RYAN SPECIALTY

FINANCIAL LINES CYBER

Retail Store Industry

Innovative Insurance Solutions for Complex Cyber Risks

RYAN SPECIALTY | FINANCIAL LINES CYBER

Cyber Exposures for the Retail Store Industry

Shopping Meets Tech

The retail store industry has undergone a dramatic transformation over the past 15 years, becoming almost entirely reliant on technology. From point-of-sale (POS) systems and inventory management tools to e-commerce platforms and delivery services, digital infrastructure now powers nearly every aspect of retail operations.

As this digital footprint expands, so does the threat landscape. Ransomware and cyber extortion have emerged as fast-growing risks, targeting retailers' critical systems and customer data. To safeguard operations and protect profitability, retail businesses benefit from prioritizing cybersecurity, ensuring their networks are both secure and resilient against disruption. In this article, we address cyber risks that can affect any retailer, from large department stores to small bodegas.

Data Privacy Issues

While ransomware dominates headlines, privacy remains one of the most critical exposures for retail businesses. With vast volumes of personally identifiable information (PII) and payment card information (PCI) being processed, either directly or through third parties, retailers remain prime targets for cybercriminals. Regardless of who handles the data, the consumer-facing entity will be impacted by any cyber breach.

High-profile breaches at companies like Target, Home Depot, and Staples have underscored the reputational and financial damage that can follow a security lapse. A single breach can erode customer trust and significantly impact revenue.

One of the most alarming threats today is double-extortion ransomware. Attackers not only encrypt systems and demand payment, but also exfiltrate sensitive data, threatening to leak it unless a second ransom is paid. Given their reliance on technology and the volume of sensitive data they hold, retailers are especially vulnerable. Robust data protection protocols, proactive security measures and incident response planning can be essential to mitigate these risks and protect both brand and bottom line.

Business Interruption Risks

Business interruption now rivals privacy breaches as one of the most damaging risks facing retailers. With operations increasingly dependent on technology, from inventory management and e-commerce to logistics, procurement, POS systems, and customer analytics, any system failure or cyber incident can bring operations to a halt.

While these technologies have driven efficiency, reduced costs and minimized errors, they have also introduced new critical points of failure. A single disruption can severely impact financial performance and brand reputation. That's why having robust business continuity, backup and recovery plans can be essential to maintaining resilience and minimizing downtime.

Why Cyber Coverage is Beneficial

Even with strong controls and thorough preparation, cyber incidents can still happen. When they do, cyber insurance can provide critical financial support, helping to significantly reduce the impact of data breaches or network disruptions and helping enable faster recovery with less financial strain.

Illustrative Loss Scenarios

THEFT OF PCI DATA

Retail business has one periphery device that still uses the default manufacturer password. Hacker finds this weakness and uses it to gain access to the network. Once inside the Common Desktop Environment (CDE), the attacker takes control of a domain controller and installs malware allowing them to steal credit card data from the POS systems.

RANSOMWARE

A hacker gains access to the network through an unpatched software vulnerability and deploys ransomware. Computer systems are down, causing the retailer to not be able to process sales or maintain correct levels of inventory. After the company pays to decrypt the systems, the hacker reveals they have stolen 200GB of PCI data and are threatening to post the information on the internet if the company does not pay another ransom.

SYSTEM FAILURE

Company performs a POS system upgrade, and due to an error in implementation, the system unexpectedly goes down for one week while the company attempts to get back up and running. During this time, the retailer can only accept cash, loses customers to other stores and suffers significant business interruption and loss of reputation.

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

Ryan Financial Lines' (RFL) policy was created to look at cyber as a peril, considering how data and systems can cause a wide array of operational challenges. Covering business interruption, data restoration, computer crime and social engineering, extortion and privacy breaches, RFL's policy is here to help in a time of crisis. Our best-in-class proposition is a blend of 1st party cost reimbursement and 3rd party defence and regulatory coverage, aided by our broad definition 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 and Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading or 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:

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

Vendors

In a time of crisis, RFL wants insureds to have access to best-in-class vendors and for the claims process to be as easy to execute as possible. RFL's cyber solution not only provides insureds with breach response options but also aligns them with resources to help limit their exposure to cyber events and to help minimize the fallout if they do experience a cyber event.

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 Networks - Unit 42

Data Mining

CyXcel

Consilio

Asceris

Epiq

Notifications

IDX

Epiq

Kroll

Forensics: Intl.

CyXcel

S-RM

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