MARSH

FOOD FOR THOUGHT — DECEMBER 2019

# Hungry to Modernize, Food and Beverage Companies Aren't Considering Technology Risks

Like those in many industries, food and beverage companies have grown ever-more complex in recent years. Every corner of their operations is now seemingly reliant on technology, which itself is evolving and growing more complicated with each passing day.

Technology can offer many benefits, helping food and beverage companies to automate key functions, improve efficiency, enhance customer experiences, and ultimately become more profitable. But in their zeal to update and reshape their operations, many organizations are not taking the time to fully evaluate their potential cyber risks.

## Embracing — But Not Vetting — New Tech

For most organizations, using the latest technologies to yield operational efficiencies is part of a strategy to remain competitive and profitable. But one of the key findings of the *2019 Global Cyber Risk Perception Survey* published by Marsh and Microsoft is that while businesses are eager to tap into the potential of innovative technologies, their assessment of the risks that come with them is not nearly as robust as it should be.

For food and beverage companies, the power of new technology is clear: It can revolutionize the traditional supply chain that's essential to their viability, turning it into a digital supply chain that's faster, more flexible, more efficient, more accurate, and better integrated. Among other things, the industrial Internet of Things (IoT) can help to connect manufacturing operations to the internet and automate key processes. And robotics can aid in distribution and fulfillment. Artificial intelligence, blockchain, cloud computing, and more present countless opportunities across organizations.

Unsurprisingly, many food and beverage companies are using or considering at least one of these and other new 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.**

