Most cyber insurance uses a customized approach to coverage, or a collection of endorsements tailored to your coverage needs.

Cyber liability insurance often covers costs relating to:

- Lost income caused by cyberattacks
- Customer notification of data breaches
- Reputational damage and public relations support
- Legal defense related to breaches
- Civil damages and settlement awards
- Repairing damage to computer systems and networks
- Free credit monitoring for affected customers
- Recovering encrypted data
- Cyber extortion and ransom demands, as well as ransom negotiations
- Provincial and federal fines and penalties
- Extortions paid to recover locked files in ransomware attacks
- Computer fraud
- Loss of transferred funds
- Loss of revenue and business interruptions due to cyberattacks
- Dependent business interruption system failures
- System failures of outsourced providers
- Strengthening and improving your system to make it more resistant to future breaches (This may be called "betterments" coverage.)

Your broker will help you identify your unique risks and find a cyber liability policy that fits your needs and budget.

Keep in mind that most of these coverages exclude employees and contractors. (For that, you'll need employee theft coverage.)

Your broker can help with the moving parts

Cyber liability insurance responds to many interrelated moving parts, and the policies themselves can get just as complicated.

But how do you know what you need to cover if you're unclear on the exposure and terminology?

Coverage to ask your broker about

Many cyber insurance policies are a mix and match of coverages based on specific risks (aka a per-insuring agreement). Your broker can help you insure the gaps in your cybersecurity plan by:

- Taking time to understand your business operations and data liability
- Narrowing down the type of cyber coverage that works best for your risk areas
- Explaining the cyber questionnaire required by the insurance company
- Matching you with the best cyber policy for your risk level
- Presenting you with a quote to fit your budget
- Explaining the details of the coverage and answering any questions you may have

Below are some common cyber policy options. Check with your broker about the ones that are included in your general policy and the ones you'll need to add on.

Cyber liability coverage option:	**What it's for:**
Forensic investigations	Costs related to computer forensic analysis. Forensics can reconstruct how a data breach occuis completedrred, identify the stolen data and assist with restoration. (Data reconstruction might also be a separate endorsement, so check with your broker.)
Litigation (defense) expenses	Defense costs related to the data breach. Check the limits and the wording on this one. Legal bills might exhaust your coverage before your claim is completed. You might want to get excess or umbrella coverage.
Regulatory defense expenses or fines	Expenses associated with provincial or federal laws. You might have to defend yourself in civil court and pay fines or penalties for noncompliance with existing data protection rules (like the Personal Information Protection and Electronic Documents Act).

Cyber event response coaching	Proactive consultation. Depending on the policy, you might get free, proactive advice from a data response coach (usually a lawyer) on compliance and security to prevent a breach. Check with your broker about this valuable coverage.
Crisis management or reputational damage	Public relations and customer notification. You'll incur costs to notify customers about the breach. You'll also have to pay for free credit monitoring services and release statements about how you're handling the incident and the steps you're taking to prevent a future breach. You'll probably need a company to do these things for you. (Some policies have a complimentary service, while others reimburse your expenses.)
Business interruption and losses	Lost business due to a security breach. If a malignant hacker takes down your website or ordering system, your clients and vendors won't be able to do business with you. Depending on the hack, you could lose weeks of revenue while restoring your systems.
Cyber extortion or ransom demand	Negotiations. If a nefarious hacker locks you out of your network and encrypts your data, you'll need help negotiating the demands. (Think about losing the use of your email, client resource manager, website, e-commerce, proprietary data, ordering systems, fleet tracking or GPS.)
Betterments	Upgrade after an attack. A betterments endorsement can help offset the cost of replacing hardware or software after a covered data breach. After the attack, you'll probably need the upgrades to correct any vulnerabilities. You might even be required to make the upgrades as part of your claim settlement.
Post-breach first party	Helps when your system is breached. It can help with data restoration, client notification and forensic analysis (for proof of the attack and how it happened).
Post-breach third party	Helps when your client's system is breached and they sue you for it. It can help with legal defense costs or forensic analysis to prove (hopefully!) you weren't the weak link that caused the breach. It's an asset to freelancers and businesses working inside their clients' systems.

