CYBER SECURITY CHECKLIST

Depicted below are suggested measures to consider when addressing your exposure to cyber claims.

	Function	Description
□	**Network Security**	Maintain a firewall. Reduce hacker access to your internal data. Utilize up-to-date virus scanning software.
□	**Hardware Protection**	Protect your computer hardware. Servers should be in a locked room protected by proper fire suppression devices.
□	**Password Protection, Backup & Encryption**	Password-protect, backup and encrypt all laptop computers, tablets and smart phones. Theft or loss of these devices is a significant source of cybercrime.
□	**Centralize Responsibility**	Centralize the responsibility for cyber security with a single individual in your company. A specific person will be better able to determine the company's risk, implement loss prevention measures and monitor re-sults.
□	**Secure Personal Data**	Restrict access to personal information. Employee records and client information including IRS numbers, credit card and financial information should be restricted to specific personnel. This information should NEVER be sent via unsecured email.
□	**Assess Vendors**	Assess the cyber security of your software vendors and important customers or suppliers. Viruses or mal-ware coming into or going out of your systems is a significant source of potential security breach.
□	**Publish Policies & Disclaimers**	If you are involved in e-commerce, publish a privacy policy and liability disclaimer regarding the use and protection of personal information.
□	**Develop Contingency Plan**	Have a written contingency plan that works. Determine what to do in the event of a loss or shutdown of your facilities. Include plans to restore operations as quickly as possible. Test the effective-ness of your plan.
□	**Create Guidelines**	Create and enforce an internet email usage policy, including social media. Employees who inappropriate-ly place comments in social media that relate to clients, customers, other employees, competitors or other third parties can provoke lawsuits against the organization. Employee posts on social media may also ex-pose a firm to fines and penalties brought by the FTC and other governmental entities.
□	**Develop Website Linking Agreements**	Agreement with hyperlinked sites should be used to limit exposure for trademark and copyright claims for other websites. Companies need to employ warnings, disclaimers, and indemnification agreements aimed at limiting exposure for claims arising from information on hyperlinked websites.
□	**Curtail Collection of Online Data**	Web servers routinely retain information regarding website visitors' personal information. Knowing what information is being collected and stored—and minimize the extent of both to go a long way in mitigating privacy claims down the road.

A comprehensive cyber insurance policy can protect against financial losses but implementing preventative measures will help reduce any loss and the premium you will pay for such a policy.

About Roanoke Trade

Roanoke Trade, a division of Roanoke Insurance Group and part of Munich Re Specialty Group Ltd., operates as a specialty insurance broker focused on surety and insurance solutions for transportation intermediaries, 3PLs, customs brokers and companies with supply chains, and is a leading provider of customs bonds, marine cargo insurance and ATA Carnets for the industry.

Contact Roanoke Trade To See The Value Of Cyber Liability Coverage

www.RoanokeTrade.com

1.800.ROANOKE

infospot@roanokegroup.com