MARSH

TAKING STOCK — DECEMBER 2019

Tackling the Retail and Restaurant Industry's Technology Conundrum

On a Monday in mid-December, a warehouse owned by a major retailer is bustling with activity as orders are being readied for delivery to stores. Suddenly, the inventory management system crashes, and remains unresponsive despite attempts to relaunch the program.

When employees restart their machines, the screens remain blank. Robots that are used to sort and ship inventory are stopped in their tracks. And it is soon discovered that the problem is not limited to one warehouse — locations across the country are having technology challenges.

Days later, the shelves at several of the retailer's locations are sparse. Orders that had to be sent in manually are yet to be fulfilled, even with employees working overtime and after temporary help is hired. And even once the systems are restored, it takes time for merchandise to be delivered and shelves fully stocked.

The ensuing investigation uncovers an elaborate cyber-attack that exploited a vulnerability of a third-party vendor to gain access to the retailer's systems, causing disruption and potentially compromising customer data. Not only were sales impacted during the busy holiday season, but the company incurred major extra expense to address the issue and get its operations up and running.

Technology Adoption Poses New Risks

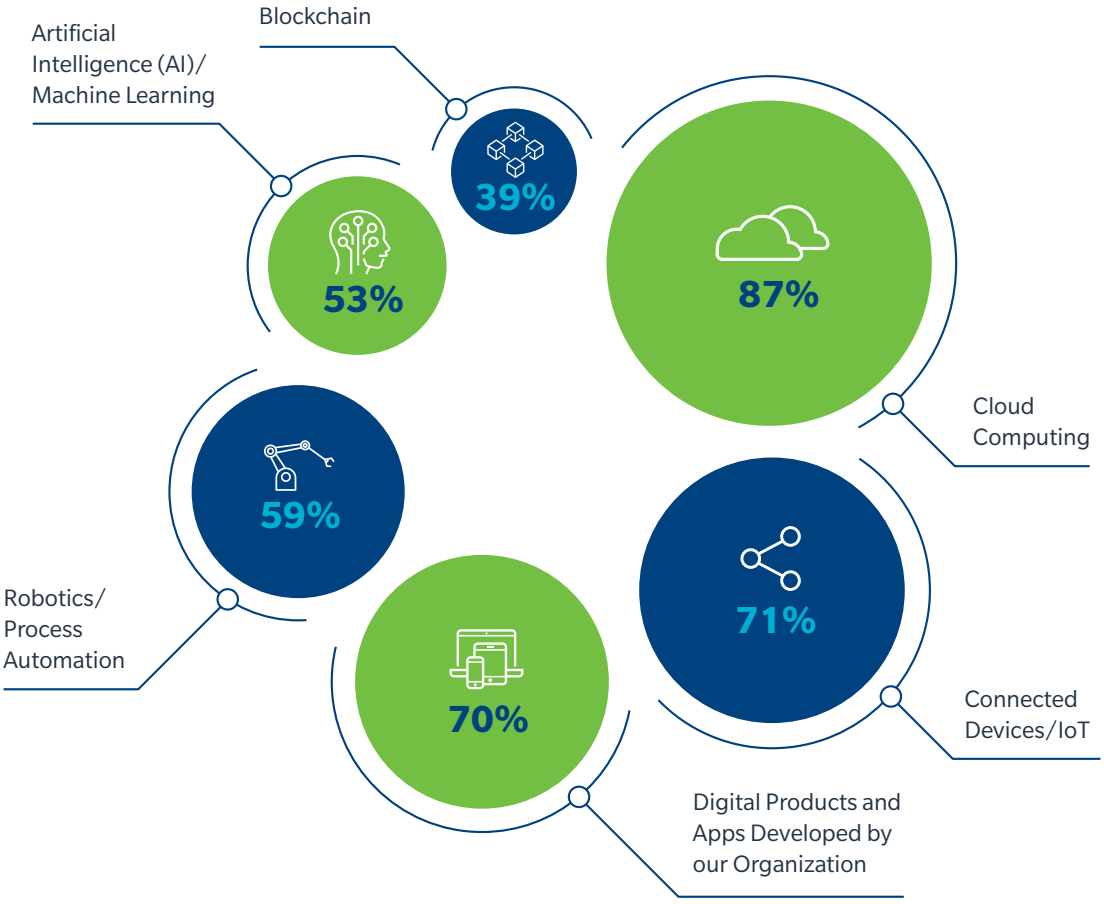
This scenario might be fictitious, but it is certainly not far-fetched. Cyber incidents are on the rise and retailers and restaurants are increasingly at risk of attacks that can paralyze their systems, leading not only to direct financial losses, but also potentially lasting reputational damage.

In parallel, technology is transforming the way retailers and restaurants do business, revolutionizing not only customer interactions but also back-end operations. Automated distribution centers allow companies to become more efficient, while artificial intelligence (AI) leverages data to improve customer interactions and create an improved, and increasingly personalized, omnichannel experience. And according to the recent *2019 Global Cyber Risk Perception Survey* published by Marsh and Microsoft, many retail, wholesale, food, and beverage companies are either already using or considering using these technologies (see Figure 1).