Extended reporting period (ERP)	Extends the dates of coverage for reported claims. An ERP allows you to extend the dates your insurance coverage will respond to a claim. It can be useful if you think you might have a claim reported against you after your policy has ended.
Claims-made basis	Claims are covered only if the claim is reported within the policy dates. A claims-made policy covers claims reported during the policy period or within the ERP. Check the declarations page of your policy for coverage dates and extensions.
Per-occurrence basis	Claims are covered based on the date of the event. Per occurrence covers incidents that occur during the active policy dates, even if they're reported years later. It's unusual for a cyber policy to be on a per-occurrence basis.
Defense within limits	Legal defense costs and retainer fees are applied to the policy limits and reduce the overall funds available for coverage. If you have $750,000 in cyber liability coverage and spend $650,000 on legal costs, you'll only have $100,000 left for future expenses (like settlement fees, credit monitoring, fines or data recovery). Ask about separating defense costs from the rest of your cyber policy or an umbrella or excess insurance policy.

A word on risk management

If it sounds like coverage could be expensive, don't cash in your cyber chips. Price isn't the best way to determine if an insurance policy covers your needs. Your risk management plan should also include an insurance strategy identifying:

- Your risk areas
- How much risk you have in those areas
- How much risk you can afford to pay out of pocket
- How much risk to transfer to an insurance company

A good insurance package (and a good broker) will work to cover the expenses you can't afford and make you whole after you've suffered a loss or liability. Cyber liability insurance is no different. It can play a big role in bridging the gaps left by other policies.

Layering your liability risk gaps

Here are a few scenarios where cyber insurance doesn't apply.

Professional liability

Cyber insurance does not automatically include professional liability (also known as E&O) coverage. This is especially important to be aware of if you're a technology services provider or technology consultant.

A client could sue you if you build a website that's breached or recommended a technology that ends up being the root cause of their data breach. These services and recommendations would fall under your technology E&O policy. If you provide technology services, ask your broker to add a technology E&O rider to your cyber policy.

Media liability

If you're a publisher, a marketer, an author, a freelancer, broadcaster, a journalist, an influencer or another media personality, you could be sued for your creations or opinions. For example, you could be sued for publishing something offensive. In this case, media liability insurance would likely respond.

But here's an exception: Imagine one of your social media accounts is hacked, and the imposter publishes offensive information. If you're sued, cyber liability insurance might be the better response. Of course, you'll need a forensic analyst to retrace the hacker's (cyber) steps to prove that the account was compromised and no longer in your control at the time of the post for cyber liability to kick in.

Stolen computer equipment

Even though cyber liability has to do with computers, it doesn't cover all losses related to computers. Let's say your business experiences a smash and grab, and your laptops are stolen. Commercial property will respond to the call. Property coverage will cover the cost to replace the laptops, but it won't cover the data that went along with it. If personal data was housed on stolen laptops, you might have multiple claims (and multiple liabilities).

Can property theft get worse? It sure can.

Property theft is always worse when data is involved. If your stolen laptops result in a client data breach and you fail to notify your clients about it, you'll probably get sued and fined for failure to comply with data breach notification laws.

If you get that far in the legal process, you'll almost certainly be required to provide free credit monitoring to any affected clients. You could also be forced to remediate your network before you're allowed to resume business. In this scenario, you'll need commercial property coverage (to replace the laptops) and cyber liability (for the initial data breach, legal defense and regulatory fines). And you'll need some add-ons like cyber business interruption and betterments. As mentioned above, cyber business interruption covers lost business revenue while you remediate your computer systems, and betterments covers required improvements to your network, including updated laptops.

And if the compromised client data happens to be credit card information, you might be on the hook for payment card industry (PCI) replacement fees. Let's say your breach involved 2,000 clients whose cards had to be reissued for a fee of $10 per card. You'd be liable for $20,000 and possibly additional penalties for failing to follow PCI security standards. A PCI fines and penalties endorsement would help with the costs.

If this all seems very convoluted, it is. But that's when you can lean on your trusted broker for advice.

Exclusions indicate the value of your coverage

One way to assess the value of a cyber insurance policy is to flip to the exclusions page, since exclusions could easily result in a denied claim. Here are a few notable ones to ask about:

Failure to maintain your cybersecurity

The "failure to maintain" clause means you must maintain your cybersecurity protocols at the same levels as (or better than) what you indicated on your cyber liability questionnaire. If you fail to do so, your claim will be denied due to negligence or failure to maintain. This exclusion can feel like a double-whammy attack. You have data breach coverage, but not really.

To avoid this situation, make sure you understand your minimum cybersecurity requirements. Some minimums are based on how you answer the initial cybersecurity questionnaire. So it's best to be truthful, even if it means paying a higher premium or retooling your network security program. (Some cyber liability policies offer proactive security tools, tips, training and ethical hacker services. Ask your broker about these options.)

