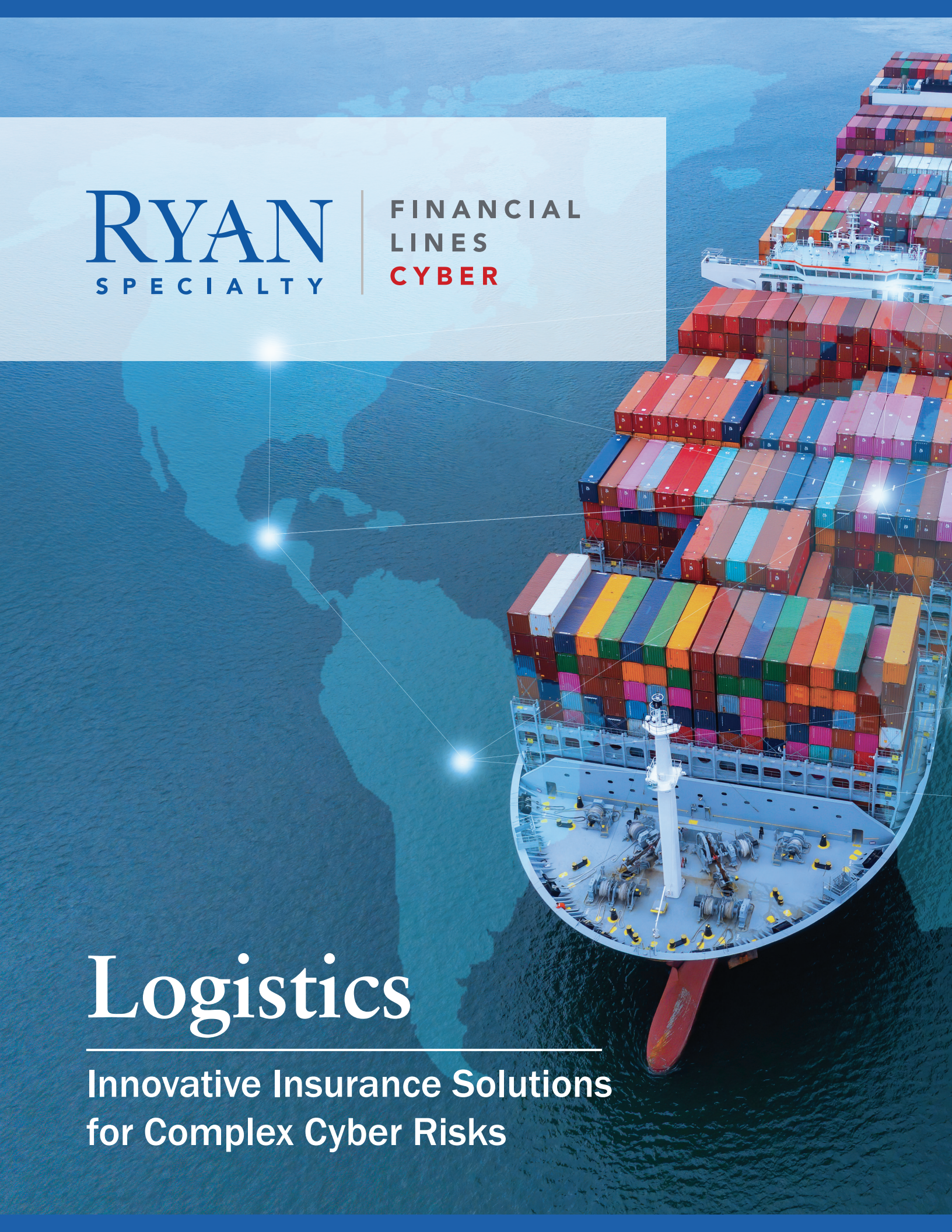
RYAN SPECIALTY

FINANCIAL LINES CYBER



Logistics

Innovative Insurance Solutions for Complex Cyber Risks

RYAN SPECIALTY | FINANCIAL LINES CYBER

Tech is necessary.

The logistics industry is undergoing a digital transformation like many others, driven by the seamless integration of technology into daily workflows. The infusion of emerging technology into critical business processes is vital for the efficient management of complex operations. A surge of innovative initiatives—ranging from automation and predictive maintenance to IoT applications and intelligent transport systems—are revolutionizing the sector. These advancements optimize route efficiency, enable demand-based supply, and significantly enhance overall efficiency while minimizing waste. It's evident that technology has become indispensable in the day-to-day operations of the logistics industry.

Tech has risks.

