HOTCHKISS
INSURANCE

CYBER COVERAGE ›

The New Norm

What if we told you that the technology and computers of our civilized world are going away. Paper is back! You can rest easy because with no internet, emails, instant messages, tweets, funny cat videos, mobile phones or the possibility of lawsuits . . . there's not much to worry about, right?

Obviously, this is not the world we live in today! It's a digital world.

The Old Question: Do You Need Cyber?

Twenty years ago, the common misconception was that only tech companies needed cyber coverage. This is simply not true.

Let's back up a couple steps. What exactly is cyber coverage? Cyber insurance, also referred to as cyber liability insurance, data breach insurance, or simply hacker insurance is an insurance product that covers the costs associated with hack attacks and data breaches.

Some Key Components:

- Cyber Ransom
- Regulatory Fines
- Reconstruction Costs
- Ongoing Credit Monitoring

A common misconception is that hacks only happen to large companies. Though the news makers are typically the large companies, small- to medium-sized businesses are impacted across the country on a daily basis. A few questions to consider:

- Do you have employees or customers?
- Do you use technology? A cell phone? Do you store contacts in that cell phone and use it for business?
- Do you take credit card payments? Did you know you can be fined up to $500,000 before you even pay the fraud and card re-issuing costs?

It doesn't matter what industry you serve. If you own a phone, a computer, have an email account, collect data, have any personally identifiable information for any of your customers, employees, or vendors, or depend on someone that has any of those items stored on behalf of your business, you need cyber coverage. With the purchase of a strong cyber policy, not only will you be protected, but it will strengthen your position with regulators, investors, customers and the public.

Common Attacks:

- Human Error: Lost and stolen laptops and phones
- Hacker
  - Average total cost is $5,920,000
- Phishing: Social Engineering Targeted at Employees
  - Example: An office manager opens an email that appears to contain an invoice, which allows the firm's online banking account to be commandeered and triggers a computer virus.
- Extortion
- Hacktivism: Social and Political "Hactivists"

In the News:

- **Garmin Paid Multimillion Dollar Ransom to Recover Data from Hackers**
  https://www.businessinsider.com/garmin-paid-multimillion-dollar-ransom-to-hackers-report-2020-8
- **Capital One to Pay $80 Million Fine for Data Breach During Cloud Transfer**
  https://www.bizjournals.com/washington/news/2020/08/06/capital-one-federal-reserve-occ.html

Ultimately, even with all the important safeguards in place and a strong IT team, you're still vulnerable. And unfortunately, 60% of businesses that have a breach will not be in business six months after the breach due to cost, reputation or recovery.

The Question Now: Why Don't You Have It?

With virtual interactions and cyber attacks on the rise, this coverage is integral to protecting your assets. Even with a strong strategy with hardware, software and cryptographic methodologies, it's nearly impossible to achieve perfect cyber security protection; but that's where this coverage comes into play.

At Hotchkiss Insurance, we simplify the process to protect clients with a cyber policy that complements their cyber protection strategy. For us it is not only about writing insurance, we pride ourselves in providing our clients with comprehensive enterprise risk management and a seamless client experience.

Because this is a complex risk, many clients are surprised by how affordable this coverage can be. We keep the pricing for these policies simple, as it ultimately depends on factors such as the number of identity records you keep, and the number of transactions you have in any given year.

It's time to make the call and gain a trusted partner to vigilantly protect your assets and keep your business from becoming a statistic.

> Even with a strong strategy with hardware, software and cryptographic methodologies, it's nearly impossible to achieve perfect cyber security protection; **that's where this coverage comes into play.**

To get started, call us at 972.512.7755

Industry-Specific Cyber Statistics:

- 43% of breach victims were small and medium businesses.
- Small and mid-sized businesses are better targets because often the illusion is that they don't need Cyber coverage and often lack a cyber plan, budgeted resources, trained security professionals and an understanding of their security needs. Most companies rely on IT support who have different skills than a cyber security trained professional.
- The banking industry incurred the most cyber crime costs in 2018 at $18.3 million.
- Supply chain attacks are up 78% in 2019.

Security Spending and Costs:

- By the end of 2020 (estimated before COVID-19), security services are expected to account for 50% of IT budgets.
- The average cost of a malware attack on a company is $2.6 million (Accenture).
- $3.9 million is the average cost of a data breach (IBM).
- The average cost in time of a malware attack is 50 days. (Accenture)
- The most expensive component of a cyber attack is information loss at up to $5.9 million per incident (Accenture).
- Including turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill, the cost of lost business globally was highest for U.S. companies at $4.13 million per company. 50% of large enterprises (10,000+ employees) are spending $1 million or more annually on security, with 43% spending at least $250,000.

hiallc.com