ROANOKE
SERVING THE USA & CANADA

WHITEPAPER

THE PATH TO IMPLEMENTING A SOUND CYBER RISK MANAGEMENT PLAN

Helping You Navigate Today's Cyber Exposures

The transportation, trade and logistics sector, like any other industry vertical, has been hit by ransomware, social engineering and other cyber threats. These threats upend operations and increase the total cost of risk for companies. In fact, transportation ranks among the top five industry sectors vulnerable to ransomware. There are several reasons why the transportation and logistics sector is so cyber-exposed, including its dependency upon third-party networks; the speed with which logistics transactions are conducted; the number of stakeholders involved in sharing information; and the potential access to confidential and sensitive financial, employment and intellectual property records.

Without a sound cyber risk management plan in place that includes cyber security measures, cyber support services, and cyber insurance, navigating today's threats may leave your operation stranded and paying out hundreds of thousands of dollars in out-of-pocket expenses.

Ransomware Is Rampant

The leading cause of cyber risks today is ransomware – a form of malware that prevents users from accessing theircomputer system or files until a ransom is paid. Moreover, cybercriminals don't discriminate when it comes to their targets– any business size or industry sector is vulnerable. Additionally, cybercriminals are continually changing up their tactics to find ways to attack, with businesses always playing defense. According to recent reports, the average bitcoin (digital money) demand in a ransomware event is $175,000, triple the amount from 2019. The payout in a typical average ransomware case for the transportation and logistics industry was about $138,000. Business interruption losses on average cost $435,000.

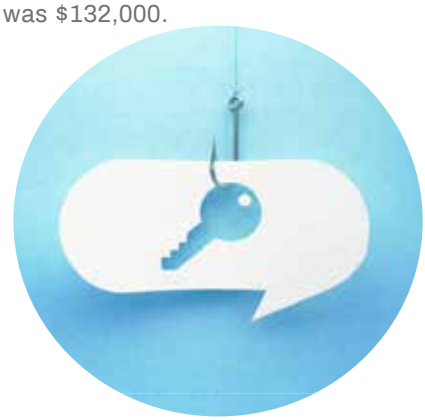
Because logistics service providers (LSPs), customs brokers, freight forwards and others are an integral part of the supply chain, freezing their business has an expensive ripple effect on trade. Cybercriminals understand that if they can manage to interrupt any aspect of the supply chain, they will reap financial benefits. Stakeholders will pay the ransom relatively quickly to get the goods moving again. The more time the supply chain is down, the more income is lost.

Social Engineering Designed For Fraudulent Wire Transfers

Social engineering tactics, which include business email compromise (BEC), are also on the rise. BECs involve scammers who target employees with access to company finances and trick them into making wire transfers to bank accounts thought to belong to trusted partners. The money, however, ends up in accounts controlled by criminals. Again, criminal organizations that perpetrate these frauds are continually honing their techniques to exploit unsuspecting victims. The average BEC loss for a small to medium enterprise (SME) in the past year was $132,000.

Phishing Scams

Phishing scams have increased during the pandemic. Phishing involves bad actors trying to trick people into doing something via an email that enables the attacker to hack a target. For example, at the onset of the pandemic, emails were sent to employees posing as the company's IT staff to manipulate individuals into visiting a malicious link concerning COVID-19 and its effect on payroll. Cybercriminals were also creating schemes around the economic stimulus checks small businesses received from the U.S. government.



Theft Of Confidential Records

The theft of financial records for monetary gain is among the other cyber exposures transportation companies face. Considerable information is being stored by logistics service providers, freight forwarders and brokers, making the industry a prime target for today's criminals. Earlier this year, for instance, a freight brokerage firm suffered a massive breach involving the theft of its customers' banking information, Social Security numbers and other confidential information. The bad actors used the account information to falsify fraudulent transactions, which resulted in a significant class-action lawsuit against the brokerage firm by its clients.

The average BEC loss for a small to medium enterprise in the past year was

$132,000.

