DATASTREAM

data driven cyber insurance

Top 5

Things to Look for In Cyber Insurance

Who Should Read This?

This guide is written for small and medium business owners who want to figure out the best way to keep their companies safe. It is primarily aimed at the Director of IT, your head of technology, the owner, or anyone else in the company who needs to protect against cyber-attacks.

Is Cyber Security REALLY a problem?

- **68%** of small business has experienced a cyber-attack in the last 12 months (2019)
- **47%** of companies between **100 – 1,000** employees are hit with a ransomware attack last year.
- The average cost to remediate a ransomware attack is **$505,827** for a company between **100 and 1,000** employees.
- Avg cost for a SMALL business data breach is **$120,000** to **$1.24 million** (2019)
- Of small businesses, **37%** suffer financial loss, **25%** file for bankruptcy, and over **9.7%** go out of business.

So, how do you protect your business?

Good IT security helps—but in all these cases... the results of getting HIT, even with some of the best security systems in place—can be disastrous.

You may want to consider... Cyber Insurance

- It covers you WHEN you still get hacked (ransomware or breached)
- Pays to get your systems restored (when possible) or replaced, so you can get your business back up and running
- Covers the costs of lost revenue while your business is down
- Helps pay to harden your systems—to reduce future attacks
- Drastically reduces liability from exposed confidential data
- Helps remediate your reputation
- Protects you from the cost of damages to third parties

Even with all of the advantages of cyber insurance, who should you select? They are NOT all the same.

Some do not provide or recommend the right coverage. When considering cyber insurance, you need to make sure it covers the most common problems including breach, ransomware, cyber-crime, cyber terrorism—and has the capability to properly evaluate your risk (based on actual data, not black-box formulas).

Not all carriers help you avoid a breach. Some don't do a proper analysis in advance of your potential problems, do not provide security awareness training, a risk reduction plan, or adequate information—critical if a problem occurs.

Most do not provide immediate help. Most insurance companies do not know your business and require you to hunt for an approved security expert if a breach occurs.

They don't recommend or leverage existing cyber-security tools. You need tools that will effectively prevent and respond to cyberattacks, plus FAST expert help, preferably from someone who knows your business, IT systems and team.

Most do not have any sources to help FIX your breach. Some will pay to replace but do little to help you recover (which is the more significant loss)—and most don't even know who can help you.

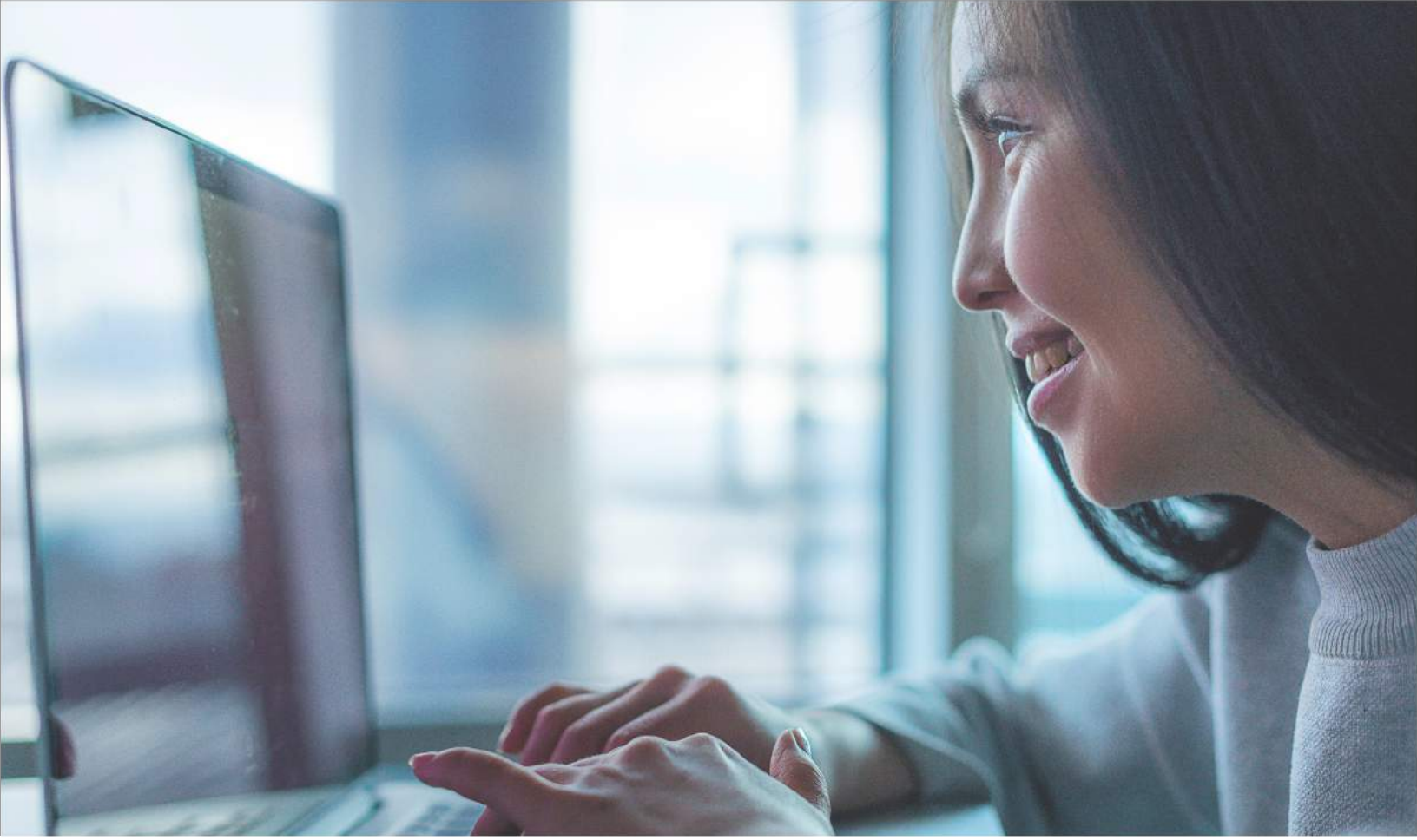
Top Five Things to Look for in a Cyber Insurer