Cyber liability aggregate limit

The amount listed is the maximum the insurance company will pay during your policy period. If you have two unrelated data breaches within the same policy period, your coverage will only go as far as the limit listed for both incidents. Once you hit that limit, your coverage stops (regardless of where you are in the claims process). If it's a shared limit, all losses (legal defense, credit monitoring, fines and penalties, settlements and data restoration) are bundled together in the same pool of funds.

Fraud and criminal or dishonest acts

If one of your employees, contractors, vendors or volunteers hacks your system or causes a data breach, you might not be covered for the claim. Check the exclusions for a dishonest acts clause. Ask your broker about getting employee crime insurance (or a fidelity bond) to cover those you employ or contract.

Intellectual property

Unlike client data, your business's intellectual property may not be covered if stolen in a data breach. You'll need to check your commercial liability or, better yet, get separate intellectual property insurance.

Notification costs and monitoring

Canada and Quebec have laws requiring businesses to notify their clients when personal information gets exposed as part of a cyberattack. Personal information is typically considered a person's name in combination with other private information (not lawfully publicly available) like their Social Insurance number, driver's license number, credit card numbers, account numbers and security codes or biometric data.

Businesses that collect data on their clients are responsible for that data. They must notify their clients if a system is breached, even if they use a third party to store client data.

For example, say you hire a vendor to manage client account information hosted through your website. On that site, clients can input data, including credit card information. The vendor experiences a data breach. Your client data is exposed. All data collectors are legally required to notify their clients about malicious data hacks. Since you collect data as part of your service, you'll need to tell your clients even though it was the vendor that got hacked.

Ask your broker if privacy breach response costs, notification expenses and credit monitoring expenses coverage are included in the policy or if you need an endorsement. Also verify the type of incident it covers: first party (you) or third party (vendors and others). Third-party coverage normally comes with an added cost and it might not be right for you. Either way, vendors you use to store client data should have their own cyber liability coverage. Ask your vendors for a copy of their cyber certificate of insurance so you can understand your liability exposure.

Your cyber risk overview

Cyber insurance policies aren't very standardized. Even the terminology differs, which can be confusing. You'll need to rely on a skilled insurance broker to match you with the best policy for your needs. They'll help you decipher the complicated networks of cyber liability insurance and lock in plan options appropriate for your business's risk levels.

For starters, you'll need to evaluate a few things about your business, such as:

- Your risk exposure and liability (data storage, computers, network security, training, employees, etc.)
- The type of cyber coverage you need to transfer your liability risk (to the insurance company)
- The amount of money you can afford to pay out of pocket if you experience a data event (before your insurance kicks in)
- Compliance issues specific to your business (privacy laws)
- How much help you'll need to maintain your data security management program (or start one)

Your insurance broker will start the process by giving you a cyber liability indication questionnaire. Be as truthful and thorough as possible in your responses. If you misrepresent the type of data your business collects, your claims history or your data or network security systems, it could mean a claim denial in the future. And a denial isn't worth getting cheaper coverage.

Types of data breaches you could be liable for

Hackers are constantly innovating their methods and skills, so it takes vigilance to keep pace with their creativity and use of technology. And once hacked, your business is an easier target for future breaches. Here are a few types of cyberattacks currently in use:

- **A denial-of-service (DoS) attack** overwhelms a website with requests from a computer (spamming IP servers, endlessly clicking ads or sending webform requests at super-fast or super-slow rates) so clients can't get through. If your business relies on a client-facing website or network that's critical to operations, this could be a disaster. And if the DoS isn't enough, there's also the distributed denial-of-service (DDoS) attack, which is like a DoS but executed simultaneously by a whole network of computers. Frightening, but effective.
- **Malware** is software designed to perform malicious tasks. Viruses, ransomware, spyware, adware, Trojans, rootkits and other intentionally harmful software can infect and disrupt a single device or thousands of them, depending on the intent. Some malware is obvious, attacking soon after installation; it makes itself known. Other malware is less obvious, silently infiltrating a device; it waits for instructions to attack. These silent malware-infected devices are bots that collectively make up a botnet. A bot herder controls the botnet, giving instructions to activate the bots to perform tasks (like spamming or a DDoS). If it sounds very "Manchurian Candidate," that's because it is.
- **Ransomware** is part of the malware family, but it's worth mentioning by name since it's gotten a lot of press. The familiar story is this: A hacker gains control of a company's network (using a phishing scheme or vulnerable device) and encrypts the network data, making it inaccessible. Data can be anything that a company relies on to get business done, such as client management systems, patient hospital records or e-commerce order management systems. Other times the data is sensitive information that could ruin an organization's image if exposed. The virus code usually contains the ransom demands and instructions for payment. If the ransom demands aren't met, the hijacked data is destroyed, released to the public or placed on the dark web. That's just plain scary.
- **Social engineering** is how malicious hackers trick you into giving up private information. Phishing and spoofing scams using emails, texts, messenger apps or phone calls are a form of social engineering that can look and feel like legitimate requests from people and websites you trust. Your website or social media profiles can be used as exploitation tools. "About Us" webpages and social media sites contain a lot of information to build a social engineering scam. Educate your employees about how cyberattacks happen and how hackers glean information to sound convincing.
- **Phishing, spear-phishing and whaling** exploit your trust so you'll click links or give up sensitive information. The request might come from a bank asking for your login information (phishing) or an urgent request from the accounting department about your deleted payroll account (spear-phishing). You might be a CEO receiving a notice about a time-sensitive subpoena requiring you to click on the attachment. These scams are simple, compelling and effective.

