



CYBER PRACTICE

Addressing Cyber Risks in the Retail, Wholesale, Food and Beverage Industry

From artificial intelligence and the Internet of Things, to robotics and industrial automation, retailers, wholesalers, and food and beverage companies are increasingly embracing new technologies to power operations, drive efficiencies, and enhance the customer experience.

While innovative technologies are transforming industry business models, they are also creating new risk exposures and points of vulnerability for actors to access and impair critical systems, networks, and hardware. And the ubiquitous use of mobile apps and devices is driving an ever-higher volume of transactions and customer data across the internet and through retailer systems, increasing opportunities for data breach and theft.

Such breaches and technology outages can disrupt critical operations and supply chains, resulting in significant revenue loss, expenses, and reputational damage.

Marsh's Cyber Risk Management Solutions

Marsh's suite of market-leading analytics can help retailers, wholesalers, and food and beverage companies understand

and measure your cyber exposure and evaluate your insurance needs. We then design best-in-class cyber risk management solutions tailored to your specific risk profile and goals.

Quantifying Cyber Risk to Optimize Investments

Effective cyber risk management starts with a thorough understanding of your organization's risks, including quantified measurement of the potential financial impact of cyber events. Quantification expresses the threat in economic terms, enabling a dollar-based comparison of cyber risk against other organizational risks. It also allows you to measure the effectiveness of your cyber risk investments. This helps you optimize cyber risk capital allocation, and informs decision-making about the coverages and limits of your cyber insurance program.

🎯 WHO IT'S FOR

Any retailer, wholesaler, or food and beverage company that either:

- Uses the internet or technology in its business.
- Handles or collects customer data.

✔️ WHAT YOU GET

Proprietary solutions and best-in-class advisory services to help you:

- Understand the cyber risk landscape and your cyber vulnerabilities and threats.
- Measure your cyber exposure through customized risk quantification and modeling tools.
- Manage your cyber risk through:
 - Tailored insurance solutions that align with existing policies.
 - Education and coaching programs.
 - Risk mitigation and loss prevention tools.
 - Response planning and performance improvement reviews.

Customized Cyber Insurance for Retailers, Wholesalers, and Food and Beverage Companies

Marsh can design customized insurance coverage that provides broad protection for loss and liability arising out of the use of technology and data in retail, wholesale, and food and beverage operations.

First-Party Cyber Coverages

- **Business interruption/extra expense:** Reimbursement for lost revenue and expenses caused by a technology failure, computer system outage, or cyber-attack, with the option to include:
 - Contingent business interruption resulting from a third-party/supply chain event.
 - Internet of Things products/services used in distribution, inventory, and warehouse operations.
- **Information asset protection:** Costs to recreate or reconfigure information and electronic data assets, with option to include cost to replace hardware or to rebuild systems.

- **Breach/event management:** Costs for notification and investigation of privacy and security breaches, including legal and forensic services, with the option to include losses from unauthorized price alteration.
- **Cyber extortion:** Ransom and investigative expenses associated with threats to steal confidential information, introduce malicious code, corrupt computer systems, or hinder system access.

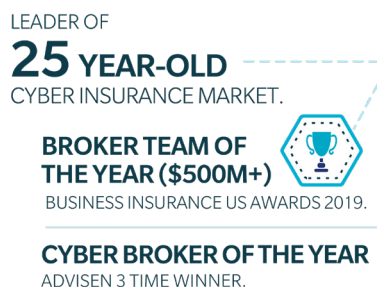
Third-Party Cyber Coverages

- **Privacy liability:** Failure to prevent breaches of confidential personal information — electronic or hard copy — or to disclose an event, with the option to include coupons, discounts, and goodwill payments in settlements and costs.
- **Network security liability:** Actual or alleged failure of computer security to prevent or mitigate an IoT or computer attack.
- **Regulatory Defense:** Costs to defend regulatory actions and for certain fines and penalties.
- **Payment Card Information:** Fines and penalties for PCI industry settlements, fraud recoveries, chargebacks, and forensic investigations.

THE HIGH COST OF CYBER RISKS TO RETAILERS, WHOLESALERS, AND FOOD AND BEVERAGE COMPANIES

Recent events highlight technology, data, and business interruption risks for retailers, wholesalers, and food and beverage firms:

- A national retail chain's fulfillment system failed, leaving it unable to complete customer orders. Full system restoration took more than one month, causing significant revenue loss, extra expenses, and forensic accounting costs.
- A major US restaurant chain suffered a two-phased malware attack affecting more than 1,000 franchisees, resulting in breach response expenses as well as litigation.
- At a retail chain, hackers used stolen credentials to log on to its vendor's online system, then exploited a vulnerability to move into the retailer's corporate system and accessed millions of its customers' payment card data.
- A global wholesaler's network was disabled by ransomware, paralyzing its manufacturing capability for several weeks and resulting in millions of dollars in lost revenue.



For more information, visit marsh.com, contact your Marsh representative, or contact:

MAC NADEL
Retail/Wholesale, Food & Beverage Industry Practice Leader
+1 203 229 6674
mac.d.nadel@marsh.com

SUSAN YOUNG
Senior Vice President
Cyber Center of Excellence
+1 206 214 3161
susan.young@marsh.com

Marsh JLT Specialty is a trade name of Marsh LLC.

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

This document and any recommendations, analysis, or advice provided by Marsh (collectively, the "Marsh Analysis") are not intended to be taken as advice regarding any individual situation and should not be relied upon as such. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party arising out of this publication or any matter contained herein. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, tax, accounting, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. Marsh makes no representation or warranty concerning the application of policy wording or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage. Although Marsh may provide advice and recommendations, all decisions regarding the amount, type or terms of coverage are the ultimate responsibility of the insurance purchaser, who must decide on the specific coverage that is appropriate to its particular circumstances and financial position.