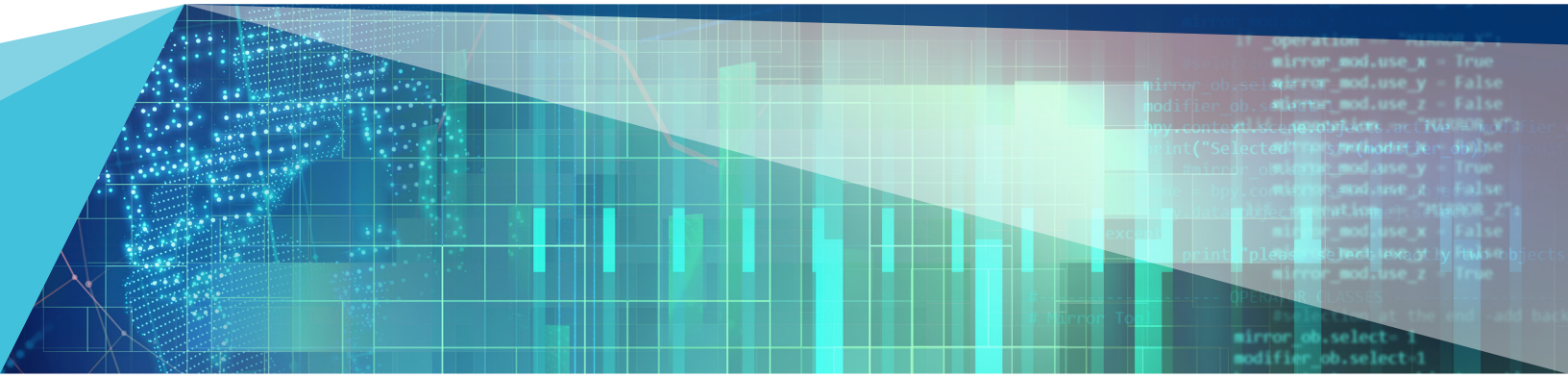
FOOD FOR THOUGHT

A PERIODIC EXAMINATION OF KEY ISSUES AND TRENDS FROM MARSH'S FOOD & BEVERAGE PRACTICE



MANAGING FOOD AND BEVERAGE COMPANIES' GROWING CYBER RISKS

Cyber risk is often considered synonymous with data breach. But for food and beverage companies, a potentially bigger threat is a disruption of normal operations from a technology failure. No food and beverage company can fully eliminate this threat, but organizations can take steps to minimize their loss of income, reputational damage, and other adverse effects of such disruptions.

CYBER-ATTACKERS EXPANDING THEIR REACH

Imagine one of your employees checks his corporate email and finds a message that appears to be from a trusted vendor. He clicks on a link in the email — and his computer freezes. A message pops up: "Your files are encrypted. Pay ransom within 24 hours in exchange for a computer key to decrypt your files." If you don't pay, your data will either be destroyed or simply kept out of reach through malicious encryption software.

An attack of this type is known as ransomware, a form of malware that cybercriminals are increasingly using to extort money from individuals and businesses. And it's just one example of how cyber-attacks have evolved.

Over the last decade, businesses have become increasingly reliant on technology. Food and beverage manufacturers and processors, for example, use computers to run production lines and track the movement of products and ingredients throughout the production process. Restaurants, meanwhile, often rely on technology to manage customer transactions, reservations, inventory, and other critical functions.

At the same time, cyber-attackers have grown more sophisticated, and expanded their reach. Criminals continue to look for opportunities to steal customers' personally identifiable information. Although parts of the food and beverage industry continue to face this threat — most notably, restaurants — cyber-attackers now also target businesses and look for opportunities to extort money or otherwise profit from technology disruptions.

For food and beverage companies that fall victim to such cyber-attacks, the potential losses can be extensive. These include the damage, corruption, or loss of data; extra expenses to replace or repair non-functioning computer and technology equipment; and business interruption — including the loss of revenue — if critical systems are disrupted.

QUANTIFYING CYBER BUSINESS INTERRUPTION RISK

To manage direct loss from a cyber-attack, including business interruption (BI), the first step is to estimate the potential financial

impact. Every cyber BI event is different, depending on such specifics as the organization's business model and how it responds. By using a scenario-based analysis to quantify cyber BI risk, a business can 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.** Cyber risks have often simply been characterized as high, medium, or low risk, but this approach is typically of limited value. Instead, cyber BI risk can be expressed quantitatively: What is the likelihood that an organization will suffer an interruption within a specified timeframe, and how severe might the loss be?
- **Identifying mitigation options.** Depending on the significance of an organization's cyber BI exposures, options may include changing business processes, re-architecting IT infrastructure to improve resilience, enhancing restoration capabilities, or strengthening technical cybersecurity controls. It's important to have a credible estimate of potential cyber BI exposure in order to properly evaluate these choices and identify the strategies that will have the greatest impact.
- **Evaluating risk transfer options.** Many businesses do not fully quantify their risk prior to suffering a loss, which means cyber BI is often underinsured or uninsured. Both cyber and traditional property insurers, however, are increasingly offering broader coverage for these exposures. Quantifying cyber BI exposures is critical to decisions about limits purchasing and other program specifics.

RISK MITIGATION

After quantification, businesses can take action to mitigate cyber BI risk. Food and beverage companies should consider several steps to better protect against the potential impacts of ransomware and other direct cyber-attacks, including:

- **Backing up files.** 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 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 regularly updated. Web browser security settings should also be in force — for example, to block pop-up ads and potentially vulnerable plug-ins.
- **Educating employees.** IT departments should stay informed about the latest tools and techniques that cybercriminals are using. And risk professionals should remember that the most effective line of defense for ransomware and other threats is an aware user. Employees should be trained 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.
- **Practicing their response.** Before an attack occurs, businesses should create incident response plans. These plans should be tested through tabletop exercises, using hypothetical cyber incidents that are realistic to their business. This can help identify areas for improvement or revision.

INSURANCE COVERAGE

Property insurance has typically excluded coverage for cyber events; 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.

Meanwhile, standalone cyber policies continue to evolve. When cyber insurance policies were originally developed, they focused primarily on hacking attacks against corporate websites. But today's cyber policies typically cover a broad range of risks 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.

As they build insurance programs to address a range of potential cyber risks, it's important that food and beverage companies coordinate their cyber, property, and casualty insurance purchasing decisions. 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.

This briefing was prepared by Marsh's Food & Beverage Practice, in conjunction with Marsh's Cyber Practice and Marsh Risk Consulting.

For more information on this topic, contact your local Marsh representative or:

GREG BENEFIELD
Food & Beverage Segment Leader
+1 615 340 2449
Greg.Benefield@marsh.com