



Do You Really Need Cyber Liability Insurance?

[Comment Now](#) Raj Sabhlok

[Follow Comments](#)



It's been a few years since anybody asked me for a report on "how I spent my summer vacation." Sadly, the truth is that while many spent their summers searching for last-minute vacation deals or browsing local flea markets, I spent countless hours shopping for something decidedly less seasonal – cyber liability insurance.

Not surprising considering this was the "Summer of Hackers," when companies like LinkedIn, eHarmony, DropBox, and Yahoo! got hit hard by [cyber attacks that exposed private information for million and millions of user accounts](#). With tens of thousands of customers transacting business online with [ManageEngine](#) each year, I needed to understand our potential legal exposure to such a breach. In the event of an attack, are we covered under our standard business liability insurance policy?

In most cases, the answer is no.

Liability for loss of customer or employee data is not typically covered under a corporate insurance policy. Some existing business insurance policies that offer general liability and directors and officers liability may provide a measure of coverage for those areas; however, most CEOs discover significant gaps in what is and what isn't covered *after* an attack. Unfortunately, by then it's too late. I didn't want to be in that boat.

However, as with anything that the financial industry can monetize via a hedge, a derivative or other financial instrument, you can now purchase cyber liability insurance.

[A recent survey](#) by Chubb Group of Insurance Companies found that 65 percent of public companies forego cyber insurance – even though they identify cyber risk as their number one concern. Meanwhile, a quarter of those surveyed are expecting a cyber breach in the coming year, and 71 percent have cyber breach response plans in place.

Ostensibly, high-profile and high-risk companies may appear to be at greater risk, but small-to-medium sized businesses are not immune. According to a recent study by the U.S. Secret Service and Verizon



TOLMAN & WIKER INSURANCE SERVICES, LLC

INNOVATIVE RISK ADVICE SINCE 1923™

BAKERSFIELD | LOS ANGELES | SALINAS | SANTA MARIA | VENTURA

Communications, Inc., [over 72 percent of all data breaches](#) occurred in SMB businesses. The average cost of a breach? Over five million dollars, according to most financial analysts. Bottom line is we are all at risk.

So why do only 35 percent of companies invest in cyber liability insurance?

For one, many executives don't know that it exists. And even if they do, they probably don't think an attack will happen to them, or they're not overly worried about the potential fallout of such a breach. However, for many more, the high cost of policy premiums is prohibitive.

Policy premiums are primarily based on your industry. For example, if you are an e-commerce company doing online transactions and storing data such as credit card information, you are considered high risk for data breach and thus subject to higher premiums. Medical-related institutions hosting data, such as date of birth information, social security numbers and medical records, are also higher risk.

Fortunately, I've discovered secrets to reducing those hefty cyber liability premiums. The most important one is to reinforce your security practices before you apply – essentially try to qualify for a “good-driver” discount. Plus, boosting security not only helps to decrease the cost; it simultaneously decreases your overall risk factor to breaches.

How do you do it? [Security](#) experts agree that the easiest place to start is strong password protection, and yet it's something that even IT-sophisticated companies often fail to master. Interestingly in all of those “Summer of Hackers” cases, [the cause can be traced back to weak passwords](#) that were either 1) not encrypted or “salted” or 2) not changed regularly.

If managing passwords for all those servers, apps, cloud services, databases, tablets and laptops seems like a chore, there are affordable password management solutions that do it for you – with a price tag in the hundreds or low thousands of dollars, compared to those high-risk premiums that can run in the millions.

Other tips to help drive down premiums include:

- Conduct **regular risk assessments** to reveal hardware, software and individual site vulnerabilities.
- Create a **written IT security policy** that identifies critical assets and defines policies for physical security, account management, and backup and recovery among other areas.
- Leverage firewalls, virtual private networks, anti-virus and anti-spam software and secure mobile solutions to **secure network access and mobile devices**.

I'm not suggesting that you won't need cyber liability insurance if you implement these types of security reinforcements. In fact, I suspect that it is destined to become part of business liability coverage soon, and customers, suppliers, boards and investors will insist that you have the appropriate amount to do business.

But what I've learned over the “Summer of Hackers” is that you can manage the cost – and the likelihood that you'll become the next casualty – by putting some simple security controls in place *today*.

Source: <http://www.forbes.com/sites/rajsabhlok/2012/10/18/do-you-really-need-cyber-liability-insurance/>