1

The Cyber Insurance Products and Coverage

It is important to understand exactly what 1st party and 3rd party losses are included in your coverage, such as: breach, ransomware, cyber-crime, cyber terrorism, and risk analysis tools. You should look for the following:

- **Complete First-Party Coverage.**
  Covers losses and damages to your company's computers, network, IT systems, and business that result from a cyber-attack.
- **Complete Third-Party Coverage.**
  Covers losses and damages to third parties, such as customers or related business, that result from a cyber-incident.
- **Clear Language and Explanations.**
  Understanding precisely what is covered and not covered is critical in really getting to know your coverage and vulnerabilities.
- **Compares Your Cyber Coverage to Your Peers.**
  Knowing how your cyber coverage compares to similar-sized companies in your industry. This allows you to make the best decisions if it's time to make a switch.



2 Pre-Breach Services

Your company should have the most up to date and appropriate analysis of your individual cyber risk in financial terms. You want to select a company that can also analyze your individual IT systems and cybersecurity risk.

- **Comprehensive Cyber Risk Analysis.**
  A detailed individual cyber risk analysis from a cyber risk model should incorporate thousands of potential risk factors. Preferably a model that includes the most data as possible.
- **IT and MSP Coordination.**
  Your company should use an insurance firm that knows your team and works directly with your MSP. This leads to a quick and efficient recovery when necessary.
- **Analyzing Your Current IT and Cyber Stack.**
  Determining the current state of your IT and cybersecurity stack. You can see your security risk compared to similar organizations of your size and industry.
- **Breach Preparedness and Security Awareness Training.**
  Your choice of insurer should be able to educate your team on how to protect your company pre-emptively.

3 Breach Response Services

Know what to do after a breach, things like PCI re-certification services, notification expenses, foreign notification, PR expenses, overtime compensation, reputational harm, etc. But also, the effectiveness of a response if an incident occurs:

- **Incorporates Current MSP.** Need a provider that works directly with your pre-vetted MSP in advance and after an incident to ensure the absolute fastest and most-effective resolution.
- **Expert and Professional Repair.** You and your MSP need access to a network of world-class cyber responders who have dealt with nearly every type of cyber incident—to help resolve issues fast.
- **Incident Preparedness.** A response team to work with you and your MSP in advance, and again after an incident to harden your systems and assure that another attack doesn't take place.
- **Breach Coach.** You also need a dedicated breach coach to help you manage a cyber incident, retain a forensic professional, notify customers, and manage crisis communication.
- **Computer Forensic Services.** You will need a forensic investigator who is assigned to work with law enforcement agencies and private firms in the collection, preservation, and examination of your digital media. Find someone who will connect you to these services and ensure that an investigation is both immediate and thorough following a breach.
- **Bricking.** Bricking is when a computer device is rendered non-functional after a cyber-attack. Your insurance company needs to replace your device if it cannot be restored.

4 Distribution

You need an insurance company that can work directly with your MSP and IT team. By leveraging the expertise of your IT team, MSP, and your insurance company, you will have the best cyber coverage, paired with the best cyber risk tools, all within a few mouse clicks.

- **Direct-Buy.**
  You can directly purchase cyber insurance from an insurance specialist who understands security and how to match your needs to the best coverage; versus a typical insurance broker who isn't a cyber expert.
- **Affiliate.**
  A company that aligns with your pre-vetted local Managed Service Provider (MSP) who already knows your business, systems and security. This assures individualized help to prevent security problems or the fastest response and remediation if there is ever an incident.

5 Cyber Tools

Work in partnership with managed security service providers (MSSP) that are certified to help prevent breaches and remediate if they occur. They should use the following tools:

- **Threat Monitor.**
  Need to use the best threat detection and monitoring services and system to help prevent breach, phishing, and ransomware attacks.
- **DDoS Mitigation.** Find people who leverage tools to mitigate a denial-of-service cyber-attack when a perpetrator seeks to temporarily or indefinitely disrupt a domain, machine, or network.
- **Credential Monitoring.**
  A good team runs alerts on your employee's credentials, passwords, and data and sends alerts if they appear to have been compromised—helping you make changes to prevent an identity breach.
- **Patch Manager.**
  Your systems are monitored to ensure all drivers and applications are up-to-date and then automatically updated, or your MSP is notified to update—ensuring you reduce system vulnerabilities.

Visualization – Picture this

Old Life

You walk in—you've been HACKED (even after all your IT prevention). All your network is bricked, "Pay **$100,000** or else…" Your customer credit card numbers are all exposed—on the dark web. Your reputation is toast; you're liable for tens of thousands in penalties. The same thing happened to your friend's business—he's gone.

You sit down, dazed and angry—how are you going to recover?

New Life

This time you walk in, hear about an attack, and all you see is a joker head with a demand for **$100,00** or your system will be wiped out. You don't like it—but have a plan. You conference call your MSP and your insurance company, and they go to work.

Your MSP secures most of the system, and your insurer pays off the amount, alerts the police simultaneously while your MSP quickly restores and cleans your system, and then swaps the hard drive. Everything is restored—you are back up. Life is good.

Brought to you by DataStream Insurance. Data-driven, MSP Approved Cyber Insurance.