Protecting Against Cyber Crimes

Cyber Liability is one of the hottest topics in insurance these days. Businesses are coming to recognize that no matter how comprehensive their systems security is, they will always be prone to hackers. Hackers can enter your computer systems through a variety of ways, like stolen passwords or network infiltration, but not all of their methods involve technology. In fact, a growing number of cyber crimes are committed through what's being called "social engineering."

In social engineering schemes, hackers take advantage of human weaknesses and temptations to get employees to give up confidential information such as, personal passwords, bank or other financial information, or give access to the computer, allowing them to enter the user's network and wreak havoc to their systems. They do this in a number of ways, for example, by sending emails to employees with falsified sender information, pretending to be another employee or manager, and tricking them to link through to "important information" related to their jobs.

The idea of luring customers into giving up their banking or personal information to strangers has been around for decades—most people by now are wary of these requests. But now, businesses as well as consumers must be vigilant against these scams as hackers are constantly scheming to access networks containing valuable information: everything from top-secret military information to confidential health records to personal financial data.

Once businesses accept that it is virtually impossible to guard against these hackers, they need to take steps to protect their valuable assets from these criminals. Training is an important component of this effort, with formalized classes for employees on when it's okay to divulge confidential information and to whom, and when it is not.

At the corporate level, sensitive information should be housed on systems different from those containing widely used information, and access to such sensitive information should be restricted to only key personnel. Employees should be trained on what suspicious malware links can look like, and companies can even implement practice drills to assess employees' preparedness. IT departments should force employees to change their passwords frequently and implement software updates as soon as they become available.

As wide-scale data breaches continue to occur, tarnishing the reputations of major corporations like Target, The Home Depot, and TJX, more businesses are realizing the importance of a good cyber liability insurance policy. These policies are designed to cover not just behemoths like Target but any small business responsible for sensitive customer, vendor, or employee information. Your Atlas Insurance agent can help you determine whether your business liability policy can provide enough protection in the event of a serious data breach or whether a separate cyber liability policy is needed.

You can choose cyber liability policies that provide coverage for a number of different risk factors, including network infiltration, regulatory fines and penalties, privacy and security breaches, data loss, business interruption, PCI protection, public relations expense, and losses due to social engineering schemes. While policies differ widely with respect to their specific coverages and premiums – premiums usually depend in large part on revenues – your Atlas insurance agent can help you sort through the process to find the solution that works best for your business. Call us at 808-628-5320 or log onto www.atlasinsurance.com. +

BY: CAROL DAVIS
ATLAS INSURANCE

Carol Davis is Senior Vice President – Property and Casualty. With over two decades of experience in the insurance industry, Carol's professional experience involves working with public entity clients throughout the state as well as large private sector clients, where she provides consulting, placement, and day-to-day risk management services.