




# Logistics Cybersuite™

A Comprehensive Approach To  
Managing The Risk Of Cyber-attacks  
For Logistics Service Providers

## Developed for Logistics Specialists by Logistics Insurance Specialists

Tailor made for our clients, Logistics CyberSuite™ is much more than an insurance a policy. This exclusive cyber program was developed for logistics specialists by logistics insurance specialists. It is a unique suite of coverages, risk management tools and resources to help you prepare for and financially overcome a cyber incident. Take a tour of the Logistics CyberSuite™ below.

Coverage Description	Why You Need It	How Coverage Responds
<p><b>*Third Party Network Coverage</b></p> 	<p>The logistics industry is dependent upon third party networks such as hosted transportation or freight management systems, load boards and other electronic data interface systems. In order to continue normal operations it is imperative that their systems remain online and operable. But what happens when they suffer a cyber incident and go down?</p>	<p>Should one of these critical partners suffer a cyber incident and negatively impact your operations, this coverage responds to your claim for a business income loss. Most Cyber policies limit coverage to your own network, so this is a significant coverage extension for any industry that relies upon third party networks.</p>
<p><b>*Cyber Crime &amp; Social Engineering Insurance Coverage</b></p> 	<p>Social engineering is a type of cybercrime that occurs when a target is manipulated into divulging confidential and/or sensitive information. Phishing attacks are a social engineering tactic in which cyber criminals use email, text and telephone messages from someone that appears to be a legitimate contact to lure the target into giving them the information they seek or even to make payment to a fraudulent account. This type of fraudulent payment loss is referred to as a "voluntary parting of funds".</p>	<p>This coverage responds when your employees accidentally release funds to fraudulent requests. This policy pays up to \$100,000 in response to a social engineering loss of this type. Many employee crime policies either exclude this completely or offer a much lower limit. This policy covers losses that may occur both within and outside of your computer network. Outside network losses are typically excluded in other cyber policies.</p>
<p><b>Extortion &amp; Ransomware</b></p> 	<p>Cyber criminals use ransomware to infect a target's system and hold that business hostage until their demands for payment are met. Payment demands vary from hundreds to millions of dollars. Until the ransom is paid, businesses are also exposed to loss of sensitive information and downtime.</p>	<p>Coverage pays ransom demands as well as additional expenses to mitigate the attempted extortion which may take the form of theft, exposure or encryption of data. A Cyber Breach Coach Team will manage the process and help you navigate the situation. In addition, any payments to cyber criminals for ransomware are handled legally and in accordance with OFAC regulations.</p>
<p><b>Data Loss &amp; Restoration</b></p> 	<p>"Data loss" refers to data that has become corrupted or deleted by accident. The average downtime for this type of loss is three days but can be much longer depending on the scope of loss. Businesses that suffer a data loss must expend time and resources to recover the lost data. The primary causes of data loss are human error, software corruption, theft, computer viruses and hardware destruction.</p>	<p>Coverage applies to the expenses to regain, repair, restore or recreate damaged, lost or destroyed data. The cost to recover and/or recreate data can be extremely high.</p>
<p><b>Data Privacy, Security &amp; Confidentiality Liability</b></p> 	<p>If your business suffers a data breach, it could compromise data entrusted to you by customers and employees. As the business owner, you may be viewed as responsible for not properly safeguarding their confidential information and potentially subject to lawsuits.</p>	<p>Coverage pays ransom demands as well as additional expenses to mitigate the attempted extortion which may take the form of theft, exposure or encryption of data. A Cyber Breach Coach Team will manage the process and help you navigate the situation. In addition, any payments to cyber criminals for ransomware are handled legally and in accordance with OFAC regulations.</p>

\*These are special coverage provisions unique to the Logistics CyberSuite™ program and generally not included in mainstream cyber insurance policies.

Logistics CyberSuite™ is underwritten by Munich Re Syndicate Ltd., combining technical expertise, risk management services, responsive claims support with the financial stability of Lloyd's. The descriptions of coverage are generalized and are subject to the specific policy's terms, conditions and exclusions. For full coverage details, please refer to the actual policy forms and terms and conditions.



Since COVID-19,  
the US FBI reported a  
**300% increase**  
in reported cybercrimes

## Cyber Risk Report Card

We utilize a leading-edge analytics platform to access your publicly available information from your website, connected networks, and company digital footprint to assess your specific cyber exposures and rank them based on overall risk. The report also includes a cyber breach financial loss calculator that provides an estimate of the hard costs involved following a cyber breach.

Business owners, risk managers and IT managers can use this information to learn the answers to three critical questions:

- 1 What is my risk level?
- 2 Where do the threats come from?
- 3 What actions should I take?

## eRisk Hub

eRisk Hub is an online portal that features a collection of educational and technical resources to help policyholders understand their exposures, establish a response plan and minimize the effects of a breach.

### Incident Response Plans

Guides and checklists to walk you through one of the most important aspects of handling any cyber incident.

### Training

Security awareness training tools, best practice guides and sample compliance and risk management policies.

### Threat Intelligence

A weekly review of worldwide cyber-attacks and emerging threats for internal IT security teams to review and take action when needed.

## Breach Coach Service

This invaluable service removes the guess work from planning for a cyber incident. Policy holders have access to pre-incident consultation to ensure you are positioned with best practices to lessen the chances of a breach.

Should a cyber incident occur, a breach coach can help you manage the incident from notification compliance to client and vendor communications and crisis management support. Services provided by leading breach response firm Lewis Brisbois Bisgaard & Smith.

## About Roanoke

Roanoke Insurance Group Inc., a Munich Re company, 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.



Contact us today to  
protect your business  
from cybercrimes

800-762-6653  
[www.roanokegroup.com](http://www.roanokegroup.com)  
[infospot@roanokegroup.com](mailto:infospot@roanokegroup.com)