# What Every Business Should Know About Cyber Insurance

Image yourself walking into the office tomorrow morning, and you can't access your computer files. Accounts payable, pending invoices, confidential client information, your latest project. All gone. Potentially forever. The only screen displayed is demanding $1,000 in Bitcoin. If I pay the ransom, will they unlock my files? How do I pay in Bitcoin? Should I notify law enforcement? Am I required to notify my clients? Which of the 48-different state and territory breach notification laws am I required to follow? How much time and money will this cost my business? What will my clients think?

Major hacks such as Target, Home Depot, and Equifax certainly bring fear to the average consumer. However, these headlines are misleading in that small to medium size businesses (SMBs) are bearing the brunt of cyber-attacks, but rarely get any national attention. According to Symantec, SMBs comprise roughly 60 percent of all breaches. Of those, roughly 1 of 2 are out of business within 6 months of the attack.

SMBs are an ideal target for cyber criminals. Unlike large businesses, SMBs lack the revenue for dedicated IT personnel that constantly monitor their network, install the latest patches, and employ complex multilayered defenses. Commissioner Luis A. Aguilar of the SEC has the most succinct summary of the cyber-security problems faced by SMBs:

> *"Cybersecurity is clearly a concern that the entire business community shares, but it represents an especially pernicious threat to smaller businesses. The reason is simple: small and midsize businesses are not just targets of cybercrime, they are its principal target. In fact, the majority of all targeted cyberattacks last year were directed at SMBs"*

Most business owners have contemplated cyber insurance, but many have hesitated to purchase what is now considered a routine cost of business by larger organizations. Mainly, it's a lack of understanding their exposure, and being intimidated by the seemingly endless number of options. To compound the problem, most insurance brokers do not have the requisite technical background, education, or experience, to fully advise you.

This two-page guide is not legal advice, nor will it cover all the deeper complexities inherent with cyber insurance. That requires a personal conversation. For the purposes of the average business owner, it should answer your most common questions.

**Do I need cyber insurance?**

If your business relies on computers to perform daily work functions, it's generally in your best interest to have a cyber policy. Even if you don't store social security numbers or medical information, you may still have credit card numbers, sensitive client information, or be susceptible to a ransomware attack. Hopefully, you never use it, but the odds are mounting ever more against you.

**Do I already have cyber coverage elsewhere?**

Approximately a decade ago, general business insurance policy began excluding this type of coverage. Your general business insurance may provide a small endorsement, typically up to $10,000. As you will see, this is generally insufficient to cover the overall cost to handle your breach when it inevitably occurs. You should consider a separate cyber policy.

**How much does cyber insurance cost?**

The cost of a basic cyber will depend on a host of factors including: Your industry, the amount of information on your computer system, your yearly revenues, and possibly the cyber security measures you currently have in place. Cyber policies are currently very affordable due to the amount of competition in the market. They can start at under $1,000 per year for a small business. Compared to what a breach will cost your firm, it's an easy investment.

# What Every Business Should Know About Cyber Insurance

**How much will a breach cost my business?**

That depends on: your industry, the amount and type of information you keep, and the type of breach. To the right are *median* service costs associated with a breach of a computer system. These numbers do not include the excessive time and stress you will experience if you try to deal with a breach on your own.

- Breach Coach Services: $400+ per hour
- Credit Monitoring: $35 - $100 per client
- Computer Forensics: $850- $2000 per hour
- Regulatory Action: *$100,000+ per breach*
- Public Relations Team: $25K+
- PCI Fines & Remediation: *$43,000*
- Business Interruption: Varies from Hours to Weeks+
- Cyber Extortion Cost: $1,000
- Client Lawsuit Cost: Unknown

You can tell by the numbers to the right that breach costs can quickly escalate beyond the normal capacity of most SMBs to pay out of pocket. Remember, Symantec stated that roughly half of small businesses are out of business within six months of a breach.

**What should be in a standard cyber policy?**

You should look for the following fundamental coverages: Breach notification, credit monitoring, computer forensics, regulatory action and compensatory awards, crisis management and public relations, PCI fines and remediation coverage, cyber business interruption, hacker damage, and cyber extortion. Certain policies are now offering extra coverage for cyber-crime, unplanned network outages, and reimbursement for lost revenue if your cloud provider goes off-line. The necessity, and amount of each coverage, depends on your business type and network structure.

**How should cyber insurance help with ransomware?**

Ransomware is the most common threat a business will face. An adequate cyber policy should pay the ransom to (hopefully) unlock your files, hire a computer forensic expert to remove the malware from your system, and reimburse your business for much of your lost revenue. That may sound simple, but at $800+ per hour, a few hours of forensic work can cost more than the cyber policy for a small business. Failure to properly examine a breach and notify the proper authorities can result in $100,000+ fines in many states. While all of this is occuring, your business is unlikely to be operating, resulting in sizeable revenue losses.

**How difficult are the applications?**

Companies that host significant amounts of sensitive information, or want unique coverage options, will need to complete a full cyber application. A specialized broker and IT professional can assist greatly in this area. Many businesses can complete a conditional application. So long as you meet the appropriate conditions, you don't have to fill out any computer related questions. You can have a quote within 10 minutes.

**Which cyber insurance companies should I consider?**

There are roughly 30 companies offering this type of coverage, and each policy has its own pro's and con's. For many business owners; Hiscox, Beazley, or Berkley are worth considering. A specialized broker will need to advise you further as each is suited to a different type of business.

# What Every Business Should Know About Cyber Insurance

**Why would a hacker target my business?**

To quote Michael Corleone from The Godfather, "It's not personal. It's just business." Unless you are widely known to hold large amounts of valuable information hackers are unlikely to specifically target you. Hackers work on the law of large numbers, meaning they are scanning every computer and network on the internet to find a specific vulnerability they can exploit for profit. In many cases they may be the only person in the world that is aware of that vulnerability, so most cyber countermeasures are irrelevant.

**What if I already use a firewall, anti-virus, etc..?**

The DEA has been battling the illicit drug trade since the Nixon administration, with little headway. Government agents making $100K per year are battling drug lords that reap billions in untaxable profits. Likewise, computer security will always be playing catch-up to innovative hackers around the globe. Computer security is useful, and should certainly be taken seriously, but none come with a guarantee. Robert Mueller, the former Director of the FBI had this to say:


*"I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again. "*

**Do I need specific cyber security measures in place to get cyber insurance?**

Not necessarily, but they are helpful. The minimum requirements necessary for each insurance company offering cyber insurance varies. This is where a specialized insurance broker can save you a lot of time and energy.

**What if I have more questions?**

Feel free to reach out to your general insurance broker. If you would like a specialist, consider contacting Joseph Brunsman at joseph@cplbrokers.com, or Dan Hudson at dhudson@cplbrokers.com. 443.949.5228

**About the Authors:**

Joseph Brunsman is the Vice-President of CPLB, Inc. Currently, he is pursuing a Master's in Cybersecurity Law. He is a former IT, with a degree in Systems Engineering (Robotics) from the United States Naval Academy. He is the co-author of True Course: The Definitive Guide for CPA Practice Insurance, as well as numerous articles found in nationwide publications. He specializes in helping SMBs find tailored cyber insurance solutions.

Dan Hudson is the President of CPLB, Inc. He is also a graduate of the United States Naval Academy, a retired Naval Officer, and a former Commanding Officer. He is the co-author of True Course: The Definitive Guide for CPA Practice Insurance, as well as numerous articles found in nationwide publications.