# Cyber security insurance—What is it and why do I need it?

## What is cyber security insurance?

Does your business maintain electronic records with personal data on your clients? Is your company prepared to absorb the significant financial implications associated with an unauthorized breach of that data? Could a virus cripple your PC network? If so, do you have enough cash reserves to make up for the downtime or can you survive the loss of business?

If you can't answer any of these questions, it may be the right time to call your insurance agent and ask about cyber security insurance. That's a catch-all term for policies that cover hacked computers, virus attacks, denial-of-service attacks, web content liability and other technology-related areas. Cyber security insurance also goes by e-commerce, e-business, information security, cyber risk, network security or hackers insurance.

As a business owner, you know that electronic records and data are just as valuable, if not more valuable, than paper or hard-copy documents. Although not physical in nature, electronic data is nonetheless "essential" in all aspects of your business activities and has intrinsic value.

Cyber security insurance is designed for the protection of intangible data. It can be easily explained as coverage for professional errors and the risks of doing business on the Internet or working with a network system. If you are automated, then you are susceptible to the threat of a breach of your systems, your data and your trust. Anyone who is running a business (or someone who is just starting out) really needs to consider this coverage as much as they would consider any other aspect of their business insurance needs.

## Why should I consider cyber security insurance for my business?

A few examples of why you need and should consider cyber security insurance:

- **Costs you could incur to make the proper mandatory notifications to your customers if a breach of your system occurs.** Many states have mandatory notification requirements which require business owners to properly notify their customers when a security breach has occurred. Some states also require these business owners to provide their customers with free credit reports for a year, which can become quite costly.

*Continued on reverse.*

- **Misuse of any information, which is either confidential or subject to statutory restrictions on its use.** Do you have any personal or confidential data on your system that a hacker would want and could gain unauthorized access to?
- **Defamation.** You, as a company, have a direct responsibility for what is on your website. Companies also can be held responsible for their employees' email content.
- **Transmission of a virus.** Did you know that a company could be held liable if a third party contracts a virus from your company's website or email, and as a result, that third party suffers a loss as a direct result of that virus?
- **Legal costs incurred in the defense of an action for loss.** Don't forget about the costs involved just to defend a company when a third party accuses or sues because of the harm or lost revenue caused to their company by your system's breach.

## Is there anything I can do to reduce my cyber security risk exposure?

You can reduce your risk by:

- installing audit features that monitor logon and logoff activities;
- providing warnings that unauthorized users may be subject to monitoring and prosecution;
- developing and implementing a trap and tracing mechanism with your local telephone company;
- implementing systems that identify outside callers;
- reporting significant security breaches to relevant government agencies;
- implementing policies and guidelines regarding the use of computing and information;

*Continued on reverse.*

- encouraging employees to use encryption technologies, if appropriate; and
- implementing security upgrades when they become available.

Some states require you to notify each individual that has been affected due to a breach of your data. A recent study by Digital Forensics Association of data breach occurrences from 2006-2010 reports people's records were "lost" on an average of 15,000 records per hour over that time span, which cost businesses more than $156 billion. Moreover, the frequency of attacks increased in 2011. Small- to medium-sized businesses represent prime attack targets for many hackers, who favor highly automated, repeatable attacks against these more vulnerable targets.

## What does a cyber security policy typically include?

- Legal liability for damages to third parties, caused by a breach of network security;
- coverage for loss caused by an administrative or operational error;
- breach of privacy coverage for damages resulting from alleged violations of HIPAA, state and federal privacy protection laws and regulations;
- customer notification expense reimbursement (policy sublimit will be set);
- public relations expense coverage;
- comprehensive business interruption expense coverage; and
- cyber extortion reimbursement coverage.

## Call us for further details

If your company uses computers in any fashion to maintain or disseminate data on your clients, you need cyber security coverage. Call our agency for further information.