MARSH

Retail/Wholesale Practice • March 2017

TAKING STOCK

RISK MANAGEMENT INSIGHTS FOR THE RETAIL/WHOLESALE INDUSTRY

RETAIL CYBER RISK GOES BEYOND DATA BREACHES

Since the advent of e-commerce, data breaches — and the loss of sensitive customer information — have been among the biggest concerns for retailers. But a growing threat for the industry is the direct harm that a technology outage can cause, including the disruption of normal operations. Although no organization is immune, retailers and wholesalers with retail operations can take steps to minimize their loss of income, reputational damage, and other potential harm from these threats.

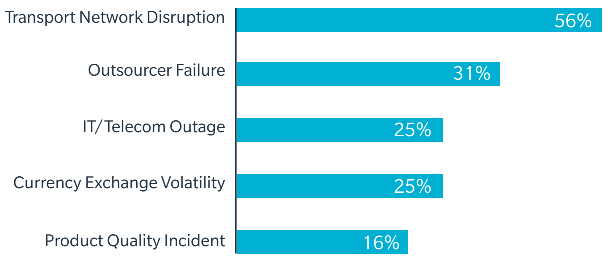
EVOLVING ATTACK METHODS

For many organizations, cyber risk is considered synonymous with data breach. The classic fear for risk professionals: A cyber-attacker compromises a company's firewalls and obtains valuable information about the business and its customers.

For retailers, which typically collect credit card information and other confidential data coveted by hackers, this has represented an especially critical risk. A data breach can lead to significant costs related to remediation, customer notification (along with credit monitoring and identity theft repair services offered to customers), and litigation. Victims of data breaches also face fines and penalties from state federal and industry regulators and reputational costs — including the potential loss of customers' trust and business.

But cyber-attacks have evolved and grown to include far more than data breaches. Meanwhile, businesses — including retailers — have become increasingly reliant on technology. As a result, technology disruption has emerged as a very real threat that equals — or perhaps even surpasses — data breaches and more traditional, tangible disruptions.

Figure 1: Leading Causes of Supply Chain Disruptions, Retail/Wholesale Industry



Source: Business Continuity Institute Supply Chain Resilience Report 2016

In addition to seeking opportunities to steal valuable customer data, cyber-attackers now target businesses themselves, looking for ways to damage systems and disrupt operations. And they've been successful: According to the Business Continuity Institute's

Supply Chain Resilience Report 2016, IT/telecom outages are the third-leading cause of supply chain disruptions for the retail/wholesale industry (see Figure 1).

One especially pernicious attack method is ransomware, a form of malware that can be used to extort money from individuals and businesses. In a typical scenario, an employee receives an email that appears to be from a trusted vendor. The employee clicks on a link in the email, leading his computer to freeze and a message to appear on the screen: "Your files have been encrypted. Pay ransom within 24 hours in exchange for a computer key to decrypt your files." If a business does not pay, its data is likely to be destroyed or kept out of employees' reach through the malicious encryption software.

The potential losses for businesses that fall victim to such cyber-attacks can be extensive. Data could be damaged, corrupted, or lost. There could be extra expense required to replace or repair non-functioning computer and technology equipment. And there could be business interruption if critical systems are disrupted — that could lead to the loss of revenue during a temporary shutdown or, in a worst-case scenario, the permanent loss of customers who take their business to competitors.

QUANTIFYING CYBER BUSINESS INTERRUPTION RISK

The first step in managing direct loss from a cyber-attack, including business interruption (BI), is estimating its potential financial impact. Although historical data can be relied on to estimate the impacts of data breaches, cyber BI costs can be more difficult to determine because every event is different. How much an event costs will depend on several factors, including the organization's business model and response.

