CYBER ATTACKS – AN ESCALATING RISK

Companies have relied on computers for years, but the number of threats facing computer networks and company data is quickly increasing.

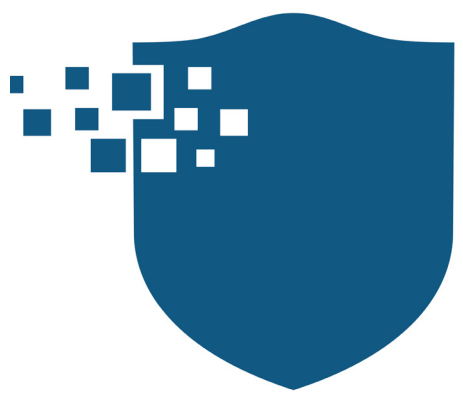
Does Your Company Need Cyber Insurance?

All of the phishing and ransomware headlines over the last year have led to a more pointed question – what if someone uses your own technology against you for their profit?

Many small and midsize businesses have relied on computer networks to be successful for over two decades. Technology has transitioned from a useful tool, to a vital resource, and finally to the core of their company's product or service offerings. Each of these transitions has made businesses more efficient, but it has also increased their exposure to a major risk. What if your technology stops working? What if it gets used against your company?

> **"The insurance industry estimates that around 25% of businesses have some level of cyber insurance coverage, while around 65% are concerned about a security breach. This discrepancy highlights the number of companies who should be actively considering cyber insurance."**
>
> **Wortham Boyle, Jones Insurance Agency**

Ransomware alone is predicted to cost companies $5 billion in 2017. Factor in data theft, security breaches, and phishing emails aimed at your company's accounting department, and the internet begins to look like a very dangerous place.



Like any other time new or massively growing financial risks confront companies, insurers are increasing their policy writing to protect companies against this threat. But what threat does cyber insurance cover? And does your company need it?

What is Cyber Insurance?

Cyber insurance protects companies against the damage that can be caused to their business due to technology threats. It's not a new product – cyber insurance has been available as a highly niche product for over a decade. In the past couple of years, however, it has become widely available to companies of all types, including small and mid-sized businesses. Due to the fast-growing level of risk companies face, coverage is growing rapidly – some estimates of total cost of coverage written in the United States are higher than $4 billion.

Does Your Company Need Cyber Insurance?

Compared to traditional types of insurance, cyber insurance policies are more complex. One reason for this is that mass availability of cyber insurance policies is relatively new, so there are few "market norms" that all underwriters feel pressured to offer.

Another reason is that, unlike general liability or commercial property insurance, the threats change constantly. For instance, ransomware attacks increased 250% in the first few months of 2017 compared to the year before. The variability in risk is very difficult for actuaries to manage when pricing policies.

Depending on the policy, cyber insurance can cover damages due to viruses, malware, data breaches, infringement of patents or trademarks, or deceptive funds transfers (when an employee is tricked into transferring company funds by someone pretending to be a high-level company executive).

One major difference in policies is whether they cover only third party damages (damages to parties other than the company holding the insurance) or also cover first party damages. For instance, if your data is deleted by someone who attacked your network, will the policy only pay the damages caused to your customers, business partners and vendors, or will it also compensate your company for the money it lost due to the data loss.

Currently, third party coverage is much more commonly offered than first party coverage. First party coverage is also much more expensive, because the likelihood of a company losing money due to a cyberattack is much higher than the likelihood of the company causing damage to third parties.

If your company retains data on customers, one of the biggest threats posed by cyber criminals is a data breach. North Carolina state law requires that businesses suffering a security breach to notify affected customers when the breach includes personally identifiable information. While this notification does damage to a company's reputation, the damage is much worse if companies don't offer credit monitoring when the customer is notified. Depending on how many customers were affected, this credit monitoring can be very expensive.

Third party coverage of data breaches often includes this credit monitoring service. In many cases, a specific "package" of services is also offered in the event of a data breach, including crisis management and communications services. These packages provide benefits far greater than just financial coverage – they provide a pre-constructed roadmap for companies facing their first data breach. This is a time when quickly making the right decisions can protect the long-term viability of the company, and these packages help companies navigate this time.

Does Your Company Need Cyber Insurance?

Is Cyber Insurance Coverage The Right Decision For Your Company?

A case could be made that almost every business would be wise to mitigate their risk and purchase cyber insurance. Depending on the type of coverage and the level of liability being underwritten, however, cyber insurance can be a major expense. Each company must evaluate the costs and benefits for themselves. As you consider cyber insurance for your own company, here are three questions that can help you determine if coverage makes sense for your business.

Do your contracts require coverage against cyber-attacks?

Because a major cyber-attack can easily render a vendor unable to meet their contractual obligations, an increasing number of business customers are requiring third-party cyber insurance as a condition for bidding on a job. If you've been prevented from bidding on work because you didn't have cyber insurance, it's a good idea to start pricing out policies, because this is likely to become more common as internet-based attacks increase in volume. It's also a good idea to gauge your liability in customer contracts – the higher your liability, the more coverage you'll need to mitigate the risk.

Do you keep customers' personally identifiable information on networked computers?

If you have a large amount of customers' data on your servers, a breach could be financially devastating because you'll need to inform them and will want to provide credit-monitoring services to them. Cyber insurance can protect against this risk.

Would data loss severely damage your company's bottom line?

Imagine that your data was encrypted and you were unable to access it. How many days could you survive without immediate access to it? Who would be unable to perform their job duties, and what payments would not be able to be collected? If the answers to these questions make you uncomfortable, it's worth considering first-party cyber insurance.

The Best Insurance Is a Well-Defended Network

Of course, the best insurance policy is to insulate yourself from risk in the first place! In addition to considering cyber insurance, we also recommend an external evaluation of your network to ensure it is well-defended against cyber threats. While insurance can provide financial reimbursement for the damages encountered as you recover from a cyberattack, it won't make the process fun or easy.

If your company is facing major technology decisions and you're considering a Managed Service Provider, call 919.779.0954 to learn how we can help make the transition a seamless one.