- **A brute force attack** does kind of what it sounds like: It keeps banging down the password door until it gets in. A brute force attack will always work (given enough time) because it tries every available character combination. Once inside, the attacker can create more sophisticated scams to access the broader network. That's why secure, randomized passwords and encryption keys remain an excellent (and easy) part of a security plan. According to the technology security company Cloudflare, it takes a password-cracking program one second to crack a five-character password, about four days to break a nine-character password and 359,000 years to crack a 13-character password. As the availability of quantum computing expands, these numbers will decrease. But for now, the benefits of a strong password and encryption are apparent.
- **Credit card skimming** is a popular way to steal a credit card without even touching it. The data thief inserts a device on a card reader to capture the magnetic strip whenever a card is swiped. If your business uses credit card terminals, you'll need to make sure you're covered for a data breach. This one's interesting because it could involve a claim against an employee (if they were in on the skim), which can mean exclusions for part or all of the claim. You'll need employee crime or fidelity (aka dishonest acts) coverage for breaches involving employees. If you accept payments online, you should also ask your lawyer about PCI data security standard (DSS) compliance. Most credit card companies have a PCI DSS page on their website dedicated to helping merchants stay compliant with these standards.
- **Digital skimming** (aka web skimming or Magecart attack) targets e-commerce sites by injecting malicious code on payment and checkout pages. Customers input their financial information, while the malicious code captures the data in real time and sends a copy to the hackers. The payment processes like a typical transaction, so the code can go undetected. Digital skimming made headlines in 2018 when British Airways discovered the code on its website, but only after it exposed the details of over 500,000 clients. According to BBC News, British Airlines faced a record £183 million ($243 million) penalty from the Information Commissioner's Office. But the overall cost of the cyberattack (lawsuits, credit monitoring, fines, forensics, data and systems repair) is estimated at $1 billion.
- **An insider threat** isn't something you want to think about, but it can happen. Employees know how your business operates and how to access important information. They could be involved in data scams or other offline data theft tactics (stealing paper files or copying digital files to a USB). If one of your employees commits a cybercrime or data breach, it could straddle the realm of fidelity and crime insurance coverage. Ask your broker if there are any exclusions in your cyber liability policy regarding insider attacks (those involving employees, directors or officers).

Ethical hackers help businesses with cyber liability

All types of hackers roaming the internet, but some of them use their skills for good. The term "hacker" is synonymous with bad people doing bad things using computer skills (stereotypically in dark rooms wearing hoodies and drinking a lot of caffeine). White hat hackers (aka "ethical hackers" or "researchers") help businesses by testing systems and exposing vulnerabilities. There are businesses built on researchers and ethical hackers who consult with companies for arranged fees to achieve a security goal.

Check with your broker about ethical hacker consultation services. Even if they aren't offered as a policy perk, you can pay for a consultation to stress test system weaknesses and expose bugs or other vulnerabilities.

Give your broker a buzz

You've stepped up to the plate for cyber liability coverage, but you're not feeling tech savvy enough to flip the switch on your own. Don't judge yourself. Even a technology professional would have difficulty understanding the nuances of insurance. That's why a seasoned broker is worth their weight in semiconductor chips. Put your impressive newfound knowledge to use and call your broker.

Wylie-Crump Limited
info@wyliecrump.com

Wylie-Crump Limited
320-151 East 2nd Ave
Vancouver, BC V5T 1B4

.