To quantify cyber BI risk, businesses can use scenario-based analyses, which determine a hypothetical fact pattern and estimate the resulting costs. A scenario-based analysis should focus on three factors:

- **Estimating the likelihood and severity of a cyber BI event.** Instead of looking at cyber risk simply as high, medium, or low risk, cyber BI risk should be expressed quantitatively: What is the likelihood that an organization will suffer an interruption within a specified timeframe, and how severe could the loss be? Each potential cyber BI scenario should be defined such that the likelihood of occurrence falls within a preselected range of likelihood based on risk management considerations.
- **Identifying mitigation options.** Depending on the significance of an organization's cyber BI exposures, options could include changing business processes, re-architecting IT infrastructure to improve resilience, enhancing restoration capabilities, or strengthening technical cybersecurity controls. In order to properly evaluate these choices and identify the strategies that will have the greatest impact, it's important to have a credible estimate of potential cyber BI exposure.
- **Evaluating risk transfer options.** Cyber BI is often underinsured or uninsured because many businesses do not fully quantify their risk prior to suffering a loss. But insurers are increasingly offering broader coverage for these exposures in both cyber policies and traditional property all-risk policies. In order to properly structure these insurance options — including selecting appropriate limits — businesses should identify and quantify their cyber BI exposures.

RISK MITIGATION

After quantifying their cyber BI risk, businesses can take steps to mitigate it. To protect against the potential impacts of ransomware and other cyber-attacks intended to cause them direct harm, retail and wholesale organizations should consider several precautionary steps, including:

- **Backing up all files regularly.** Many businesses do not regularly back up files on a separate system. Being able to recover data can make the loss of access to one source substantially less harmful.
- **Keeping all software up to date.** As part of an overall cyber risk avoidance strategy, IT administrators should ensure that operating systems, antivirus software, and web browsers are updated regularly. Web browser security settings should also be in force — for example, to block pop-up ads and potentially vulnerable plug-ins.
- **Educating employees.** The most effective line of defense for ransomware and other threats is an aware user. Employees should be trained on how to spot potentially dangerous emails and to not open attachments or click on links in unsolicited emails, including those that appear to be from suppliers, vendors, and other trusted sources. IT departments should also stay informed about the latest tools and techniques that cybercriminals are using.
- **Testing response plans.** For most businesses, it's not a question of "if" a cyber loss will occur — it's "when." So before an attack occurs, businesses should create incident response plans and

maximize their effectiveness through tabletop exercises. These exercises should use hypothetical but realistic cyber incidents, allowing risk professionals to identify areas for improvement or revision.

INSURANCE COVERAGE

Businesses should also consider their insurance options, including cyber, casualty, and property policies that address both the direct loss and liability that might arise from a cyber event. When cyber insurance policies were originally developed, they focused primarily on the hacking of corporate websites. Over the last 15 years, however, the coverage has evolved to address several risks. Broadly, cyber policies now cover risk arising from:

- The handling or collecting of confidential information.
- Operational reliance on technology.

Today's cyber policies thus may cover the failure of technology and the resulting interruption or loss of revenue — irrespective of the root cause. Insurers are also increasingly recognizing the interdependence of businesses, especially as respects technology, and are typically willing to include contingent business interruption (CBI) in cyber policies. A cyber policy can also cover an event that causes property damage — for example, damage to a computer or server. Cyber policies, however, are not generally meant to cover technology failures stemming from physical events — for example, building collapses, flooding, fire, or other physical perils.

Property insurance, meanwhile, has typically excluded coverage for cyber events; instead, these policies have traditionally been triggered by physical losses only. But as businesses increasingly experience business interruptions from ransomware and other forms of cyber-attacks without physical damage, property insurers appear more open to providing coverage. Some leading property insurers have recently said their policies will affirmatively cover specified first-party cyber events. Other property insurers may allow for similar coverage in their policies, usually by endorsement, on a case-by-case basis.

As they build insurance programs to address a range of potential cyber risks, it's important that retailers coordinate efforts around cyber, property, and casualty insurance purchases. Risk professionals should work with their insurance advisors to perform a diagnostic of these policies to determine current levels of coverage, identify any gaps or exclusions, and develop strategies to best manage their organizations' cyber risks.

MARSH

This briefing was prepared by Marsh's Retail/Wholesale Practice, in conjunction with Marsh's Cyber Practice, Marsh's Property Practice, and Marsh Risk Consulting.

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

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

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. This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh's prior written consent. 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, accounting, tax, 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. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or re-insurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.