FIGURE 1

Most retail, wholesale, food, and beverage organizations are considering or using a range of new technologies.

Q: For each of the following technologies, please indicate which consideration or usage scenario best applies to your organization.



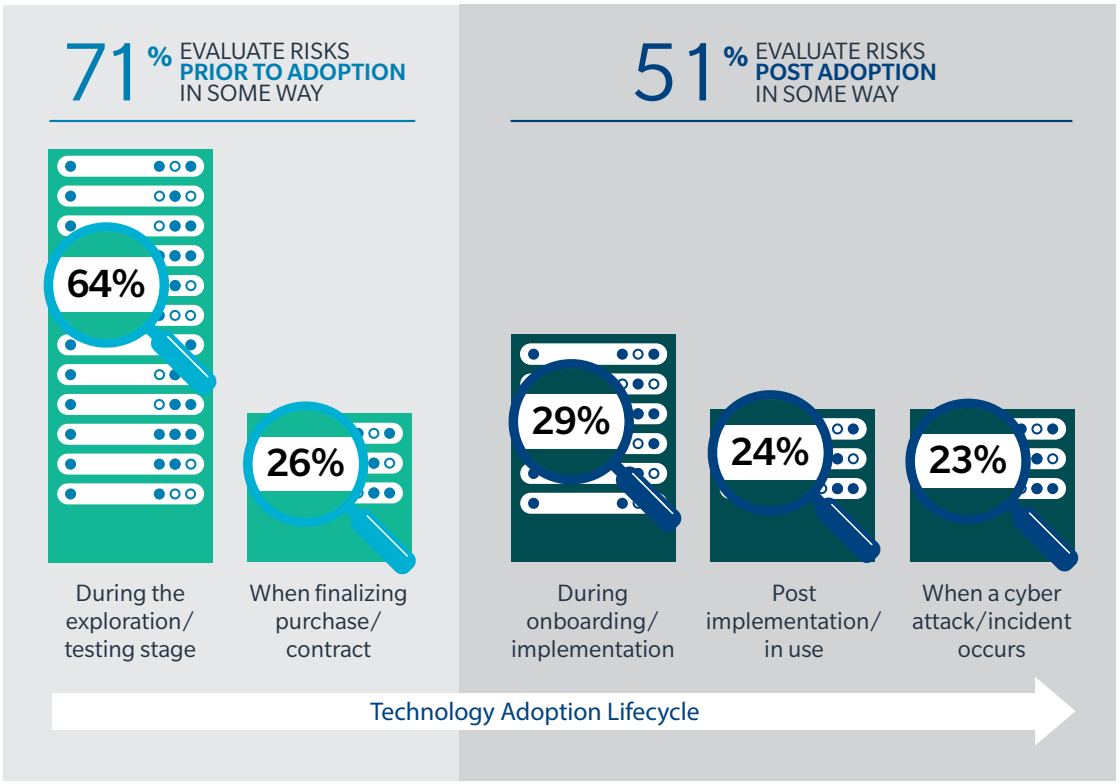
Despite their myriad advantages, new technologies, especially connected ones, could become major liabilities if infiltrated by cyber-attackers. But notwithstanding the potentially ruinous risks, only 28% of industry respondents to the Marsh and Microsoft survey said they evaluate the risks of new technologies both prior to and after adoption, while only 5% evaluate risks during all possible stages of the lifecycle (see Figure 2). And more worryingly, 8% of industry respondents don't carry out any evaluation.

While adopting the latest technologies can lead to operational benefits, including greater efficiency and lower costs, businesses that do not take comprehensive measures to understand, measure, and address the risks associated with these new technologies could be compounding their cyber risk. And the evolving nature of both cyber risk and technology means that continuous assessment is essential to determine whether and how these technologies are expanding a company's risk profile.

FIGURE 2

Retail, wholesale, food, and beverage companies most commonly evaluate cyber risk during the exploration/testing stage of technology adoption.

Q: When adopting and implementing new technologies, such as those you have just identified, at which of the following stages is cyber risk typically evaluated in your organization?



Only **28%** evaluated risks both prior to and after adoption.

Just **5%** evaluate risks at all possible stages of the lifecycle.

8% don't evaluate at all.

Strengthening the Weakest Link

Today's world is inter-connected and technology-dependent. And while that can lead to greater efficiency, it can also amplify risks. Retailers and restaurants are increasingly relying on technology to power their supply chains, with more businesses than ever before automating their entire distribution processes. But while a digitized process has tremendous advantages, what happens when the system breaks? The whole process — from orders to deliveries — can be brought to a screeching halt, leaving shelves empty, perishables rotting in warehouses, and brands tarnished.

