CONNER STRONG & BUCKELEW

Ran in Greater Philadelphia Chamber of Commerce in November 2015

4 Reasons You Don't Have Cyber Insurance (But Should)

NOVEMBER 3, 2015

TERRENCE J. TRACY, CPA | MANAGING DIRECTOR AND EXECUTIVE VICE PRESIDENT | CONNER STRONG & BUCKELEW

Odds are that your business isn't insured for a cyber attack. Only about 20 percent of U.S. businesses are, according to some industry estimates.

Cybersecurity is still mystifying for most business owners, who often don't understand the fundamentals of the issue. Without this knowledge, they underestimate the odds of something bad happening to them – essentially the root cause of anyone being underinsured in the first place.

When we talk to clients about cyber insurance, there are some common responses we hear. If you don't have cyber insurance, here are four guesses why, with some explanation of the realities that may belie your assumptions.

> "Just like any crime, there are all kinds of reasons cyber crime is committed, and they don't have to be good ones to hurt your business."

1. You think there's no reason for someone to attack you

Do you store any customer information? Are you connected to the Internet? Guess what – that's all the reason necessary to make you vulnerable to attack.

One of the biggest misconceptions about cyber crime is that there needs to be a well-thought-out reason behind it. Surely, financial gain is often in mind, but sometimes attacks are perpetrated solely to boost the attackers' egos. Furthermore, attacks don't have to take place from outside your organization – a disgruntled employee often has the easiest access.

Just like any crime, there are all kinds of reasons cyber crime is committed, and they don't have to be good ones to hurt your business.

2. You don't know the costs of a security breach

You've probably had more than a few computer viruses over the years. They might have slowed down your computer, but otherwise no big deal, right? A true attack, in which your records are stolen, erased or used for criminal reasons, will cost a lot more than anti-virus software.

IBM and The Ponemon Institute, an organization that studies information security, estimate that breaches due to malicious or criminal attacks now cost businesses an average of $170 per record stolen, which translated to $3.79 million total per breach for the 350 businesses that participated in their joint report, "2015 Cost of Data Breach Study: Global Analysis."

The main cost is simply lost business, whether because existing customers leave, or your reputation is damaged in a way that makes new customers stay away. That's not to mention costs to restore anything damaged or replace something stolen, and lost productivity managing the problem.

3. You think hacking requires a lot of skill and effort

You probably have a mental image of hackers sitting in a dark room filled with electronics, cracking complex firewalls by feverishly typing away at their keyboard. In reality, there's a lot easier way to get access to someone's sensitive files: ask for them.

Think about it – thieves always look for the weakest link. If it's difficult to crack a password, why not pretend your someone's boss, call the IT department, and ask for the password? Or, they could call any employee, pretend to be from the IT department, and request their login information.

These types of tricks are known as social engineering because they manipulate people, not systems, to exploit sensitive information. When any prank caller can become a cyber thief, it certainly changes your perspective on cyber risk.

4. You think you're too small of a target

Yes, your small- or medium-sized business probably doesn't need to worry about a sophisticated attack from a nation state like those you read about in the news. But don't think just because you only read about massive data breaches that only large companies are threatened.

In fact, smaller companies have more to worry about. An attack on a business without the massive assets of a multinational conglomerate can mean that they don't have the ability to withstand and recover from an attack. With lower margins for losses, there's even more reason to manage that risk.

To further complicate matters, all these issues are changing on a daily basis. According to a report released in October from the Insurance Information Institute, cyber attacks and breaches are growing in frequency and cost, on pace to exceed a record 800 data breaches in the U.S. this year – almost certainly an underestimate, given how many companies are unaware they have been hacked at all.

All these factors point to one final point – it's no longer a matter for businesses to consider whether to acquire cyber insurance, but a question of whether they'll do so before they're hacked themselves.

If you'd like to learn more, visit us at www.ConnerStrong.com.

Ran in Greater Philadelphia Chamber of Commerce in November 2015

CONNER STRONG & BUCKELEW