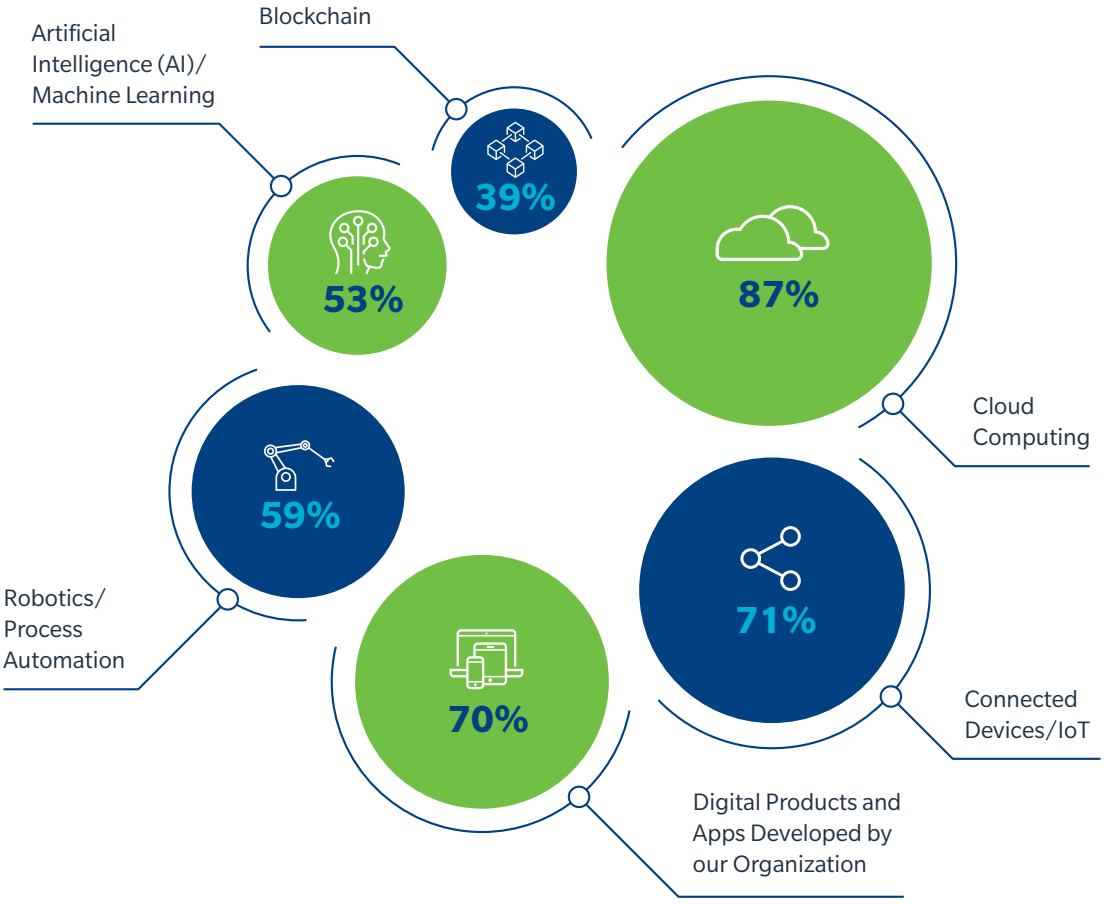
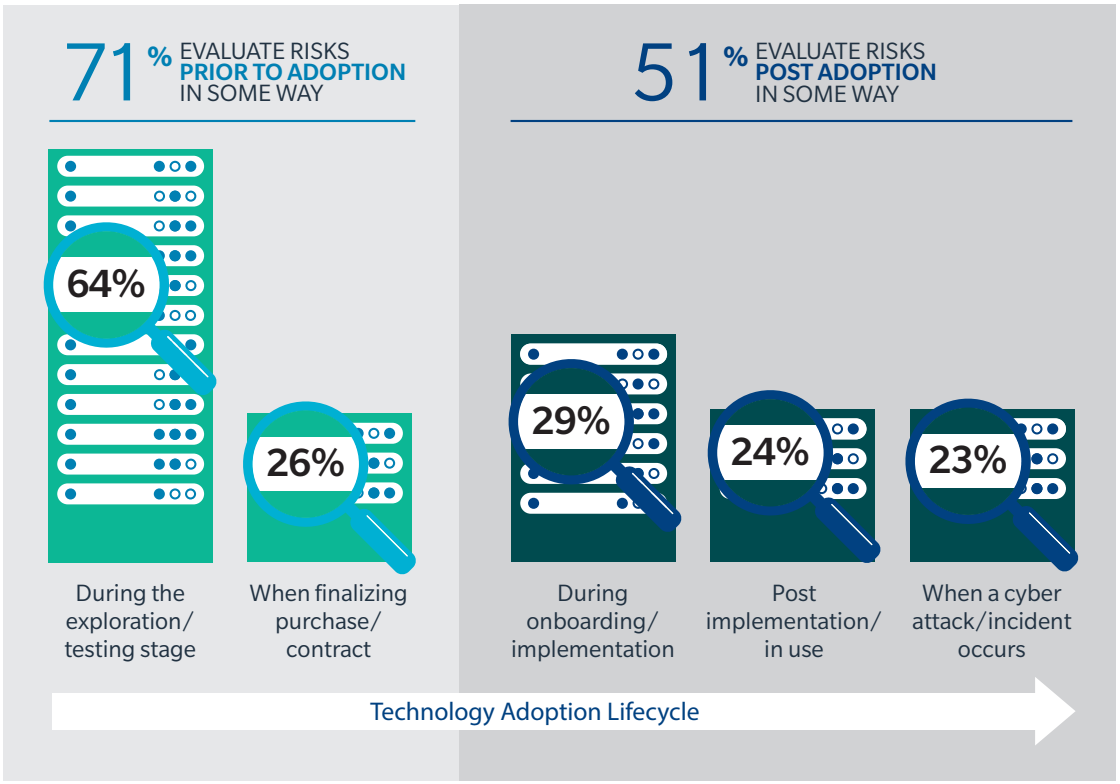


FIGURE 2

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.

And yet, only 28% of retail, wholesale, food, and beverage companies evaluate the risks inherent in new technology both prior to and following its adoption (see Figure 2). Just 5% evaluate risks at all stages of the adoption lifecycle, from exploration and testing through post-implementation and in the event of a cyber loss. But what is perhaps most troubling: 8% don't evaluate new technology risks at all.

