TAKING STOCK

Elevating Retail Cyber Risk Management to the Next Level

Cyber-attacks continue to grow in complexity and occur frequently, and retail is among those industries at greatest risk. Although retailers have long had to contend with cyber risk — with many effectively doing so — new approaches are needed to meet new challenges. This edition of Marsh's *Taking Stock* series includes a Q&A with Reid Sawyer, Marsh's US Cyber Risk Consulting Leader, about the threats retailers are facing and how they can better manage them.

REID SAWYER
US CYBER RISK CONSULTING LEADER
MARSH

Q: How would you describe the cyber risk environment for retailers today?

A: Retailers are facing constantly evolving threats and potential sources of exposure. Brick-and-mortar and online retailers are collecting reams of data about their customers to support apps, rewards programs, and other efforts to enhance the customer experience. They also collect sensitive information on employees, suppliers, and others throughout the course of normal business operations. This data can include names, addresses, dates of birth, credit card information, social security numbers, and more. Such information makes retailers prime targets for hackers who can use a variety of attack methods to obtain access, including phishing and social engineering.

Hackers are also increasingly conducting direct attacks against businesses across all industries, using ransomware, malware, and other sophisticated methods. Retailers, like many businesses, often rely on third-party vendors to provide non-core services. These third parties often have access to, or process, company data. And retailers' relationships with them could potentially lead to cyber risk vulnerabilities because they could act as an entryway for attacks on retailers' corporate networks. Vendors could also become victims of hacking attacks themselves.

Nearly three-quarters of US retailers have experienced at least one breach in the past and the threat for retailers is only increasing. According to the retail edition of the 2018 Thales Data Threat Report, half of all US retailers have reported being breached in the last year.

Q: What lessons can we learn from 2017's WannaCry and notPetya attacks?

A: WannaCry and notPetya are examples of how sophisticated and destructive the techniques used by cyber-attackers have become. NotPetya, for instance, disabled servers and computers used by businesses around the world and across several industries.

The notPetya attack was notable for two reasons. First, it targeted operating systems that had not been properly patched. Second, it used aggressive malware code designed to disable functioning systems and rapidly spread to all machines it could find once inside businesses' networks.

For businesses across all industries, including retailers, this is a sign of what's to come. Future cyber-attacks will likely feature tools with these same characteristics.

Q: How are regulatory requirements evolving?

A: Regulatory requirements are becoming more stringent. Retailers that do business in Europe must now comply with the EU General Data Protection Regulation (GDPR), which took effect in May 2018. The law has expanded both individuals' personal information rights and organizations' compliance and breach notification obligations. It also has granted regulators far greater enforcement powers than they had before, including the ability to impose fines of up to €20 million or 4% of a company's annual global revenue — whichever is greater — on organizations with confirmed violations.

Similar laws are also being enacted in the United States. For example, the California Consumer Privacy Act of 2018, which takes effect in 2020, will grant consumers the right to know how their data is being used, to choose not to have their personal information resold by businesses that collect it, and to have their data deleted by businesses. Meanwhile, the Securities and Exchange Commission (SEC) recently released guidance on understanding and disclosing business-material cyber risks to investors. This means that effective cyber risk management must be a board-level issue for all companies, including retailers.

Q. Are retailers effectively managing their cyber risk?

A: Many retailers have robust information security programs for their corporate enterprise IT and credit card processing environments. However, as they transform digitally — enhancing customer experiences, expanding their supply chain, and embracing workforce mobility — the cybersecurity exposures they could face are growing faster than many retailers' capabilities. Given that, their ability to understand the full magnitude of cyber risk is being challenged.

Q. Beyond their existing efforts, what else do retailers need to do to manage cyber risk?

A: The cyber risk strategy of most retailers is founded on compliance and regulatory requirements rather than enterprise risk management fundamentals. Requirements under the Payment Card Industry Data Security Standard, the Sarbanes-Oxley Act of 2002, and data privacy regulations tend to be the baseline for retail information security programs. These are significant undertakings, but they have become separated from business expectations for risk management. Regulatory expectations should be viewed as minimum acceptable performance, but retailers should understand that this may not be sufficient to meet organization risk management goals.

A common compliance review tends to be binary and simplistic — we either met or did not meet a compliance objective. Meeting objectives is good; not meeting them is bad. Compliance-based audits, on the other hand, may detail risk in the language of low, medium, and high or red, yellow, and green. Enterprise risk management characterizes identified exposures in terms of economic impact to the enterprise in local currency — for example a $5 million manufacturing risk. Retail CISOs and CIOs need to take the additional step of quantifying identified cyber risks in terms that business leadership and boards of directors can understand and assimilate.

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

For more information, visit marsh.com, contact your local 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. 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.