Mitigating Risk: A Complete Information Security Program

The first course of action to help mitigate the risk of a cyberattack is to recognize your firm is a target and to be prepared:

- **Implement a foundational information security program.** This program should follow cyber security standards set forth by the National Institute of Standards and Technology (NIST).
- **Put into writing your data privacy** and information security procedures and processes and share them with all employees and third-party vendors. Assess how much data you're collecting and storing and your data access capability to implement strong data-protection processes.
- **Effectively manage your third-party vendors** and the contracts with each of them to limit your liability regarding data privacy and data security. Vendors should pay for a breach to the extent they have contributed to it.
- **Implement a robust endpoint monitoring tool** to identify malicious behaviors and to detect, quarantine, eradicate, and then limit the nature of the incident and get the company up and running, or prevent cybercriminals from shutting your system down in the first place.
- **Ensure viable backups** of your data exist so you can restore the data and minimize the duration of your business interruption. Research indicates following a ransomware attack, a company can experience three to 15 days of interrupted business. The general rule of thumb is the 3-2-1 backup strategy: organizations should keep three backups, on two different storage mediums, with one being disconnected/offline/off site.
- **Educate employees** on an ongoing basis. Your perimeter is only as strong as what's inside. Inform and bring awareness to employees on what to look for to prevent phishing attacks, wrongful release of funds and other criminal cyberattacks. Provide real-life examples in simulated phishing tests. Advise employees to be suspicious of links. If it doesn't look right, doesn't feel right, avoid clicking on a link. Most importantly, stress that employees should ask questions before carrying out a request.
- **Make sure you have a fluid incident response plan** and that everyone throughout the organization recognizes his or her roles and responsibilities in the plan.

THE ROLE OF CYBER INSURANCE

Cybersecurity also involves cyber consulting services and a cyber insurance program. Ensure you have an industry-specific cyber policy in place with specific services available and the insurance coverages required to address cyber exposures.

Consulting Services

- **The support of a cyber coach** to help you with a strong response plan and to navigate the steps in the aftermath of an incident – from notification compliance to client and vendor communication and crisis management.
- **Outside counsel** to help you with the services provided by a forensics firm in identifying the cause and extent of the incident and minimizing or stopping it. Without a thorough forensics assessment to determine how the incident occurred, cybercriminals will be able to strike again.
- **Expertise in ensuring regulatory compliance**, including complying with state notification laws and ransom payments. Treasury laws prevent ransom payments to individuals on the sanction list.
- **Communication and negotiation with the cybercriminals** in the event of a ransomware attack. Keep each of the stakeholders involved, including the insurance carrier, apprised of developments.
- **Rebuilding** the attacked system.
- **Assistance with third-party messaging** to help with reputational damage.

Cyber Insurance Coverages

Transportation and logistics cyber-specific insurance coverages should include the following:

- **Business Interruption** – Covers loss of income for a cyber event occurring within your own network as well as that of an outsourced technology vendor. If a network you are dependent upon goes down, you will be covered for your loss.
- **Cyber Crime** – Covers transfer of funds to a third-party as a direct result of a fraudulent written, electronic or telephone instruction designed to mislead the company. In addition, covers fraud as a result of invoice manipulation. You will be reimbursed for lost funds from fake invoices.
- **Extortion & Ransomware** – Covers the costs involved in ransom demands and the expenses to mitigate an extortion attempt of disclosing, encrypting, or theft of data by an extortionist.
- **Data Access & Business Interruption** – Covers the costs of cyber events affecting your customers, employees and vendors who may incur financial loss due to a data breach or other cyber event caused by you.
- **Data Loss & Restoration** – Covers the costs to regain, repair, restore or recreate damaged, lost or destroyed data. Even if your data is backed up, there is a significant expense in getting the data to fit your upgraded system or to be integrated into a third-party system.
- **Data Incident Response** – Covers reasonable expenses for professional crisis management and PR costs, forensic fees, and legal and consulting fees to limit further loss. Also, covers the costs to manage statutory requirements, notification costs, and credit monitoring services as a result of your firm's improper use of personal data or resulting from any theft, loss, or unauthorized disclosure of personal data in your care, custody or control.

Cyber risks for business are on the rise, with 81% of large businesses and 68% of small businesses suffering a cybersecurity attack in the year 2020. The transportation, trade, and logistics sector in particular has been targeted by cyber criminals and requires a robust cyber insurance and risk management solution. Roanoke offers Logistics CyberSuite™, which is designed to provide transportation companies with the cyber solutions they need.

About Roanoke

Roanoke Insurance Group Inc., is a specialty insurance broker focused on surety bond and insurance solutions for logistics service providers, customs brokers and companies managing supply chains. Founded in 1935, Roanoke was the first provider of customs import bonds as well as the first appointed ATA Carnet provider in the United States. Roanoke has decades of partnership with the trade community as a trusted provider of insurance, surety bonds, ATA Carnet products and specialty services.

800-762-6653 infospot@roanokegroup.com www.roanokegroup.com