CARPENTER INSURANCE
"Home For All Your Insurance Needs"
EST. 1935

Privacy and Cyber Security

With the enormous amount of sensitive information stored digitally, companies need to take the proper measures to ensure this data is never compromised. Ultimately, it is the responsibility of business owners to protect their clients' data. Failing to do so can result in a data breach, which costs companies billions of dollars every year. Understanding the risks involved with data security can help you prevent a privacy breach.

Know the Risks

The first step in protecting your business is to recognize basic types of risk:

- Hackers, attackers and intruders—These terms are applied to people who seek to exploit weaknesses in software and computer systems for their personal gain. Although their intentions are sometimes benign, their actions are typically in violation of the intended use of the systems that they are exploiting. The results of this cyber risk can range from minimal mischief (creating a virus with no negative impact) to malicious activity (stealing or altering a client's information).
- Malicious code—This is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system.
  - Viruses: This type of code requires that you actually do something before it infects your system, such as open an email attachment or go to a particular Web page.
  - Worms: This code propagates systems without user interventions. They typically start by exploiting a software flaw. Then, once the victim's computer is infected, the worm will attempt to find and infect other computers.
  - Trojan horses: Trojans hide in otherwise harmless programs on a computer, and much like the Greek story, release themselves when you're not expecting it and cause a lot of damage. For example, a program that claims to speed up your computer system but actually sends confidential information to a remote intruder is a popular type of Trojan.

IT Risk Management Practices

To reduce your cyber risks, it is wise to develop an IT Risk Management Plan at your organization. Risk management solutions utilize industry standards and best practices to assess hazards from unauthorized access, use, disclosure, disruption, modification or destruction of your organization's information systems. Consider the following when implementing risk management strategies at your organization:

- Create a formal, documented risk management plan that addresses the scope, roles, responsibilities, compliance criteria and methodology for performing cyber risk assessments. This plan should include a characterization of all systems used at the organization based on their function, the data stored and processed and importance to the organization.
- Review the cyber risk plan on an annual basis and update it whenever there are significant changes to your information systems, the facilities where systems are stored or other conditions that may affect the impact of risk to the organization.

Due Diligence When Selecting an ISP

In addition, your organization should take precautionary measures when selecting an internet service provider (ISP) for use for company business. An ISP provides its customers with Internet access and other Web services. In addition, the company usually maintains Web servers, and most ISPs offer Web hosting capabilities. With this luxury, many companies perform backups of emails and files, and may implement firewalls to block some incoming traffic. To select an ISP that will reduce your cyber risks, consider the following:

- Security – Is the ISP concerned with security? Does it use encryption and SSL to protect any information that you submit?
- Privacy – Does the ISP have a published privacy policy? Are you comfortable with who has access to your information, and how it is handled and used?
- Services – Does your ISP offer the services that you want and do they meet your organization's needs? Is there adequate support for the services provided?
- Cost – Are the ISP's costs affordable and are they reasonable for the number of services that you receive? Are you sacrificing quality and security to get a lower price?
- Reliability – Are the services provided by the ISP reliable, or are they frequently unavailable due to maintenance, security problems and a high volume of users? If the ISP knows that their services will be unavailable, does it adequately communicate that information to its customers?
- User supports – Are there any published methods for contacting customer service, and do you receive prompt and friendly service? Do their hours of availability accommodate your company's needs?
- Speed – How fast is your ISP's connection, and is it sufficient for accessing your email or navigating the Web?
- Recommendations – What have you heard from industry peers about the ISP? Were they trusted sources? Does the ISP serve your geographic area?

Government Regulation

There aren't many federal regulations regarding cyber security, but the few that exist cover specific industries. The 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley (GLB) Act and the 2002 Homeland Security Act, which includes the Federal Information Security Management Act (FISMA) mandate that health care organizations, financial institutions and federal agencies, respectively, protect their computer systems and information. Language is often vague in these laws, which is why individual states have attempted to create more specific laws on cyber security. California led the way in 2003 by mandating that any company that suffers a data breach must notify its customers of the details of the breach. Currently, all 50 states and the District of Columbia have data breach notification laws in place.

Protection is our Business

Your clients expect you to take proper care of their sensitive information. You can never see a data breach coming, but you can always plan for a potential breach. Contact Milton Carpenter Insurance today—we have the tools necessary to ensure you have the proper coverage to protect your company against a data breach.