TRADE ROANOKE

You've Been Hacked! Now What?

Computer security experts joke that there are only two types of companies: those that know they've been hacked, and those that will be hacked. Considering that the data for just one shipment may pass through multiple PCs, websites, servers, clouds and third party vendors; transportation and logistics companies are exposed to data breaches throughout their business activities. It should come as no surprise that some of your industry associates have also become victims of computer hackers with some companies spending over $100,000 to address and resolve the problem.

A recent example is that of a logistics company whose CEO sent the CFO an email with wire instructions to send $25,000 to an account in Russia, purportedly one of their vendors. The CFO arranged the wire and sent off the $25,000 as requested. Unfortunately, the email request was not actually made by the CEO. A hacker gained access to their email server and sent the phony email. That hacker is now $25,000 richer since both banks involved refused to accept any liability.

While the insurance industry is historically cautious in creating new products for new exposures, Cyber Liability Insurance is a relatively new insurance policy that's becoming more affordable to logistics companies. Electronic data breach is not covered under a Business Package policy because it's designed to cover tangible assets only. Likewise, Errors and Omissions coverage will not respond unless the loss is caused by an error or mistake that you make. A Cyber Liability policy is written specifically to address several aspects of financial loss due to electronic data breach.

While Cyber Liability coverage can be customized to suit your specific needs, there are seven aspects of coverage that a logistics company should consider:

1. Data Loss Coverage: this covers the financial loss of recreating data that has been lost or corrupted.

2. Notification Expenses: most states have specific laws that require you to notify parties of the loss of their data. Some laws even go so far as to require that you pay for credit monitoring as well.

3. Regulatory Investigation Expense: many regulatory agencies have an interest in keeping your customers' data secure The State Department, TSA, CBP and Bureau of Industry and Security, just to name a few, may investigate following a data breach.

4. Public Relations: coverage is available for damage control following a data breach and can include marketing costs.

5. Business Interruption: lost revenue due to data breach, hacking or even a virus can be covered.

6. Content Liability: covers intellectual property claims and/or slander.

7. Data Loss in Transit: coverage is available to logistics providers who are engaged in the transport of computer or data storage devices loaded with data. This component covers the financial loss to the cargo owner or third party following a theft, misrouting or other loss of the device.

1475 East Woodfield Road, Schaumburg, IL Suite 500 60173-4903 USA
Toll-Free in the US: +1-800-ROANOKE | Fax: +1-847-969-8200
Visit us at www.RoanokeTrade.com or email us at infospot@roanokegroup.com
Providing insurance brokerage and surety solutions as a division of Roanoke Insurance Group Inc.

Your insurance provider should be able to offer various options for covering this exposure, but keep in mind there are many ways to proactively reduce your exposure. Here are a few suggestions:

- Consider the extent of your cyber exposure and how to proactively minimize the risk of data breach. Data is not just what's in your customer file, but includes employee information such as social security numbers, retirement accounts, health insurance records, etc.
- Create and reinforce a workplace internet usage policy for staff and restrict unauthorized downloading of software and apps.
- Review web hosting, software and data storage vendor contracts to ensure they have an action plan in place in the event of a breach. Ask for proof of Cyber Liability and Professional Liability Insurance naming your company as Additional Insured.
- Review your own terms and conditions of service and consult with counsel as to whether they should be updated to address electronic data transfer and data collection of client information.
- Discuss your cyber liability exposures with your insurance advisor and consider some of the cyber liability insurance products that are available.