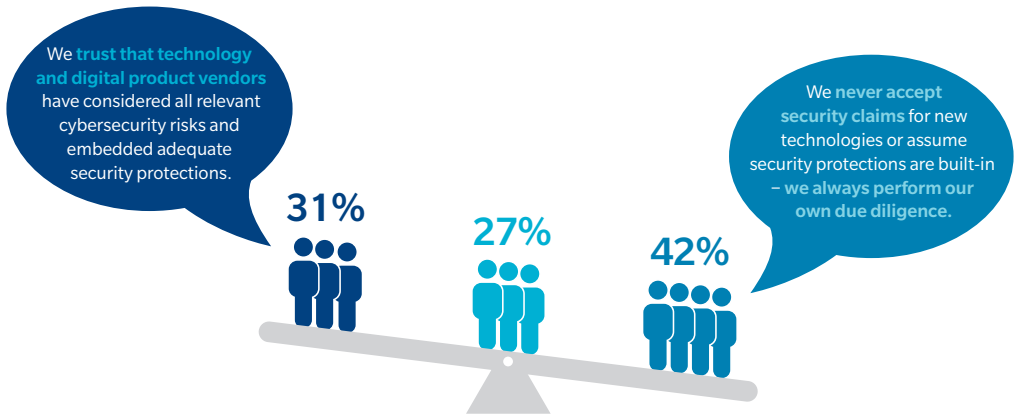
This inattention to potential technology exposures could have ruinous consequences for organizations. Consider a food and beverage manufacturer that is in the middle of an already hectic day when its automated production lines grind to a halt. Despite several attempts, employees cannot bring the systems back online, and there are nowhere near enough workers to manually operate the lines. Meat, dairy, and other perishables are spoiled and orders cannot be fulfilled, leading to lost revenue, extra expense, and a domino effect on retail and other customers that don't receive their orders and are losing revenue themselves. An investigation uncovers an elaborate cyber-attack that exploited a vulnerability in third-party software used to run the production lines and which was not properly evaluated following a recent update. And even after the issue is resolved and production resumes, irate customers decide to change suppliers.

For any food and beverage company leveraging new technology but failing to conduct its due diligence, this hypothetical scenario is all too realistic. And it's an even bigger risk for those organizations that are not looking at technology risks outside of their own walls. Less than half of industry respondents to the Marsh and Microsoft survey said they perform due diligence to verify that the devices, tools, or apps supplied by their technology vendors have effective security protections in place (see Figure 3).

FIGURE 3

One-third of retail, wholesale, food, and beverage organizations assume technology vendors have considered all relevant cyber risks.

**Q: For each of the following pairs of statements, please indicate which most strongly reflects your organization's attitude.**