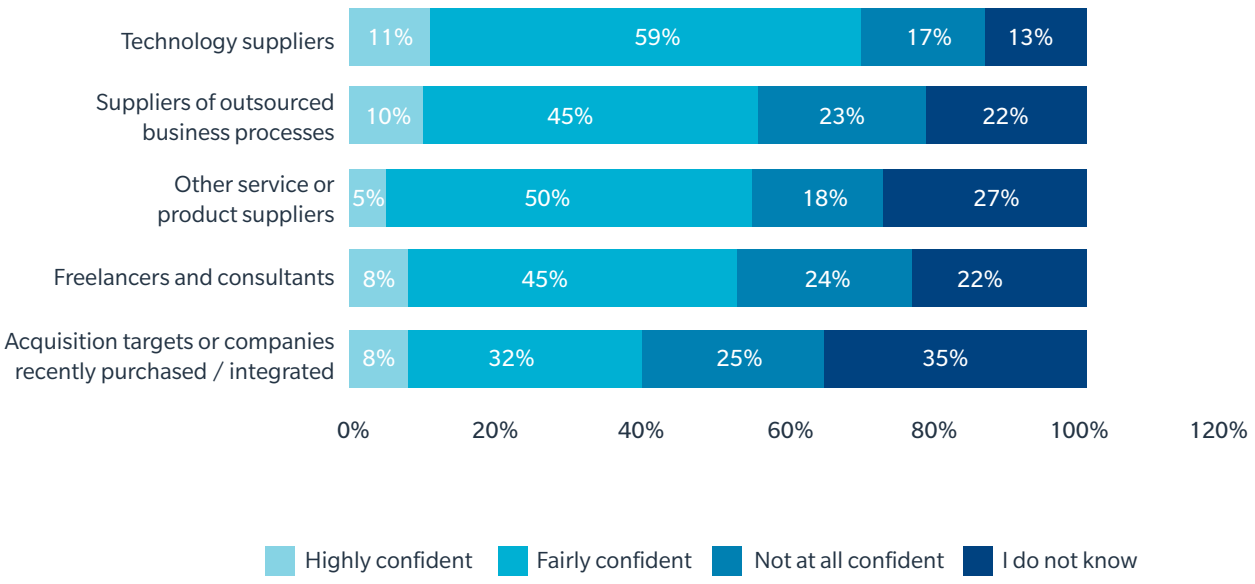
So if technology is so crucial to the internal operations of a business, why are we not seeing more organizations focus their efforts on ensuring that technology investments don't work against them? And equally important, do retailers and restaurants understand the potential risks posed by their supply chain partners?

Almost 20% of industry respondents to the Marsh and Microsoft survey said their supply chain posed a cyber risk to their organization. And yet, only 10% of industry respondents said they are highly confident in their organization's ability to prevent or mitigate cyber risk originating from suppliers of outsourced business processes (See Figure 3).

FIGURE 3

Confidence in Organization's Ability to Prevent / Mitigate Cyber Risk from Third Parties

Q: How confident are you in your organization's ability to prevent / mitigate cyber risk from the following?



And worryingly, less than half of industry survey respondents (42%) said they always perform their own due diligence of new technologies, devices, or apps provided by vendors instead of accepting security claims by their vendors. A robust vendor vetting process should include an evaluation of the cyber security controls embedded or built into technology and devices supplied by vendors as well as a thorough understanding of any network and information access to which the vendors will be granted.

When it comes to cyber preparedness, we tend to see a distinction between those organizations that have already fallen victim to cyber-attacks, like 2017's NotPetya, and those that have been spared. The latter seem less able to envision the impact that a black swan event could have on their operations. As such, we need to change the frame of reference from recognizing that the risk exists to really understanding the magnitude of that risk and taking proactive action to protect operations.

The Way Forward

The threat posed by cyber incidents is not going away. Rather, as attackers become more astute and technology continues to proliferate, cyber breaches are only likely to increase. In the face of this persistent threat, retailers and restaurants should take the following steps to become more cyber resilient:

1. **Build a strong culture of cybersecurity.** Cyber risk is a strategic threat to the entire business. All stakeholders must be involved in decisions about cybersecurity; the C-suite should continuously have cyber on its radar and boards should regularly include it on their agenda. Moreover, the entire organization should stand behind a rigorous cyber risk management strategy that includes the appropriate governance, prioritization, resources, and resilience-building measures.
2. **Continuously assess the risk posed by new technologies.** An evaluation of the risk impact of new technologies and devices should not just happen before implementation. Instead, engage in continual reviews throughout the technology lifecycle, with input from key stakeholders from across the business.
3. **Trust, after verifying.** Be cognizant that your risks are not restricted to your organization — your security is only as strong as its weakest link, which is often a third-party vendor. Evaluate the security of your vendors' devices and technologies against your own organization's technology footprint, cyber exposures, and business model. Pay special attention when a technology is critical to your core operations and can bring your company to a standstill if it is impacted.
4. **Measure cyber risk in economic terms.** Replace technical jargon with a quantified cost in dollars that can be understood across the business. Armed with economic data, you can better utilize funds allocated for cyber by targeting investment towards the largest exposures and optimize the balance of technology versus insurance, which can provide crucial protection against cyber-related losses.
5. **Change your mindset.** Do not limit your focus to technology and controls, but invest in planning, training, response rehearsal, and collaboration both internally and with outside resources to ensure continual operations during and after an incident.

This briefing was prepared by Marsh's Retail/Wholesale Practice in conjunction with Marsh JLT Specialty Cyber Practice.

For more information, 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