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

Protecting Against Security Breaches

Financial institutions are top targets for security breaches. While the media often reminds us of high-profile network leaks, financial institutions of all sizes are at risk. Because the unintentional release of sensitive customer information is a larger risk than ever, it is essential that you be prepared to react efficiently and effectively in the event of a breach.

In order to prepare for breaches in security, financial institutions must tighten their data security controls and plan for a potentially significant financial blow should these controls be insufficient. With continual threats of viruses, hackers and unauthorized use of sensitive information, your institution must respond by preventing, detecting and responding to cyber attacks through a well-orchestrated cyber security program.

The Safeguards Rule

The Federal Trade Commission (FTC) issued the Gramm-Leach-Bliley (GLB) Act, which requires financial institutions to ensure the security and confidentiality of sensitive personal information. The Safeguards Rule, which requires all financial institutions under FTC jurisdiction to take steps to keep customer information secure, was issued with the GLB Act. The measures enacted depend on the size and complexity of the company, the nature and scope of its activities and the sensitivity of the customer information it possesses. The FTC requires each plan to include the following components:

- A designated coordinator of the information security program
- An assessment of risks to customer information in each relevant area of the company's operation and an evaluation of the current safeguards for controlling these risks
- A program in place to prevent security breaches
- Service providers that, by contract, maintain appropriate safeguards
- Regular adjustments to the information security program in light of relevant circumstances, changes in the company's operations or results of security monitoring

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 facility.

Employee Training

Employees using data are the first line of defense against security breaches. Thorough training is a keystone of any information security program. Follow these guidelines to promote employee cooperation:

- Conduct background checks before hire.
- Ask employees to review and sign your company's confidentiality and security policy.
- Limit access to information to those employees that require it for job duties.
- Require employees to use strong passwords, incorporating both upper and lower case letters, symbols and numbers.
- Train employees to store materials such as laptops or mobile devices in secure places.

- Train employees to encrypt information, lock rooms and file cabinets, and report all attempts to obtain customer information.
- Remind employees of the legal requirement to keep information secure and confidential, and impose disciplinary policies for violators.
- Immediately deactivate passwords for employees who are terminated.

Network and Information Systems

Design your information systems so that they are as protected as possible from security breaches:

- Take precautionary measures when selecting an internet service provider (ISP). Verify the provider's commitment to security.
- Use appropriate audit procedures to detect improper disclosure or theft of customer information immediately.
- Dispose of customer information in a secure way, shredding papers and erasing data on electronic hardware such as computers or hard drives.
- Maintain inventory of your company's computers and other mobile devices.

In the Event of a Breach

A swift, appropriate response is important if your company experiences a security breach. Follow these steps to minimize damage:

- Preserve and review files or programs that might reveal the extent of the breach.
- Secure any information that may have been compromised.
- Notify consumers, law enforcement and businesses if the breach poses the risk of identity theft, criminal activity or other related harm. State laws regarding notification vary.

Transferring the Risk

Cyber security is a serious concern for all financial institutions. The cost of a security breach can be considerable, and may include the following:

- Credit monitoring services for affected customers
- Creation of new account numbers and re-establishing secure account numbers
- Issuing new credit or debit cards
- Hiring a crisis management or public relations firm
- Class-action lawsuits
- Irreversible damage to the corporate brand

Be sure you are taking steps to prevent security breaches and creating a plan in case one does occur. Contact Financial Institutions to learn about our risk management resources and insurance solutions, such as Internet and media liability, security and privacy liability, and identity theft insurance.