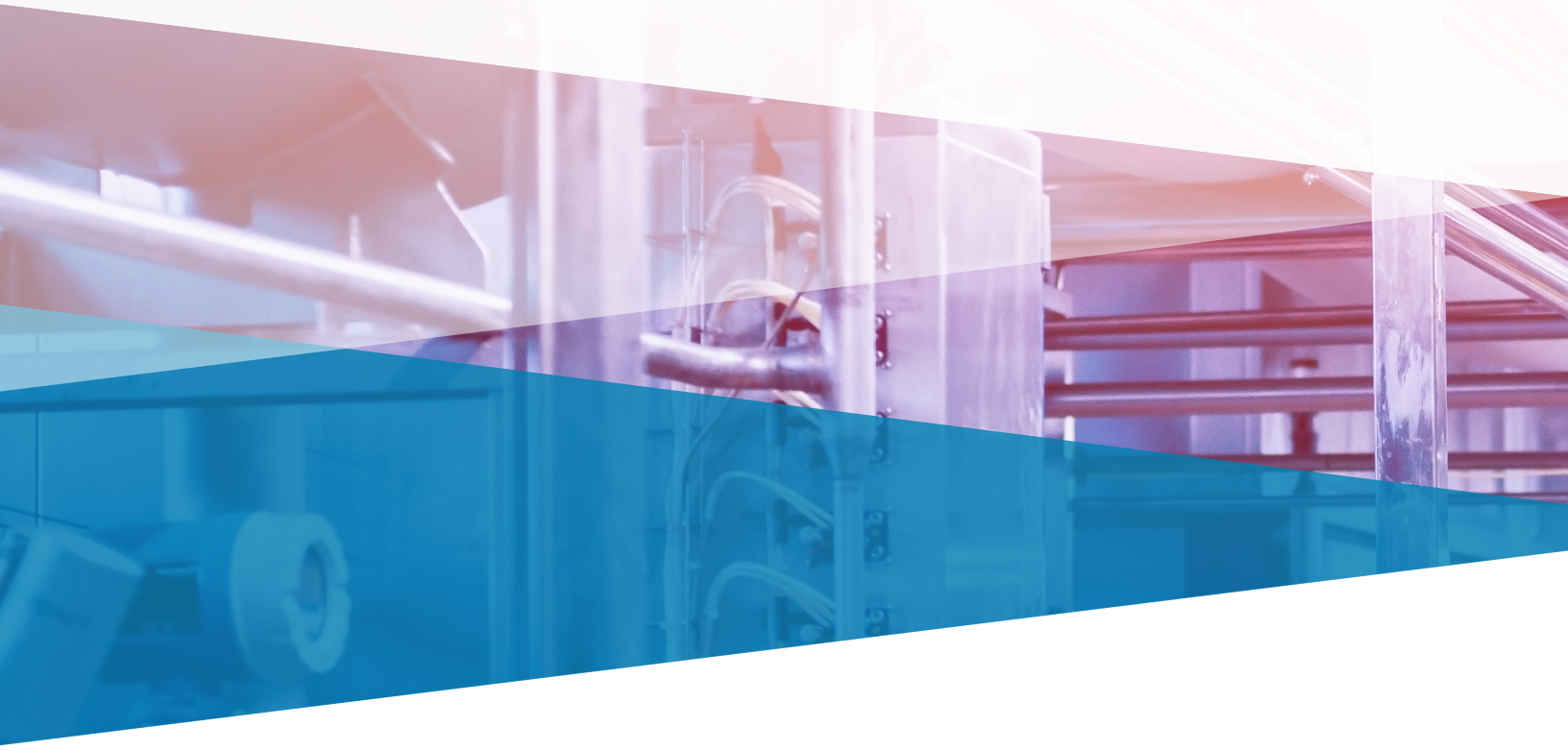


## Achieving Cyber Risk Resilience

The net result of these trends is that many organizations are not resilient to cyber risks that could cripple them. Changing that starts with considering the following actions:

- **Build a strong cybersecurity culture.** Cyber risk must be treated as a strategic threat rather than a purely technical one. Don't relegate cyber risk solely to IT; involve all key stakeholders in its management. And make it a regular board agenda item.


- **Frame cyber risk in economic terms.** Dollars and cents are the lingua franca that you should use to express cyber risk instead of technical jargon. If everyone's speaking the same language, it will be easier to understand what's at risk and maximize your investments in both cyber risk transfer and risk mitigation.
- **Don't focus solely on prevention.** Technology and controls are important, but so are planning, training, response rehearsal, and engaging outside resources. Insurance also has a critical role to play.
- **Continually assess your risk.** Evaluate the risks from new technologies and devices throughout their lifecycle—before, during, and after implementation.
- **Carefully manage third-party risks.** Evaluate security of vendor devices and technologies against your organizations' technology scheme. Engage your supply chain partners about bilateral supply chain risk and shared responsibilities. And continually review third parties' approach to managing risks, including ensuring that their standards are as rigorous as your own and requiring them to purchase adequate insurance.



**This briefing was prepared by Marsh's Food and Beverage Practice, in conjunction with Marsh JLT Specialty Cyber Practice.**

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

GREG BENEFIELD
Managing Director
National Food & Beverage Segment Leader
+1 615 340 2449
greg.benefield@marsh.com