While most logistics companies primarily focus on the movement of goods and may not handle very large volumes of sensitive consumer data, some logistics companies also specialize in the transfer of sensitive information or process payments via credit cards. Especially in these cases, it's crucial to safeguard any sensitive data with robust, up-to-date network security controls and stringent security procedures. Cybercriminals target all industries, and unfortunately, no one is immune to their attacks. Ensuring comprehensive cybersecurity measures is essential to protect against potential threats.

As tech use increases, risks are increasing too.

Logistics organizations face significant risk exposure as they keep up with the relentless pressure to meet global demand for materials and finished goods. They must maintain sophisticated systems to streamline their processes, whether managing today's dominating e-commerce delivery requests from retailers, or providing essential delivery services for other industries, including healthcare and manufacturing. Logistics companies are pivotal in sustaining societies worldwide, so in today's environment, supply chain management is not only challenging but also continuous. To minimize costs and meet demand, logistics companies fundamentally rely on technology, and any disruption to these around-the-clock business operations can have devastating effects, extending far beyond the logistics industry alone.

For the logistics industry, increased use of technology applications can be essential for supply chain efficiency, including:

Software-as-a-Service (SaaS) applications have increasingly become part of the supply chain management process, offering a range of routing solutions from the warehouse to the end-buyer.

Transportation Management Systems (TMS) are software systems that facilitate interactions between the organization's orders, and the process used to dispatch products to their final destination.

Warehouse Management Systems (WMS) optimize warehouse operations by overseeing inventory tracking, streamlining the receipt and placement of goods, assisting with picking and packing for shipping, and monitoring worker productivity.

Inventory Management Systems offer features like demand forecasting, reorder point notifications, and multi-location management, often integrating with tools such as barcoding and REID for accurate tracking.

Supply Chain Management (SCM) Software manages the broader spectrum of a company's supply chain, coordinating with suppliers, handling procurement, and providing real-time inventory visibility.

Fleet Management Systems focus on vehicle maintenance, fuel management, driver monitoring, and GPS-based route planning for companies with fleets of vehicles.

Route Optimization Software ensures delivery routes are efficient and on time, adapting to real-time conditions and using predictive analytics to optimize multi-stop deliveries.

Cargo and Freight Tracking Apps provide stakeholders with real-time updates on shipments, using GPS for location tracking and offering features like temperature monitoring for sensitive cargo.

Enterprise Resources Planning (ERP) unify core business processes such as accounting, HR, finance, and sales into one system, providing complete visibility and automating manual tasks.

These applications are engineered to increase productivity and decrease costs. However, if a system failure occurs at any point, a logistics company could find themselves with the sudden costs of both dealing with resolving an individual system failure as quickly as possible and additionally needing to manually overhaul their technological processes to address underlying system issues.

Logistics companies also face significant threats from failures in electronic navigation devices that use **Global Positioning Systems (GPS)**. Some transportation modes lack sophisticated backup systems to track their fleets, and this increases a logistic company's vulnerability to operational disruptions in the event their primary navigation device fails, forcing them to rely on potentially less efficient secondary systems, if available. Transitioning between systems can be time-consuming, leading to periods where the location of stock and vehicles is unknown, causing delays and other problems fulfilling service agreements. Additionally, physical events such as crashes become a concern if the electronic navigation system fails, potentially resulting in physical injury, property damage, or even total loss of cargo.

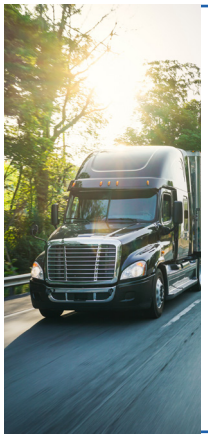
Illustrative Loss Scenarios

Business Interruption

A logistics company was managing the supply chain process for a large supermarket chain. The stock was in the warehouse when their transportation management system experienced a system failure. Route scheduling and transportation management could not be performed by the software, so an alternative solution was implemented. This alternative solution required additional time to process. The stock was delivered late and the supermarket sued the logistics company for breach of contractual duty to deliver the stock in time and for loss of their own revenue as a result of not having the stock.

Ransomware

A logistics company's main portal experienced network failure due to a NotPetya cyberattack, ransomware attack prohibiting accessing to data until 300 bitcoin ransom demand had been paid. The ransomware exploited a vulnerability in Microsoft Windows. This event meant that the company was unable to accept new orders during this time and terminals (independent terminal operating division) were unable to operate causing delivery delays. The company estimates a $300 million in loss of revenue and over 150 hours that the systems were down.



