CRIME, SECURITY AND LIABILITY

Project Cargo Firms Exposed to Cyberattacks

Transportation and logistics professionals increasingly use automation to expedite the everyday process of moving cargo through the supply chain. What were once time-consuming, tedious and manual processes are now completed with the touch of a button.

BY LA DONNA LOGAN
ROANOKE TRADE

Improved computers, high-speed internet and ever-changing software integrations make it all happen. In today's automated environment, you can track and locate freight faster than you can dial the number of the carrier handling the move. However, as with all luxuries, these time-saving tools come at a cost.

When data is transferred through the supply chain, it may pass through numerous websites, servers, PCs, clouds and third-party vendors, which expose each company involved to potential data breaches. Just consider how many emails alone are sent externally over the course of one shipment. In addition, the advances in technology that allow live tracking and tracing capabilities (bar codes, RFID tags and GPS, for example) also allow thieves access to that same information. The data spans companies and countries and regardless of protocols and security measures each company has taken, no system is impervious to a cyberattack. In the project cargo industry, a data breach can occur anywhere and anytime.

Data thieves are relentless and their attacks have become more sophisticated and include the use of malware, multiple forms of intrusive and malicious software and email scams. While certain malware attacks have been reduced due to the addition of spam filters, ransomware is still problematic.

Ransomware is embedded in an email attachment or hyperlink which seems legitimate, but when opened, it encrypts digital files and demands a ransom, usually via bitcoin, to release them. It is untraceable and there is no guarantee of the return of your files should the ransom be paid.

Business email compromise scams are more difficult to recognize as attachments are not required, it is simply a conversation from a recognized internal email address. Cyber criminals use company websites and social media to access specific information and the company's hierarchy. An email from someone with an important title making an urgent request is often successful, as the thieves use psychological manipulation combined with a sense of urgency.

LIMIT EXPOSURE

Understanding exposure to cyber crime and ensuing liability is vital for a company. Whether it is a computer virus, a stolen laptop or theft of confidential information from a company server, if a data breach results in the theft and/or use of intellectual property, a business can expect considerable financial losses. These incidents may initiate a regulatory investigation, require the need for forensic analysis as well as generate claims for expenses and losses. There is also potential for business interruption expenses, crisis management and legal defense. While working through the breach, the uncomfortable task of notifying all affected parties may be also required.

Cyber crime will continue and cyber security is not guaranteed, therefore cyber liability is something each link in the project cargo supply chain should guard against. This carries true for forwarders, shippers, vendors, carriers and anyone else who has a hand in the shipment regardless of the magnitude of involvement.

Multiple U.S. government agencies as well as foreign governments have special divisions solely focused on cyber crime. One agency advises to have procedures in place that include training employees to understand how to recognize a potential threat and what measures to take if one occurs. They also recommend IT departments should have prevention controls in place and continually monitor activity.

Another agency has a division dedicated to cyber insurance, as each company must protect themselves in the event you become a victim of a data breach. This form of coverage is crucial due to the effects a data breach will have on your company. Every company has exposure, therefore making sure you have sufficient measures in place to protect against an attack and any fallout will provide both protection and coverage. **BB**

La Donna Logan is marine manager at Roanoke Trade, a division of Roanoke Insurance Group Inc., specializing in insurance and bond services for international trade and transportation.