Precautions for Better Cyber Security

Business operations in the technology industry revolve around the functionality of computers, network connections and the Internet. It's no secret that computer use comes with many risks, including damaging viruses, hackers, the illegal use of your system to attack others, the use of sensitive data to steal identities and other illegal actions. As a result, companies must respond by preventing, detecting and responding to cyberattacks through a well-orchestrated cyber security program.

Get Familiar with Risks

The first step in protecting your business is to take notice of the multitude of cyber risks:

Hackers, attackers and intruders: These people 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 data).

Malicious code (viruses, worms and Trojan horses):

- **Viruses:** This malicious code requires a user to take action to let a virus into the system, such as opening an email attachment, downloading a file or visiting a webpage.
- **Worms:** Once released, this code reproduces and spreads through systems on its own. They usually start by exploiting a software flaw; then, once the victim's computer is infected, the worm will attempt to find and infect other computers through a network.
- **Trojan horses:** This disguised code claims to do one thing while actually doing something else. For example, a program that claims to speed up your computer system but is actually sending confidential information to a remote intruder.

The convenience of using computers is accompanied by many risks. Companies must respond by preventing, detecting and responding to cyberattacks through a well-orchestrated cyber security program.

Risk Management Planning

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 its 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.

In addition, your organization should take precautionary measures when selecting your internet service provider (ISP) for use for company business.

ISP Considerations

Almost all ISPs offer Web browsing capabilities with a varying degree of user support and Web hosting capabilities. Your company should determine what ISP to use, along with a plan for backing up emails and files and what firewalls to implement.

To select an ISP that will reduce your cyber risks, consider the following:

- Security: How concerned with security is the ISP? Does it use encryption and secure sockets layer (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 support: 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 your business needs?

- Recommendations: What have you heard from industry peers about the ISP? Were they trusted sources? Does the ISP serve your geographic area?

Cybersecurity is a serious concern for your business. Contact Gallagher Risk Management - Tulsa to learn about our risk management resources and insurance solutions for emerging technology exposures.