Business Interruption

The majority of logistics companies rely on heavy semi-trucks to deliver goods. Most modern heavy-duty trucks use the SAE J1939 for their internal networks. The system is used to electronically control the drivetrain components of a vehicle for safety, fuel efficiency, etc. An instrument cluster attack allowed an attacker to control the brake pressure halting all trucks in motion and companies do not receive their goods on time.

These examples are hypothetical scenarios used solely to illustrate potential outcomes and not reflective of policy terms and conditions or the facts of a specific claim.

RFL's Cyber Solution

RFL's policy was created to address cyber as a peril, considering how data and technology systems can cause a wide array of operational challenges. Addressing areas such as business interruption, data restoration, computer crime, social engineering, extortion, and privacy breaches, RFL's policy is here to help your clients in a time of crisis. Our leading-edge proposition is a blend of 1st party cost reimbursement and 3rd party defence and regulatory coverage, aided by our broad definitions of data and computer systems.

1ST PARTY

Crisis Response: Intended to help mitigate the costs and expenses to respond to a system event or privacy breach event

Cyber Extortion: Intended to help mitigate the costs and expenses to respond and resolve an extortion demand that threatens to release or destroy data and/or disrupt or damage the computer system

Computer System Interruption: Intended to help mitigate the net income losses and additional operating costs that occur during a business interruption event due to systems and/or data being taken offline in a malicious attack or other operational failure. Coverage may include:

- Renting, leasing or hiring external equipment to reduce the duration of a material interruption
- Additional operating costs including services, premises, employing contract staff, and overtime cost
- Costs to switch service from a named IT vendor to a new provider if the service cannot be restored within the indemnity period (when event is caused by vendor systems)
- Procuring product or services from alternative sources to meet contractual obligations in supplying the insured's customers
- Paying any service credits or contractual penalties that the insured is contractually required to pay as a result of a material interruption

Reputational Damage: Intended to help mitigate the loss of net income due to a reduction in business or the loss of a service contract with a client in the wake of the public being notified of a system event, privacy breach event, or network security event

Fraud and Social Engineering: Intended to help mitigate the direct financial loss from the wrongful transfer of money by fraudulently accessing the computer system or intentionally misleading an authorized person to transfer funds to a third party purporting to be a vendor, client, or employee. This cover also extends to the financial loss arising from the unauthorized access of a client's telecommunication system by a malicious third party

Data & Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading/replacing affected software applications or equipment

3RD PARTY

Privacy Breach and Other Third-Party Liability: Intended to help mitigate the defence costs and damages arising from:

- Unauthorized disclosure or access to personal or confidential corporate data
- Liability that arises from other cyber events such as the transmission of a malicious code, contract breaches due to a BI event, and unauthorized access to data by a third party

RYAN SPECIALTY | FINANCIAL LINES CYBER

Vendors

Privacy Counsel: US

Pierson Ferdinand LLP

Incident reporting:

RFLCyber@pierfed.com

833-737-7444

Alternate counsel options:

McDonald Hopkins LLC

Cipriani & Werner, PC

Mullen Coughlin

Wood Smith Henning & Berman LLP

Privacy Counsel: Intl.

Kennedys Law LLP

Incident reporting:

RyanFinLinesIR@kennedyslaw.com

UK/EMEA- +44 203 137 8749

AUS/APAC- +613 9498 6688

Alternate counsel options:

Weightmans LLP

Pinsent Masons LLP

Forensics: US

CyXcel

S-RM

Kroll

IronGate

CrowdStrike

PNG Cyber

Palo Alto -Unit 42

Forensics: Intl.

CyXcel

S-RM

Data Mining

Asceris

Consilio

CyXcel

Epiq

Notifications

Epiq

IDX

Kroll

Please note that the use of these vendors is subject to the terms, conditions, and reporting requirements outlined in your policy. We reserve the right to amend our vendor panel at any time.

Who We Are

Ryan Financial Lines (RFL) was formed in March 2024 to offer clients a wide-ranging, single platform of financial lines insurance products. Ryan Financial Lines brings together the Management and Professional Liability talent at Ryan Specialty Underwriting Managers to provide greater synergies and efficiencies that further enhance risk management solutions and services for our clients and carriers. This unified approach brings together our expansive network of expertise with more than 70 teammates located across key territories, including North America, United Kingdom, Europe and Latin America.

ryanfinlines.com

US: RFL-US-Cyber@ryanfinlines.com | International: RFL-UK-Cyber@ryanfinlines.com